Diss. ETH No. 18762

How to Secure Supply Chains Against Counterfeit Products Using Low-Cost RFID

A dissertation submitted to
ETH ZURICH

for the degree of
DOCTOR OF SCIENCES

presented by

MIKKO OLAVI LEHTONEN

MSC (TECH), HELSINKI UNIVERSITY OF TECHNOLOGY

Date of birth
20 April 1981
citizen of
Finland

accepted on the recommendation of

Prof. Dr. Elgar Fleisch
Prof. Dr. Friedemann Mattern

2009

Acknowledgments

I wish to express my gratitude to all who supported me during my Doctoral Thesis, for this work could not have been completed without their help.

First, I want to thank my supervisor Prof. Dr. Elgar Fleisch for inspiring me with the vision of the Internet of Things which anchors this work in the intersection of technology and business, and for providing me great guidance throughout the thesis. I want to thank my co-supervisor Prof. Dr. Friedemann Mattern for his valuable comments and for challenging my views, my project manager Dr. Florian Michahelles for passing on to me a huge amount of knowledge of all aspects of academic work and for working close with me in each step of the way, and topic-wise my predecessor Dr. Thorsten Staake for helping me to get a head-start with the topic and for being another mentor for me.

For an exciting and fruitful collaboration I want to thank all my project partners, especially Manfred Aigner, Walter Bisson, Kristina Bogataj, Daniel Boos, Trevor Burbridge, Craig Cook, Paul Davis, Olaf Dressel, Fabien Gourmanel, Eric Gout, Dr. Mark Harrison, Dr. Oliver Kasten, Hans-Jürgen Körner, Dr. Carsten Magerkurth, Jens Müller, Nina Oertel, Matthias Pfletschinger, Antti Ruhanen, Michael Schelper, Andrea Soppera, and Dr. Harald Vogt. I also want to thank Prof. Dr. Srdjan Capkun, Mark McGlade, Mikko Nikkanen and Dr. Justin Picard for sharing their perspectives in interesting discussions.

My colleagues at ETH and HSG deserve a big thank you for the stimulating working environment and for teaching me German. I especially thank Jasser Al-Kassab, Oliver Baecker, Albrecht Bereuter, Cosmin Condea, Ali Dada, Erica Dubach Spiegler, Thomas Fischer, Dr. Christian Floerkemeier, Dr. Heiko Gebauer, Tobias Graml, Monica Heinz, Dr. Alexander Ilic, Tobias Ippisch, Stephan Karpischek, Claire-Michelle Loock, Dr. Christian Metzger, Dr. Felix Pütz, Dr. Patrick Schmitt, Alexander Skorna, Prof. Frédéric Thiesse, Elisabeth Vetsch-Keller, Felix von Reischach, Stephan von Watzdorf, Markus Weiss, and Thomas Wiechert. I also thank Ali Mouhsine for lending me his creative hand for my final presentation.

Last, I want to thank my whole family for their support and love, Paula and Pekka, Maija and Teemu, Päivi and Olle, Olli and Hanna. The most special thank you goes to my wife Karima: *merci pour être là*.

April 2010, Zurich

Mikko Lehtonen

Table of Contents

List of Figures

List of Tables

Abstract

Counterfeiting of branded and trademarked products is an industrial-scale problem that continues to affect industries and societies alike, harming legally run businesses and their clients. Brand owners may expect new technical countermeasures emerge from the information technology (IT) that is being introduced for improved supply chain management. In particular, many products will be tagged with radio frequency identification (RFID) technology that can uniquely identify multiple products at once without a line of sight. However, low-cost RFID tags that will be deployed in quantities of several millions can be cloned. If this threat is not addressed, low-cost tags do not enable secure product authentication and thus their value in anti-counterfeiting is rather limited. Moreover, brand owners lack the knowledge and tools to evaluate the effectiveness of different technical anti-counterfeiting measures.

This thesis investigates how supply chains can be protected from counterfeit products using low-cost RFID tags. To address tag cloning, two new concepts are proposed for the detection of cloned tags in supply chains where products are traced. These concepts use the visibility that the RFID system provides and they are evaluated based on expert interviews, analytical modeling, a simulation study, and prototype construction. To illustrate that these concepts can be implemented on low-cost RFID, their applicability on EPC Class-1 Gen-2 tags is demonstrated.

In addition to developing novel security concepts, this thesis takes a systematic approach to model security in anti-counterfeiting. The level of security in product authentication is formalized and linked to the overall level of security that technical anti-counterfeiting measures provide to a supply chain, and the effect of security on a counterfeiter's business is modeled.

Results of this thesis suggest that the proposed measures can reliably detect cloned RFID tags when products are traced. Imperfect visibility causes false alarms and false negatives, the latter of which need to be addressed by another level of product verification. Modeling of security in anti-counterfeiting reveals that the effectiveness of existing technical countermeasures is best improved by increasing the product check rates. Since a solution based on low-cost RFID can achieve orders of magnitude increase in product check rates, for example through integration of authenticity checks to normal product handling processes, such a solution can be very effective in protecting a supply chain from counterfeits. Furthermore, the presented econometric analysis explains how factors like high lot size and serial numbering itself contribute to a higher counterfeit product detection rate. Findings of this thesis are used to derive guidelines and an implementation roadmap for the use of low-cost RFID in anti-counterfeiting.

All in all, results of this thesis suggest that low-cost RFID can be an effective anti-counterfeiting technology inside supply chains, despite some uncertainty in the checks themselves. This represents a paradigm shift from a high cost-to-break toward a high counterfeit product check rate which is achieved by easy and fast checks. In this way technical anti-counterfeiting measures can take a bigger role in affected companies' anti-counterfeiting strategies and make counterfeiting financially unattractive instead of treating the symptoms of the problem.

Zusammenfassung

Das Fälschen geschützter Produkte ist ein Problem von industrieller Größe, welches Industrie und Gesellschaft zugleich betrifft. Produkteigentümer können neue technische Gegenmassnahmen durch die Einführung von Informationstechnologie in der Supply-Chain erwarten. Um das Management der Supply-Chain zu verbessern, werden zukünftig viele Produkte mit RFID-Chips ausgestattet. Diese Technologie erlaubt es mehrere Produkte auf einmal berührungslos und ohne direkten Sichtkontakt zu identifizieren. Problematisch ist jedoch die Tatsache, dass in der Produktion günstige RFID-Tags (EPC/RFID), die in der Praxis in Zukunft millionenfach Verwendung finden könnten, auch einfach gefälscht werden können. Sollte dieses Problem nicht gelöst werden, können mit der Technologie ausgestattete Produkte auch nicht sicher authentifiziert werden, was ihren Wert im Einsatz für die Fälschungssicherheit von Produkten stark einschränkt. Problematisch ist zudem, dass viele Markenhersteller nicht über das nötige Wissen und die Mittel verfügen, um die Effektivität verschiedener technischer Massnahmen zu evaluieren.

Diese Arbeit beschäftigt sich mit der Frage, wie EPC/RFID-Chips eingesetzt werden können, um die Supply-Chain vor gefälschten Produkten zu schützen. Um das Einführen von geklonten Tags in die Supply-Chain zu erkennen, werden zwei neue Konzepte vorgestellt, die auf der, durch das RFID System mittels Nachverfolgung von Produkten, erzeugten Visibilität basieren. Die Konzepte werden anhand von Experteninterviews, Modellierung, Simulationsstudien und einem konstruiertem Prototyp evaluiert und ihre Anwendbarkeit durch die Umsetzung auf EPC Class-1 Gen-2 Tags demonstriert.

Zusätzlich zur Entwicklung neuartiger Sicherheitskonzepte, beschäftigt sich diese Arbeit auch mit der systematischen Modellierung von Sicherheitseffekten im Bereich der Fälschungssicherheit. Die Sicherheit im Bereich der Produktauthentifizierung wird formalisiert und der Gesamtsicherheit aller technischen Massnahmen zur Absicherung der Supply-Chain gegenübergestellt. Desweiteren, wird der Effekt auf das Geschäft des Fälschers modelliert

Die Ergebnisse dieser Arbeit weisen darauf hin, dass bei der Nachverfolgung von Produkten mit den vorgeschlagenen Massnahmen geklonte RFID Tags zuverlässig identifizieren werden können. Unzureichende Visibilität führt zu Fehlalarmen und fälschlich erkannten Tags. Letzteres Problem muss durch eine andere Art der Produktverifikation angegangen werden. Die Modellierung von Sicherheit und Fälschungssicherheit zeigt, dass die Effektivität der bereits existierenden technischen Massnahmen am besten durch eine Erhöhung der Überprüfungsrate von Produkten erreicht werden kann. Da beim Einsatz von EPC/RFID basierenden Lösung die Überprüfungsraten von Produkten sich um eine ganze Grössenordnung steigern kann, beispielweise durch die Integration von Authentizitätsprüfungen in den normalen Abwicklungsprozess, kann eine solche Lösung sehr effektiv zum Schutz innerhalb einer Lieferkette sein. Desweiteren erklärt die präsentierte ökonometrische Analyse, den Einfluss von Faktoren, wie z.B. eine grosse Chargengrösse und das Vorhanden sein einer serielle Nummerierung, zu einer Erhöhung der Erkennungsrate von Fälschungen führen. Die Erkenntnisse dieser Arbeit werden zum Ableiten von Richtlinien und einem Implementierungsplan zur Nutzung von EPC/RFID zur Erhöhung von Fälschungssicherheit genutzt.

Alles in Allem zeigen die Ergebnisse dieser Arbeit, dass EPC/RFID, abgesehen von einigen Unsicherheiten bei der Überprüfung selbst, eine effektive Fälschungssicherheitstechnologie innerhalb von Lieferketten darstellt. Dies repräsentiert einen Paradigmenwechsel, von der Erhöhung des Aufwands zum Knacken des Schutzes zu einer Erhöhung der Überprüfungsrate von gefälschten Produkten, welche durch einfache und schnelle Überprüfung erreicht wird. Hierdurch können technische Fälschungssicherheitsmassnahmen eine grössere Rolle in der Fälschungssicherheitsstrategie von betroffenen Unternehmen einnehmen und so das Herstellen von Fälschungen finanziell unattraktiv machen anstatt lediglich die Symptome des Problems zu behandeln.

Tiivistelmä

Tavaramerkkien väärentäminen ja kopiointi koskee monia teollisuuden aloja, vahingoittaen laillisesti toimivia yrityksiä ja heidän asiakkaitaan sekä yhteiskuntia yleensä. Uudet toimitusketjujen hallintaan käytetyt tekniikat, kuten radio frequency identification (RFID) -tekniikkaan perustuvat tunnisteet jotka voivat tunnistaa useita tuotteita yhdellä lukukerralla ilman suoraa näköyhteyttä lukijan ja tunnisteen välillä, mahdollistavat uusia teknisiä toimenpiteitä tuoteväärennöksiä vastaan. Mutta yleisimmät RFID-tunnisteet ovat yksinkertaisia elektronisia laitteita jotka voidaan kopioida väärennettyihin tuotteisiin. Jos tätä uhkaa ei oteta huomioon, nämä RFID-tunnistet eivät mahdollista luotettavaa tuoteautentikointia. Yleinen ongelma on että tuotemerkkien omistajilla ei ole tarvittavaa tietotaitoa määrittää erilaisten teknisten vastatoimien tehokkuutta tuotemerkkien suojelussa.

Tämä väitöskirja tutkii kuinka toimitusketjuja voidaan suojata tuoteväärennöksiltä käyttäen yksinkertaisia RFID-tunnisteita. Tunnisteiden kopiointinnista johtuva turvallisuusongelma ratkaistaan ehdottamalla kahta uutta tapaa havaita kopioidut tunnisteet käyttäen RFID-tekniikan tarjoamaa näkyvyyttä. Ehdotettuja ratkaisumalleja arvioidaan asiantuntijahaastatteluden, analyyttisten mallien, simulaation ja prototyypin avulla. Tekniikoiden soveltuvuus yksinkertaisille tunnisteille demonstroidaan EPC Class-1 Gen-2 -tunnisteisiin perustuvalla toteutuksella.

Uusien teknisten ratkaisumallien lisäksi tämä väitöskirja ehdottaa systemaattista tapaa mallintaa kuinka tehokkaasti tekniset vastatoimet autentikoivat tuotteita, suojaavat toimitusketjua, ja kuinka vastatoimet vaikuttavat tuoteväärentäjän liiketoimintamalliin.

Ehdotetut ratkaisumallit havaitsevat kopioidut tunnisteet luotettavasti kun alkuperäisten tuotteiden paikat toimitusketjuissa tiedetään riittävällä tarkkuudella. Puutteellinen näkyvyys johtaa vääriin havantoihin mitkä voidaan todentaa muilla autentikointimenetelmillä. Vastatoimien tehokkuuden mallinnus näyttää, että nykyisten teknisten vastatoimien tehokkuutta voidaan parhaiten parantaa kasvattamalla tarkisttettavien tuotteiden määrää. Koska RFID-tekniikkaan perustuva ratkaisu voi merkittävästi kasvattaa tarkisttettavien tuotteiden määrää, esimerkiksi yhdistämällä tuoteautentikoinnin muihin tuotteidenkäsittelyprosesseihin, RFID-tekniikkaan perustuva ratkaisu voi tehokkaasti havaita tuoteväärennökset toimitusketjuissa. Lisäksi esitetty ekonometrinen analyysi selittää kuinka tekijät kuten eräkoko ja sarjanumerointi vaikuttavat tuoteväärennösten havaitsemiseen. Perustuen näihin havantoihin, tämä väitöskirja esittää kuinka yksinkertaisia RFID-tunnisteita voidaan käyttää vastatoimena tuoteväärennöksiä vastaan.

Tämän väitöskirjan tulokset ehdottavat että yksinkertaiset RFID-tunnisteet voivat tehokkaasti suojata toimitusketjuja tuoteväärennöksilta, huolimatta tietystä epävarmuudesta joka aina liittyy tuoteautentikoinnin tuloksiin. Tämä edustaa uutta ajattelutapaa joka painottaa suurta tarkastettavien tuotteiden määrää erittäin luotettavan tuoteatentikoinnin sijasta. Näin käytettynä tekniset vastatoimet voivat tehdä tuoteväärentämisestä taloudellisesti kannattamatonta ja ottaa isomman roolin tuoteäärennöksien vastaisissa strategioissa.

I Introduction

I.1 Product Counterfeiting

In today's global marketplace there is an increasing threat that physical products are not what consumers and end-users think they are. A designer hand bag, a branded MP3 player, a box of chocolate or a bottle of cholesterol medicine might all turn out to be inexpensive knock-offs which only imitate the looks and functional quality of the original products. These are examples of *product counterfeiting*, unauthorized manufacturing of articles which mimic certain characteristics of trademarked or branded products. Counterfeit products typically origin from countries like China, United Arab Emirates, Taiwan, and Indonesia, and they enter western markets mostly through commercial traffic (Taxation and Customs Union, 2008). Large volumes of counterfeit products are also sold and consumed in their countries of origin to satisfy the need for less expensive goods. All in all, product counterfeiting is harmful not only for the legally run businesses and their customers, but also to the affected economies as a whole.

Product counterfeiting is not a new phenomenon. According to the World Intellectual Property Organization (WIPO), the history of product counterfeiting dates back more than 2,000 years (WIPO, 2009). After being fueled by globalization in the end of the 20th century, product counterfeiting has relatively recently reached its modern, industrial-scale form; technology, infrastructure, and know-how to manufacture and package even sophisticated products are spread all over the globe, and digital imaging and printing are highly developed and easily accessible. Parallel to this technological development, intangible assets such as intellectual property and brands are accounting for an increasing share of many companies' equity. As a result, product counterfeiting has become a lucrative illegal business across industries and the world has witnessed a boom of counterfeit and pirated products during the last twenty years (Grossman and Shapiro, 1988b; OECD, 1998, 2007; Staake, 2007).

Product counterfeiting can target virtually any kinds of physical products. According to Grossman and Shapiro, "*[c]asual observers are becoming increasingly aware of the presence of fakes and trademark-infringing knockoffs in the markets for a wide variety of products, including not only the traditionally forged, luxury consumer goods such as designer clothing, watches, perfumes, and leather items, but also higher-technology consumer electronic products such as computers and stereo equipment. ... [and also] records and tapes, foods, pharmaceuticals, and an expanding range of industrial goods, including parts for automobiles and airplanes, fertilizers, pesticides, military hardware, and medical devices*". What makes this statement especially important is that it is published already in 1988, more than 20 years ago (Grossman and Shapiro, 1988a). Thus the existence of counterfeit products in virtually all product categories today should not come as a surprise.

The most serious cases of product counterfeiting are those where a substandard counterfeit product is consumed or used unknowingly by a deceived consumer or end-user. These cases are

are referred to as *deceptive* counterfeiting and they can expose the involved consumers and end-users to health, safety, or security risks. Deceptive counterfeiting is especially dangerous when it targets *security-relevant* products such as car or airplane spare parts, food and beverages, and pharmaceuticals. These products need to conform to adequate quality and safety standards, but counterfeit products do not provide such guarantees. For example, counterfeit drugs might have no active ingredients at all, an insufficient or excessive quantity of the active ingredient, or the wrong active ingredients, and are repeatedly responsible for lost lives, especially in the third world countries (Hopkins et al., 2003; Purefoy, 2008).

One way how counterfeiters deceive consumers – and cash in big profits – is by selling counterfeit products to the same distribution channel through which the genuine products are distributed. This channel is denoted as the *licit supply chain* in contrast to the *illicit supply chain*. If a counterfeit product is deceptively sold to a partner of the licit supply chain, an unsuspecting consumer is likely to end up buying this counterfeit product as a genuine article. Though the majority of counterfeit products never enter licit supply chains, those that do have the most severe consequences. Furthermore, the economics of injecting counterfeit products to licit supply chains make it an especially lucrative business for counterfeiters: first, by exploiting licit supply chains counterfeiters do not need to invest in their own distribution channels which is expensive and tedious, and second, by selling counterfeit products as genuine goods counterfeiters can generate higher profits. An example from the pharmaceutical industry illustrates how counterfeit products can enter licit supply chains even in well-regulated markets.

In 2003, counterfeit Lipitor, the world's top selling prescription drug that reduces cholesterol, was found in 15 US states inside the licit supply chain (Pfizer, 2007). A US-based medical distributor company illegally imported counterfeit Lipitor, produced in Central-America, together with illegally diverted original Lipitor, destined to be sold outside the US. The counterfeit and illegally diverted tablets were co-mingled and repackaged by another company, passed through shell companies to create false pedigrees, and finally distributed to the pharmaceutical supply chain (Department of Justice, 2006; Kansas City Business Journal, 2005). Since the counterfeit tablets were visually virtually indistinguishable from the authentic tablets and had proper packaging and falsified pedigrees, they could flow unnoticed in the licit supply chain. The counterfeiters first come to light several months later when Lipitor's manufacturer Pfizer received patient complaints about the taste of the counterfeit tablets. The Food and Drug Administration's (FDA) forensic chemistry center tested the counterfeit drugs and found out that the tested tablets did contain Lipitor's active ingredient but the effectiveness of the counterfeit tables was not proved and they were unlikely to help lower cholesterol (FDA, 2003b). The case resulted into the largest recall of counterfeit medicines to date in the US constituting a total of about 200,000 bottles of Lipitor in six batches, worth approximately $40 million (FDA, 2003a).

The risk of product counterfeiting has forced industries and governments to invest in countermeasures. Many associations launch public initiatives to fight product counterfeiting on industrial, national, and global levels. Among others, such associations include Organisation for Economic Co-operation and Development[1], International Anti Counterfeiting Coalition[2], Business Action to Stop Counterfeiting and Piracy[3], Coalition Against Counterfeiting and Piracy[4], and United Nations Interregional Crime and Justice Research Institute[5].

Brand owners also want to take measures against product counterfeiting on their own. While some brand owners have a zero tolerance regarding counterfeiting and piracy others engage in countermeasures in case by case basis by evaluating the costs and benefits of different courses of action. In some cases brand owners are even forced to take measures due to external pressure. For instance, a biotechnology company was sued in 2001 on behalf of patients who were sold counterfeit version of one of its products from reputable pharmacies in California. As a result, the affected company was pushed to add holograms to help authenticate its products and the case was resolved outside the court for an undisclosed amount (Hopkins et al., 2003, p. 70).

Brand owners have different anti-counterfeiting approaches in their arsenal. These approaches are summarized in Fig. I-1 and they include consumer information and education, legal actions, private investigations and cooperation with enforcement agencies, and technical countermeasures. The goal of consumer education is to decrease the demand for counterfeit products and increase the awareness of negative effects of counterfeiting. This measure is blunt and somewhat inefficient and mostly adopted by associations and governments instead of single brand owners. The goal of legal actions is to prosecute and punish counterfeiters and confiscate their illegally-financed assets. The downside of legal actions is that they might not scale to solve the problem because most counterfeit players cannot be detected and prosecuted. Furthermore, even if detected, counterfeit players are not always prosecuted due to lacking law enforcement in their countries of origin, and the fines due to illicit trade can be small compared to the illegal profits. Therefore legal actions are mostly seen as a basic prerequisite for brand protection instead of the final measure (Staake and Fleisch, 2008). The goal of private investigations and collaboration with enforcement agencies, such as customs, is to support seizures of counterfeit products and detection and prosecution of counterfeiters. And last, the goal of technical measures is to help brand owners prove the origins of suspicious goods, protect the licit supply chain, and detect counterfeit products in the illicit supply chain. Technical measures are particularly important since they can prevent product counterfeiting in a tangible way.

This thesis seeks to provide a contribution for anti-counterfeiting by researching countermeasures based on radio frequency identification (RFID) technology. RFID is an emerging automatic identification (Auto-ID) technology based on small and inexpensive electronic transpon-

[1] OECD (2009). http://www.oecd.org/sti/counterfeiting

[2] IACC (2009). http://www.iacc.org

[3] BASCAP (2009). http://www.iccwbo.org/bascap

[4] CACP (2009). http://www.thetruecosts.org

[5] UNICRI (2009). http://counterfeiting.unicri.it/resources.php

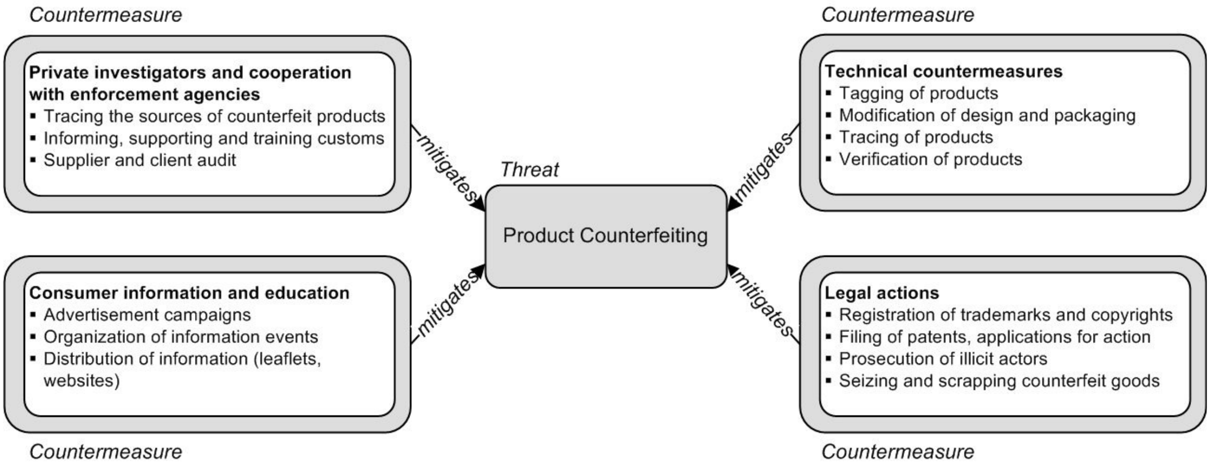

Countermeasure
Private investigators and cooperation with enforcement agencies
▪ Tracing the sources of counterfeit products
▪ Informing, supporting and training customs
▪ Supplier and client audit
Countermeasure
Technical countermeasures
▪ Tagging of products
▪ Modification of design and packaging
▪ Tracing of products
▪ Verification of products
mitigates
Threat
Product Counterfeiting
mitigates
mitigates
mitigates
Consumer information and education
▪ Advertisement campaigns
▪ Organization of information events
▪ Distribution of information (leaflets, websites)
Legal actions
▪ Registration of trademarks and copyrights
▪ Filing of patents, applications for action
▪ Prosecution of illicit actors
▪ Seizing and scrapping counterfeit goods
Countermeasure
Countermeasure

Figure I-1: *Summary of approaches to fight product counterfeiting*

ders, or tags, that are attached to physical products. The biggest benefits of RFID compared to older Auto-ID technologies such as barcodes is its ability to identify multiple products at once and without a line of sight. Furthermore, RFID tags have microchips and digital memory which enable ”smart” functionalities like access control to a tag’s memory. Having a broad set of possible usage scenarios, RFID represents a ”platform technology” that is not destined to any single application, though many of the currently envisioned usage scenarios deal with supply chain management and logistics. The industrial and societal benefits of RFID technology are under research in several research programs and both public and industrial projects; for instance, European Union has a cluster of 30 RFID projects[6]. In that context, anti-counterfeiting is only one application where RFID can be applied.

This section continues by sharpening the arguments for further research on RFID in anti-counterfeiting. These arguments constitute the practical motivation behind this thesis.

I.2 Motivation for Research

The previous subsection already scratched the surface applying RFID technology in anti-counterfeiting. This subsection details the motivation behind this thesis by formulating five high-level arguments for further research in this area. The overall research question will be derived in subsection I.3 based on this motivation.

I.2.1 Negative Effects of Product Counterfeiting

The first argument for further research on anti-counterfeiting is that product counterfeiting is all in all a harmful practice. Various reports and scholarly publications discuss the negative

[6] Cluster of European RFID Projects (2009). http://www.rfid-in-action.eu/cerp

effects of product counterfeiting on brand and trademark owners, consumers, and the affected economies as a whole (OECD, 1998; Staake, 2007; OECD, 2007; Harper et al., 2006). Though industry-funded reports that discuss the matter have a tendency to exaggerate and dramatize these effects in order to lobby for stronger measures against illicit trade, the following five negative effects of product counterfeiting are generally agreed upon.

First, in the case of deceptive counterfeiting, consumers and end-users can get substandard or dangerous products which can be harmful for them (Harper et al., 2006) and decrease the perceived quality of the brand and thus the brand value (Staake, 2007). Second, counterfeit products substitute genuine products leading to direct losses of revenues for the brand owner. Staake (2007) argues that not only the deceptive counterfeit products but also the non-deceptive counterfeit products that are often sold for a lower price lead to substitution. Third, counterfeiting can increase the number of liability claims for the brand owner, including complaints and warranty repairs and possible law suits because of incidents caused by fake products (Hopkins et al., 2003, p. 239). Fourth, counterfeiting can lead to increased expenditures for brand owners since they need to invest in brand protection and related activities, including private investigations, legal measures, collaboration with enforcement agencies, and product recalls.

The fifth negative effect of counterfeiting affects economies as a whole; counterfeiting decreases the returns on investments in marketing, design, research, and development, discouraging returns from innovativeness (OECD, 1998, 2007). Innovation contributes to economic growth (e.g. Cameron, 1998) and by reducing the returns from innovation, counterfeiting reduces the incentive to innovate which leading to reduced economic growth. Moreover, counterfeiters avoid paying taxes and duties and they are not model employers employers.

In order to be objective one needs to recognize that product counterfeiting can also have positive effects on brand owners and consumers. Certain brand owners tolerate the problem since counterfeit products increase the visibility of their brand. In reality, however, this might as well be an argument to justify a passive anti-counterfeiting strategy. One can also argue that counterfeiting increases the availability of cheaper products which benefits consumers (Grossman and Shapiro, 1988a), though this benefit is shortsighted since it dissolves the returns of innovative companies. As a conclusion, the positive effects of product counterfeiting remain small at best and are by far outweighed by the negative effects.

⇒ ***Product counterfeiting harms brand owners, consumers, and affected economies.***

I.2.2 Extent of Product Counterfeiting

Product counterfeiting is not just a marginal phenomenon. Rather, counterfeiters are well organized, work in an industrial scale and make use of modern manufacturing technologies and complex distribution systems (Staake, 2007). Furthermore, contrary to outdated believes, counterfeiting is not restricted to luxury goods but it affects manufacturers of practically all kinds of branded and trademarked products already since 20 years (Grossman and Shapiro, 1988a;

Bush et al., 1989). The large extent of counterfeiting constitutes the second argument for future research on anti-counterfeiting.

Single examples illustrate the extent of the problem. For instance, German customs secured 117 containers of counterfeit and pirate products in the Hamburg port between August and November 2006, constituting probably the world's largest counterfeit seizure to date. The infringing goods included more than one million pairs of counterfeit Nike, Adidas, and Puma sports shoes, counterfeit toys, and over 100,000 counterfeit textiles, with a corresponding overall original retail value of over 383 million euros (Zoll, 2006). Similarly in the U.S., federal officials seized $200 million in fake goods in December 2007 discovering a scheme that involved more than 100 containers of counterfeit products imported to the Port of Newark, New Jersey (United States Attorney, 2007). The infringing goods included apparel and luxury good brands such as Nike, Burberry, Chanel, and Polo Ralph Lauren.

Enforcement statistics constitute a reliable data source for product counterfeiting. European customs seize millions of infringing goods every year. In 2008 the number of seized counterfeit and pirated goods by European customs reached all time high of 178 million articles, a significant increase from 25 million articles in 1999 (cf. Fig. I-2). During the same period the number of opened customs cases involving counterfeiting or piracy grew tenfold from about 4,700 to 49,000 cases per year. Cigarettes, DVDs/CDs and clothing continue to be infringing intellectual property rights in large quantities and there has been a worrying increase in sectors that are potentially dangerous to consumers including pharmaceuticals, electrical equipment, and personal care products (Taxation and Customs Union, 2008). Though part of the increase in seizures can be explained by broadening of the European borders by ten new member states in 2004 and two in 2008, the trend is clear: the extent of product counterfeiting is expanding[7].

The overall extent of product counterfeiting cannot be directly measured because the problem is opaque but there have been serious attempts to measure it indirectly. Staake (2007) presents detailed macroeconomic calculations based on customs seizure statistics suggesting that counterfeit consumption amounts to 0.36% of the merchandize imports of the EU-25 market. On the global level, Staake further estimates that 2% of the world's GDP appears to be an upper boundary of the extent estimates. OECD estimats that counterfeit and pirated items which are traded internationally account for about 2.4% (USD 176 billion) of world trade in manufactures, i.e. imports or exports (OECD, 2007). This analysis is based on an examination of the degree to which different counterfeit or pirated products are detected in international trade and the extent in which different economies are detected as sources. This estimate considers only international trade, so it does not include the large volumes of counterfeit and pirated goods produced and consumed within economies.

Though these estimates provide only rough numbers and they would greatly benefit from more

[7] Sometimes reported average growth rates can be misleading since they are sensible to the chosen time period. Trend analysis provides more objective findings, for instance a linear curve $y = a \cdot x + b$ fitted to the 1999-2008 data using the least squares method yields a 9.8 million annual growth rate (a) with a 39 million y-intercept (b)

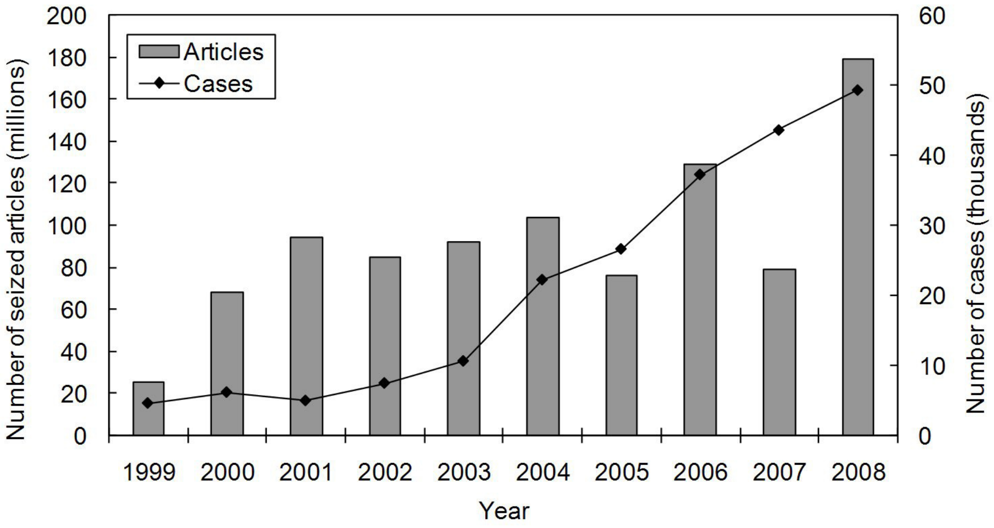


Figure I-2: *The number of counterfeit articles seized and the number of counterfeiting cases investigated by the European customs (Taxation and Customs Union, 2008)*

precise data, such as precise estimates of the ratio of inspected products by customs, they demonstrate that product counterfeiting is a large industrial-scale problem.

⇒ ***Product counterfeiting is a large and growing problem.***

I.2.3 Shortcomings of Existing Technical Countermeasures

The two previous subsections establish the general motivation for anti-counterfeiting activities by demonstrating the extent and negative effects of the problem. This subsection establishes the need for further research on technical anti-counterfeiting measures by pointing out shortcomings in existing approaches.

Technical anti-counterfeiting measures enable brand owners and licit supply chain partners verify the authenticity of physical products. Various technologies are currently applied as technical countermeasures against product counterfeiting including security papers, watermarks, security threads, holograms, microprinting, and security inks (cf. subsection II.5 for more examples). An important motivation behind research about RFID in anti-counterfeiting is that the existing technical anti-counterfeiting measures have shortcomings; despite the abundance of commercially available product authentication techniques, product counterfeiting is still a growing problem and brand owners have a constant need for new security features.

One part of the problem is that secure and easy authentication of physical products is still a technical challenge and as a result there are no standard solutions based on a single technology platform. The problem can be illustrated with banknotes that require a very high level of

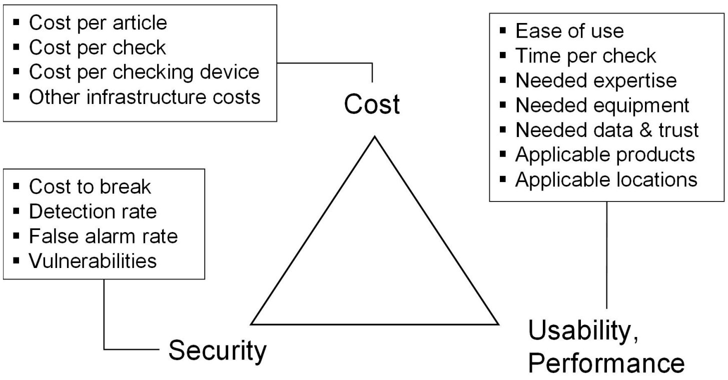


Figure I-3: *Major tradeoffs in technical anti-counterfeiting measures*

security against counterfeiting. For example the 50 Euro banknotes[8] have ten different publicly disclosed security features (plus an unknown number of undisclosed ones). The disclosed security features include, for instance, a hologram patch, a watermark, microprinting, and ultraviolet ink. Since some of these features can become substantially easier to counterfeit over time as printing technologies develop or new materials become available, multiple features are needed to provide security in the long term. This diversified solution approach tries to maximize the level of security, but it is otherwise hardly an optimal one; in order to authenticate a 50 Euro banknote, knowledge and devices to check all security features is needed.

An optimal product authentication feature would be very secure, not expensive, and easily verifiable. But security never comes for free and thus a product authentication system always need to balance between the cost, level of security, and performance & usability of the solution (cf. Fig. I-3). These fundamental tradeoffs are present in all security applications (e.g. Schneier, 2003; Eisenbarth et al., 2007). Indeed, Hopkins et al. (2003, p. 258) argue that machine-readable authentication features (high usability) fail in practice because of the high cost of the feature and the reader, high complexity of reader control and distribution, and because the system can be compromised if readers get in wrong hands.

The shortcomings and benefits of existing product authentication techniques are studied in an EU-funded project SToP (Lehtonen et al., 2008). This evaluation is based on a comprehensive review of both Auto-ID and non Auto-ID based product authentication techniques and it considered cost, security, and usability & performance aspects of the evaluated techniques. The results of this evaluation confirm the difficulty of finding a good balance between the major tradeoffs of security applications. One identified problem with the existing approaches is that even if a product authentication technique provides an adequate level of security, there are many more requirements that need to be fulfilled by a product authentication technique to be an effective anti-counterfeiting tool in a supply chain environment. Most importantly, these requirements include a low cost and effort to check a product and a low response time.

[8] European Central Bank (2008). http://www.ecb.int/euro/banknotes/security/html/index.en.html

Table I-1: *Shortcomings and benefits of existing technical anti-counterfeiting measures*

	Shortcomings	Benefits
Cost	• Dedicated checking equipment required • Single or few hardware vendors • Cost of multiple checks (no bulk checking)	• Possibly very low cost to secure one product • Possibly short time to check one product
Security	• Lack of measures based on detection of copied articles / copied security features • Features tend to become easier and cheaper to copy with advances of technology	• There are very secure ways that rely on unique features of individual articles • Only few requirements for network security (sometimes public key infrastructure) • Very little or no privacy problems
Usability & Performance	• Lack of ways to authenticate pharmaceutical dosage forms themselves (and not the packaging) • Lack of platform solutions and interoperability standards that work for various products • Some techniques (e.g. forensics) have a long check time	• Only somewhat low level of trust (disclosure of confidential information) needed • Secure authentication is possible after product leaves the protected channel • Also non-experts can verify products

The majority of available technical countermeasures are based on preventing imitation of products with hard-to-copy features, but there are also few commercial solutions based on serialization and detection of duplicated serial numbers. Several ways of putting hard-to-copy features on different kinds of products have been developed, most of which require proprietary verification devices. Those existing techniques that are considered highly secure today, such as forensic analysis of a product's natural or artificial features (e.g. microscopic taggants), or the use of sophisticated security labels that have special physical properties, often fail regarding these other requirements; the check can bee time-consuming since it requires laboratory experiments, the check can be done only with special equipment, the check can be performed by a trained expert only, or the technique can be applied only to certain kinds of products. The last of these shortcomings is specially problematic for companies who need to protect different kinds of products since it can mean that different verification devices are needed.

Table I-1 summarizes the shortcomings and benefits of existing non Auto-ID based technical anti-counterfeiting measures. The general shortcomings of the existing measures are that the features can become easier to forge with advances of technology (today a hologram printing machine costs less than $10,000[9]), a lack of platform solutions that can authenticate different kinds of products, a need for dedicated checking equipment and single hardware vendors, and a relative high cost to perform multiple checks. The general benefits of existing approaches are possibly very high resistance to copying (i.e. high cost-to-break, cf. subsection III.2), short time to check one product (except for forensic analysis), and that the security features can be used always during the product's life cycle. These approaches have typically no privacy concerns and pose only few requirements for information security. Last, with approaches based on products' unique natural features, the variable cost to secure one product is very low.

⇒ ***Existing technical anti-counterfeiting measures have shortcomings.***

[9] Wired magazine (2007). http://www.wired.com/science/discoveries/news/2007/02/72664?currentPage=all

I.2.4 Emergence of RFID Technology

This subsection sharpens the argument for focusing on RFID technology in the research on novel technical anti-counterfeiting measures.

RFID is currently being adopted as a new Auto-ID technology in various industries. It has especially strong advocates in the consumer goods and retail industry where many potential benefits are asserted including improved availability of goods on shelves, decreased stock levels and improved lead times, automatic and more accurate inventory, decreased shrinkage, increased security, and greater visibility in general (Kärkkäinen, 2003; Jones et al., 2005; Leimeister et al., 2007). Overall, adoption and diffusion of RFID is the most strongly driven by the following industries: consumer goods and retail, aviation, pharmaceutical and health care, automotive, logistics and transport, apparel, as well as consumer electronics and high-tech.

The value of the RFID market in 2008 (including tags, readers and software/services for RFID cards, labels in all form factors) was approximately 5.3 billion USD with about 2 billion tags sold worldwide (IDTechEx, 2009b; ABI Research, 2008). Most of the deployed tags are low-cost devices whose only function is to store a unique ID number of the tagged object. As the prices of RFID tags continue to decline and item-level tagging becomes more common, the number of sold tags will continue to grow year by year. Against this background it is not surprising that numerous RFID market studies published by market research institutes, industry associations, standardization organizations, and technology providers promote high growth rates for RFID within the above listed industries (e.g. Bovenschulte et al., 2007; BRIDGE, 2007). Many of the past studies and predictions, however, have been overly optimistic owing to an ”RFID-hype” around the technology, and the experienced adoption rates have been smaller than many of the predictions. Schmitt (2008, p. 2) reviewed statements of actual RFID adoption rates that exclude this bias finding adoption rates of 7% and more within the identified industries. Even despite the economic downturn, the RFID market is estimated to grow 5% in 2009, the most active application domains being logistics & retail, financial, security and safety, passanger transport and automotive, and healthcare (IDTechEx, 2009a).

So far mandates have been an important driving force behind RFID adoption in pallet and case levels. In June 2003, Wal-Mart, the world’s larges retailer, announced that their top 100 suppliers would be required to use RFID tags on their cases and pallets by 2005. Only little later the mandate was rolled out with all suppliers (RFID Journal, 2003). In October 2003, the U.S. Department of Defense (DoD) announced that its 43,000 suppliers will be required to use RFID tags on pallets and cases, as well as on single items costing $5,000 or more, delivered to the DoD beginning 2005 (Collins, 2004). In addition to cases and pallets, RFID tags are also appearing on single items. Gap Inc., a multinational apparel producer, was among the first companies to use RFID in a retail supply chain in item-level with their three-month pilot in 2001 (Texas Instruments, 2001). More recently, significant advances in item-level RFID in the retail supply chain has been made by players such as Marks & Spencer, Gillette, Tesco, and Metro (Gaukler et al., 2007).

The general benefits of RFID technology in the identified industries include asset management and tracking of products, security, inventory management and availability, decrease of manual errors, and customer-oriented usage. Increased security against counterfeit products is only one of the many potential benefits that RFID can provide to a supply chain and the technology will be deployed in many cases anyway due to its other benefits. On the one hand, this is a cost advantage since only a part of the infrastructure cost needs to be justified by the anti-counterfeiting business case. On the other hand, this opens a new technology platform that can be used to develop novel technical anti-counterfeiting measures.

⇒ ***Many products will be tagged with low-cost RFID anyway.***

I.2.5 Practical Problems of Brand Owners

For a potential end-user company, investment in a technical measure against product counterfeiting can be considered an investment in security; the countermeasures are applied to secure the company and its distribution channels, consumers, and intellectual property against product counterfeiting. Moreover, these countermeasures are a part of a war of escalation where both the licit and illicit players react to each other's moves by applying improved techniques, methods, and strategies. To be able to make rational and well-judged decisions in this war of escalation, end-user companies need to know the real risks that counterfeit products pose to them and how different countermeasures mitigate these risks. Limited knowledge of the risks and countermeasures can lead to bad decisions—excessive investments in security where the same effect could be achieved much more economically, or creation of a feeling of security that does not provide real protection.

Today brand owner companies lack the knowledge and tools to evaluate the benefits of RFID in anti-counterfeiting. For instance, most RFID-based product authentication approaches exist today only as concepts or proposals within the scientific community and only basic RFID-based product authentication approaches are currently employed in practice. In particular, brand owners' own experience with product authentication is mostly limited to prevention-based, hard-to-copy features and therefore the potential of measures that detect cloned tags (cf. subsection II.5.4) is not well understood. To be able to evaluate how RFID can contribute in brand protection, brand owners need a better understanding of RFID as an anti-counterfeiting technology.

In addition to the problems that are present in every RFID deployment project, such as the choice of frequency range, tags and tagged objects, as well as integration of reader devices and business process changes, the specific challenge of an anti-counterfeiting deployment is how security can be engineered into the RFID system. While various RFID implementation guidelines and checklists are published by practitioners[10,11], they do not cover the use of RFID

[10] Cluster of European RFID Projects (2009). http://www.rfid-in-action.eu/public/results/guidelines/rfid-implementation-checklist

[11] Intermec 2009). http://epsfiles.intermec.com/eps_files/eps_brochure/RFIDChecklist_brochure_web.pdf

in anti-counterfeiting. In particular, brand owners have a limited knowledge of the level of security that different RFID-based security measures provide. Knowing the level of security is important because this is primarily what the brand owners are paying for in anti-counterfeiting. However, evaluation and comparison of the level of security is difficult since each security measure has a certain *intrinsic level of security*, but the level of security of a working system is ultimately defined by the practice (Bishop, 2003). In other words, also usability and performance need to be considered. As a result, most brand owners lack the expertise to evaluate the protection provided by RFID-based anti-counterfeiting measures.

A big part of the uncertainty that characterizes brand owners' views of RFID technology, and the security it provides, stems from the threat of tag cloning. In a *tag cloning attack* an adversary reads the data written on a genuine tag and write it to another tag to create a cloned tag (cf. Fig. I-4). Unprotected RFID tags[12] are vulnerable to tag cloning attacks and for example EPC Class-1 Gen-2 tags provide only limited protection against it. Owing to the possibility of reading multiple tags at once from distance and without line of sight, tag cloning attack is furthermore highly scalable. It can be assumed that counterfeiters can obtain large numbers of valid serial numbers written on genuine tags by scanning large numbers of genuine products in retail shelves, warehouses, trucks etc, if they need to do so. Furthermore, if the serial numbers are assigned consecutively instead of a randomized way, counterfeiters can also easily guess large quantities of valid serial numbers. As a result, critics do not consider RFID suitable for secure product authentication and anti-counterfeiting (Scalet, 2007).

The research community addresses tag cloning attack primarily with cryptographic authentication protocols that prevent adversaries from producing perfect clones of RFID tags (Juels, 2006); while an adversary can obtain a tag's serial ID number (here: the object's serial number such as an EPC, cf. subsection IV.1) relatively easily, obtaining a secret key stored inside a tag is considerably harder since the tag never transmits the secret key in clear text form.

The challenges in implementing cryptographic authentication protocols on RFID tags revolve around the trade-offs between tag cost, level of security, and performance in terms of reading speed and distance (cf. Fig. I-3): it is not very hard to protect an RF device from copying with an unlimited chip size and power budget, but it is challenging when the device is a passive barcode-replacing low-cost RFID tag. These tags will be deployed in numbers of several millions and end-user companies have a strong financial incentive to minimize their cost.

Though the research community always provides improvements to the aforementioned trade-offs, advances in technology benefit crackers as well by decreasing the price of computation power, for instance. Indeed, a series of severe attacks against proprietary ciphers of commercial RFID devices between 2005 and 2008, namely SpeedPass^{TM} (Bono et al., 2005), MiFare^{TM} Classic (Courtois et al., 2008), and Keeloq^{TM} (Bogdanov, 2007), demonstrated the risks of insufficient protection and evoked the need for strong standard cryptography. As a result, the RFID security community is more and more focused on providing security through lightweight

[12] E.g. tags where all memory fields can be read and written without restrictions

implementations of state-of-the-art ciphers, instead of inventing new ciphers.

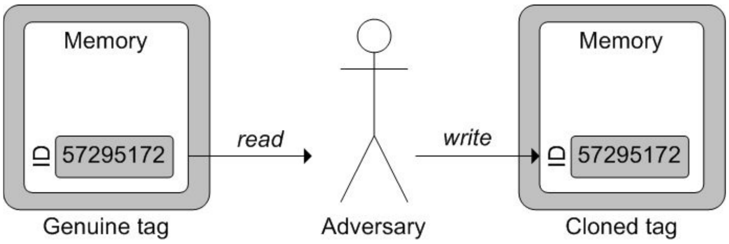


Figure I-4: *Tag cloning attack*

Passive tags that support for cryptographic tag authentication protocols (*crypto tags*) exist in the HF frequency band (e.g. MiFare$^{\text{TM}}$ DESFire EV1[13]), and are planned in the Microwave frequency band (HP's Memory Spot chip[14]), but such tags are not yet commercially available in the UHF frequency band that is often used in logistic applications. This has been recognized in research programs; for example, researchers in the University of Graz, Austria, have demonstrated standard cryptography on silicon in a way that complies with the rigid energy consumption requirements of passive UHF tags (cf. subsection III), and the National Science Foundation has started funding a project to develop a secure passive RFID tag to secure the multi-billion dollar U.S. pharmaceutical supply chain (RFID Ready, 2009).

However, cryptographic units will increase the tag price. Furthermore, if an RFID tag needs to store a secret key, the tag needs to be protected against side-channel attacks and physical attacks (Weingart, 2000)—a task that has increased the cost and complexity of smart cards. These are reasons to believe that passive low-cost RFID tags cannot be protected against cloning using cryptographic authentication protocols in the near future *without* increasing the tag's cost or decreasing the tag's performance in terms of read time and range. As a result, cryptography will not solve the authentication problem for the most inexpensive tags that will be deployed anyway for their business value in other applications than anti-counterfeiting.

Moreover, misconceptions about security in product authentication perplex the evaluation of RFID-based anti-counterfeiting measures. The first misconception is that a product can be considered genuine if it can provide an uninterrupted trace that goes back to a legitimate manufacturer (e.g. GS1 Germany, 2006). This method is not secure per se since it does not establish the link between the product and its history, i.e. a proof that the product under study generated the presented events. The corresponding threat is copying the history of a genuine product to go along with a sold counterfeit product. The second misconception deals with the serialized transponder ID (TID) numbers – unique hardware numbers of RFID tags. Since a TID number is protected from rewriting, the argument goes, a tag is genuine if it has the right TID number.

Though TID provides a practical hurdle against adversaries who want to produce copied tags,

[13] NXP (2009). http://www.nxp.com/acrobat_download/literature/9397/75016504.pdf

[14] HP (2006). http://www.hp.com/hpinfo/newsroom/press/2006/060717a.html

this scheme does not qualify as secure authentication since it relies on a static identifier unprotected from reading, much like the MAC addresses of network cards. However, the United States Department of Homeland Security (2008) posits in its privacy impact assessment on the passport card that *"...there is a powerful tool that can be used to remove the risk of copying. This tool is the Tag Identifier, or TID. The TID is available on all Gen 2 RFID tags"* (Koscher et al., 2008). But given that all chip manufacturers—existing and new ones—have the power to produce and sell chips with any TID numbers they want, and that it is possible to build a relative simple device that imitates RFID tags including their TID numbers, it is hardly appropriate to call the TID a "*powerful tool [...] to remove the risk of cloning*" (cf. subsection VI.1 for a thorough security analysis of TID numbers in anti-counterfeiting).

As a conclusion, brand owners still lack the knowledge to use RFID as an anti-counterfeiting tool. Much of the lacking knowledge deals with the tag copying attack and how it can be addressed using different security measures, but also more general guidelines are missing. This constitutes the fifth argument for the presented research.

⇒***Brand owners do not know how to use RFID in anti-counterfeiting.***

I.3 Research Question and Methods

The research approach of this thesis is detailed below by presenting the theoretical research gap, the overall research question, and the research methods and projects.

I.3.1 Theoretical Research Gap

The role of theory in information systems research is to explain and predict real-world phenomena such as human and organizational behavior (Hevner et al., 1997); when existing theories cannot explain or predict a real-world phenomenon, there exists a research gap. This subsection underlines a research gap where the-state-of-the-art research does not resolve the aforementioned practical problems of brand owners.

There are various approaches to determine that a product is not what it claims it is, including countless ways to mark or label genuine products so that they can be distinguished from counterfeits. However, no solution is perfectly secure and counterfeiters can learn how the genuine products are marked and try to incorporate the same features on counterfeit articles. This kind of practical thinking and a climate of secrecy have dominated the way how product authentication techniques have been designed in the past. While the focus has been on the war of escalation against counterfeiters, the theoretical basis behind product authentication remain immature. In particular, the existing theory behind authentication does not explain how products can be authenticated by track and trace data.

Moreover, the existing theory about the level of security does not explain the level of protection that different technical solutions provide in practice to a supply chain; first, such a model should combine the intrinsic level of security of preventive approaches (i.e. cost-to-break) with the properties of the detection-based approaches, and the way the solution is used in practice. Second, since the level of security depends on the threat, this model should also take into account the properties of counterfeit products. Only such a comprehensive model would have enough degrees of freedom to capture the overall effect that the product authentication system has on a counterfeiter.

Furthermore, the existing theory does not answer what are the properties of an ideal product authentication solution and how well can they can be reached by low-cost RFID technology. Low-cost RFID tags such as the EPC Class-1 Gen-2 lack the hardware resources to do symmetric or asymmetric encryption on their own (cf. subsection I.3.3), but they will be deployed anyway in large quantities due to their value in other applications. A product authentication solution for low-cost RFID could therefore secure large quantities of products with a small marginal cost.

Based on the aforementioned practical problems of brand owners and the theoretical research gap, the following research question is chosen to provide guidance throughout this thesis:

How can a supply chain be effectively protected against counterfeits using low-cost RFID tags?

The research field of this thesis is a combination of design science, where the goal is to maximize the utility of a system that is being designed, and behavioral science, where the goal is to explain or predict human and organizational behavior (Hevner et al., 1997). This mixture of research paradigms is reflected in the research methods presented below.

I.3.2 Research Methods and Research Projects

The research question of this thesis is approached with a combination of research methods. First, this work is grounded over a thorough literature review of related scholarly contributions and existing product authentication techniques. Based on the state-of-the-art research on related fields of security research, an analysis framework is developed to assist how to model security of technical anti-counterfeiting measures. The goal of this conceptual work is to have a sound foundation for understanding and modeling the effectiveness of technical security measures.

Then a focus is given to the design science in terms of development and evaluation of product authentication techniques for low-cost RFID. Two novel detection-based product authentication techniques are developed for low-cost RFID to complement the state of the art. In addition to the two developed techniques, the level of security of the existing TID-based product authentication scheme is evaluated. Various evaluation methods are employed in this work depending on the nature of the technique under study. These methods include a survey and interviews with RFID chip manufacturers, a real-world based simulator study, analytical modeling combined with quantitative analysis, and prototype building. This mixture of research methods provides a holistic and well-grounded approach to answer the research question.

This work is conducted in the Auto-ID lab of University of St.Gallen/ETH Zurich, close to EU-funded projects SToP (project No. IST-034144) and BRIDGE (project No. IST-033546).

Stop tampering of products (SToP) aims at developing ambient intelligence-based and network-oriented systems for the efficient and secure authentication of products and it includes end user companies from the luxury goods industry, pharmaceutical and life sciences industry, and aerospace industry. The project includes development and trialling of a product verification infrastructure that uses RFID tags as well as barcodes to authenticate different kinds of products in real-world work processes. The project runs from November 2006 to June 2009. (http://www.project-stop.eu)

Building radio frequency identification for the global environment (BRIDGE) addresses ways to resolve the barriers to the implementation of RFID in Europe, based upon GS1 EPCglobal standards. BRIDGE project has one business application work package (WP5) dedicated to development of track and trace based anti-counterfeiting measures. Close work with both end user companies and technology experts in these two projects enables formulation and validation of managerial guidelines based on the findings of this work. The project runs from July 2006 to June 2009. (http://www.bridge-project.eu)

I.3.3 Assumptions and Limitations

This subsection lists the assumptions behind this work and the resulting conceptual limitations of the research approach. Making assumptions explicit is important since the topic of this work is closely related to security engineering. The presented assumptions also serve as definitions of commonly used terms.

1. *Licit supply chain:* The subject of the researched countermeasures is a licit supply chain that is affected by product counterfeiting. The licit supply chain includes multiple companies, or *players*, who have lawful intents and do not intend to trade with counterfeit products. However, all inputs of this supply chain are not secured and thus it is possible that counterfeit products are sold as genuine products to a player in the licit supply chain from the illicit supply chain. The assumed supply chain is furthermore industry agnostic and represents, for instance, fast moving consumer goods industry, apparel industry, pharmaceutical and life sciences industry, and luxury goods industry.

2. *Illicit supply chain*[15]*:* Parallel to the licit supply chain, there exists an illicit supply chain

[15] The notions of licit and illicit supply chain have first been formalized by Staake (2007)

which produces and delivers counterfeit products. Illicit and licit supply chains coexist and illicit supply chain partners seek to infiltrate the licit supply chain with counterfeit products. Malicious intents of illicit players are not known to the licit players so they do not know when they are dealing with companies who sell counterfeit products. Also the illicit supply chain has consumers or end-users creating a demand for fakes. This means that both deceptive and non-deceptive cases of counterfeiting occur.

3. *RFID infrastructure:* The licit supply chain has an RFID infrastructure that enables (partial) tracking and tracing of logistic units, including single products, and the tagged logistic units have unique identifiers. Not all supply chain players capture and share the track and trace data such that the provided visibility is not complete. Also read errors (missing reads) are possible. Furthermore, it is assumed that RFID tags are applied on item level at least for some products for the mere comfort of being able to speak of product authentication (instead of pallet or case authentication), though the investigated security measures apply to authentication of aggregated logistic units as well. Last, the infrastructure is used to enable multiple business applications in the field of logistics and supply chain management, anti-counterfeiting being only one of them.

4. *Low-cost RFID tags:* The employed RFID tags are low-cost tags such as EPC Class-1 Gen-2 (EPCglobal Inc., 2005a). These are inexpensive (ca. \$0.10 in large volumes (Carrender, 2009)), provide only basic functionalities (e.g. 96-bit identifier, password-protected memory access, 16-bit pseudo random number generator), and are expected to be employed in large volumes for tracking of physical objects.

5. *Willingness to check products:* At least some partners of the licit supply chain are willing to check products to detect counterfeit articles. This assumption is made explicit since the use of technical countermeasures is limited to scenarios where this willingness exists.

Owing to the above mentioned assumptions, this work is not explicitly focused on solving the problem of counterfeiting in the aerospace industry where the problem affects the maintenance, repair and overhaul (MRO) process of airplane spare parts. The MRO process is not the supply chain which manufactures and delivers the airplane parts but the process where these parts are used. This, however, is only a minor limitation since the developed supply chain-focused anti-counterfeiting concepts can be applied also to the MRO process with minor modifications.

This work also does not focus on security issues of RFID back-end systems such as how authenticity and integrity of an EPCIS can be provided. The back-end security requirements of the investigated techniques are made explicit throughout the thesis but how they can be provided falls out of the scope of this work.

I.4 Organization of This Work

The rest of this work is organized as follows.

Section II equips the reader with background information about the role of intellectual property rights in the modern economy, different dimensions of illicit trade, RFID technology, basic concepts behind security engineering and cryptography, as well as existing product authentication techniques. This section also defines most of the terminology that will be used throughout this thesis.

Section III reviews related work in the fields of managerial research on anti-counterfeiting strategies, level of security, economics of security, and RFID security. A broad view to these relating research fields is provided and the most important contributions are summarized in the end of each subsection.

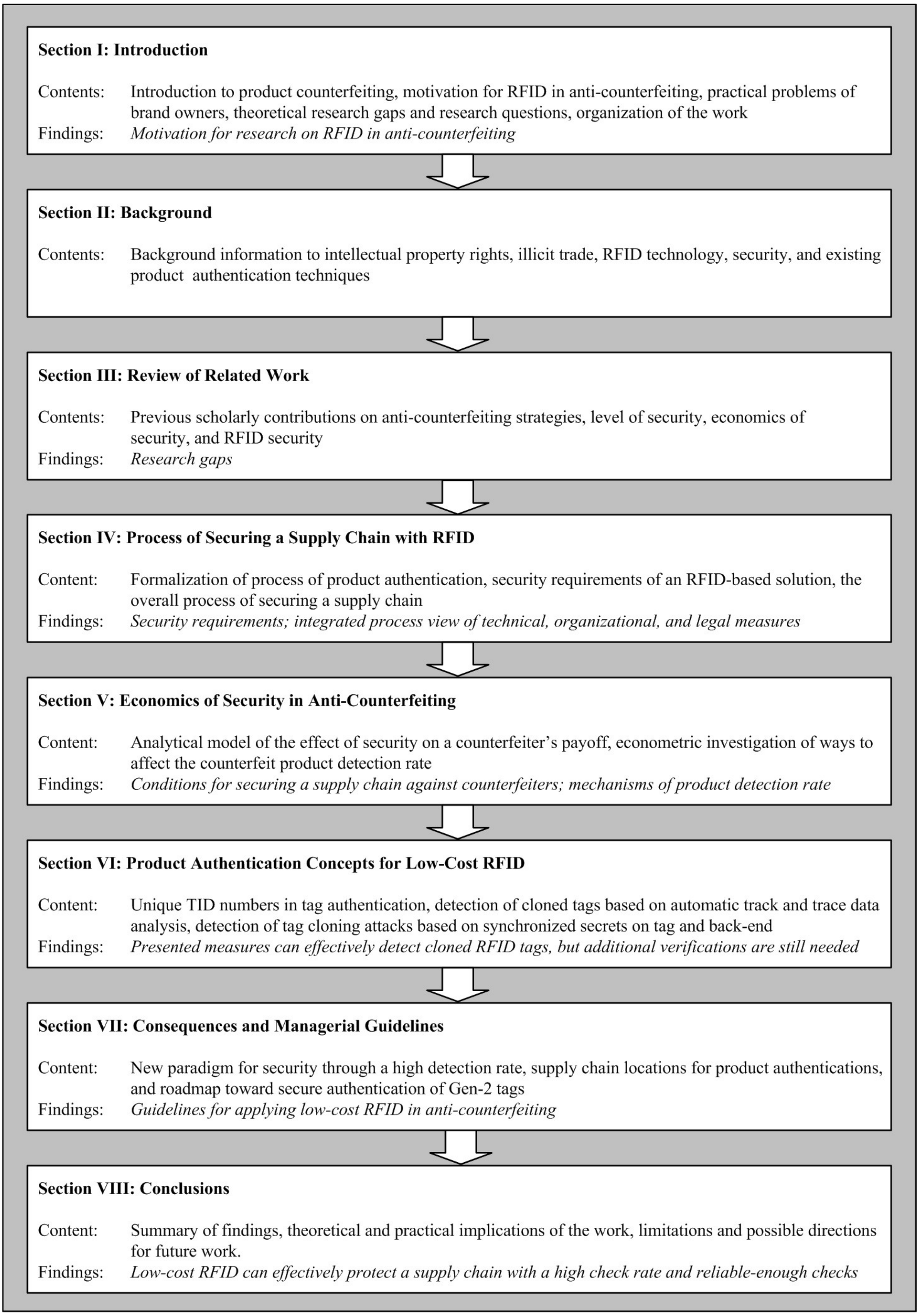
Section IV synthesizes the state-of-the-art research on security and anti-counterfeiting strategies to create a systematic view of security in anti-counterfeiting. This includes description of the process of product authentication, security requirements of an RFID-based solution, and the integrated process of technical, organizational, and legal countermeasures to secure a supply chain.

Section V presents an economic investigation about security in anti-counterfeiting by studying how the process of security affects a counterfeiter's payoff and how a brand owner and a counterfeiter can affect the counterfeit product detection rate. Furthermore, the economic conditions of considering a supply chain secure against financially motivated counterfeiters are derived.

Section VI contains the major technical contribution of this thesis by presenting and evaluating novel concepts for securing supply chains by detecting cloned RFID tags and RFID tag cloning attacks. In addition, an analysis of the level of security of unique TID numbers is presented. All the studied techniques can be implemented on standard low-cost RFID tags such as the EPC Class-1 Gen-2. The level of security of the described approaches is analyzed with various methods including expert interviews, a mathematical model, and a real-world based simulation study.

Section VII discusses the managerial consequences of low-cost RFID-based countermeasures. The biggest consequence is presented as a paradigm shift toward more effective use of technical countermeasures. To support brand owners in operationalizing the new paradigm, application guidelines about supply-chain locations for authenticity checks and an implementation road map toward secure authentication of EPC-tagged products are presented.

Section VIII summarizes the most important results of this thesis by presenting how the research question is answered and suggests directions for future research.



Section I: Introduction

Contents: Introduction to product counterfeiting, motivation for RFID in anti-counterfeiting, practical problems of brand owners, theoretical research gaps and research questions, organization of the work

Findings: *Motivation for research on RFID in anti-counterfeiting*

Section II: Background

Contents: Background information to intellectual property rights, illicit trade, RFID technology, security, and existing product authentication techniques

Section III: Review of Related Work

Contents: Previous scholarly contributions on anti-counterfeiting strategies, level of security, economics of security, and RFID security

Findings: *Research gaps*

Section IV: Process of Securing a Supply Chain with RFID

Content: Formalization of process of product authentication, security requirements of an RFID-based solution, the overall process of securing a supply chain

Findings: *Security requirements; integrated process view of technical, organizational, and legal measures*

Section V: Economics of Security in Anti-Counterfeiting

Content: Analytical model of the effect of security on a counterfeiter's payoff, econometric investigation of ways to affect the counterfeit product detection rate

Findings: *Conditions for securing a supply chain against counterfeiters; mechanisms of product detection rate*

Section VI: Product Authentication Concepts for Low-Cost RFID

Content: Unique TID numbers in tag authentication, detection of cloned tags based on automatic track and trace data analysis, detection of tag cloning attacks based on synchronized secrets on tag and back-end

Findings: *Presented measures can effectively detect cloned RFID tags, but additional verifications are still needed*

Section VII: Consequences and Managerial Guidelines

Content: New paradigm for security through a high detection rate, supply chain locations for product authentications, and roadmap toward secure authentication of Gen-2 tags

Findings: *Guidelines for applying low-cost RFID in anti-counterfeiting*

Section VIII: Conclusions

Content: Summary of findings, theoretical and practical implications of the work, limitations and possible directions for future work.

Findings: *Low-cost RFID can effectively protect a supply chain with a high check rate and reliable-enough checks*

Figure I-5: *Organization of this work*

II Background

To provide background information for this work, this section reviews the legal framework behind anti-counterfeiting, provides an introduction to RFID technology and security engineering, and reviews existing technical anti-counterfeiting measures.

II.1 Intellectual Property Rights

Intellectual property rights provide the legal rights to fight product counterfeiting and they help define different dimensions of illicit trade. Therefore they need to be considered before discussing technical anti-counterfeiting measures.

According to the World Intellectual Property Organization (WIPO), intellectual property (IP) refers to *"creations of the mind: inventions, literary and artistic works, and symbols, names, images, and designs used in commerce."*[1]. Intellectual property—ideas and knowledge—is an increasingly important part of trade; most of the value of new medicines, high technology products, films, music recordings, books, software, branded clothes or new varieties of plants lies in the amount of invention, innovation, research, design and testing, or information and creativity involved. Not to mention brands.

Brands constitute a vital instrument how companies communicate the life style, values, and quality of their products to their customers and a great share of many companies equity. World's top brands include large multinational corporations like Coca-Cola, IBM, General Electrics, and Nokia[2]. Though brands and branding are typically associated with modern marketing management, their roots date to ancient history. For instance, Greek and Roman wine bottles bearded impressions to show high quality, and in Middle Ages English bakers were obliged to mark their bread (primarily for liability reasons though) (Kaikati and LaGarce, 1980). Moreover, infringers were severely punished; in 1544 Charles V of France passed a verdict that anyone who put a false mark of authenticity on Flemish tapestry would have his right hand chopped off (Hopkins et al., 2003, p. 242).

Today, intellectual property rights give inventors and authors the right to prevent others from using their intellectual property usually giving the creator an exclusive right over the use of his or her creation for a certain period of time. According to theory, the social and economic role of intellectual property rights is to guarantee return on investments in creative work and to foster economic growth through increased innovation (e.g. Cameron, 1998; Park and Ginarte, 1997). Intellectual property rights come in many flavors, the most important of which being patents, trademarks, copyrights, geographical indications, and industrial designs (cf. Table II-1).[3] These are described below based on (WIPO, 2004).

[1] WIPO (2009). http://www.wipo.int/about-ip/en/

[2] Interbrand (2009). Best Global Brands 2008, http://www.interbrand.com

[3] In addition, IPRs cover layout-designs of integrated circuits and plant variety rights of a new variety of plant

- *Patents* protect inventions as new solutions to technical problems. Merely discovering something that already exists in nature is not an invention but human intervention must be added, as well as industrial applicability and non-obviousness. Patent gives an exclusive right to the invention. In return for the exclusive right, the inventor must adequately disclose the patented invention to the public.

- *Trademarks* are sign which distinguish the goods or services of one enterprise from those of another and they are targeted for consumers. They can use words, letters, numerals, pictures, shapes and colors, or any combination thereof. Some countries even allow for the registration of dimensional signs (e.g. the Coca-Cola bottle), audible signs (e.g. the lion roar that precedes MDM films) or even olfactory signs (e.g. perfume smells). Moreover, trademarks are used to protect brands that are the essence of a competitive economy. They differentiate offerings through innovation which makes them relevant to the consumer.

- *Copyrights* protect results from intellectual activity in the industrial, scientific, literary or artistic fields, such as books, music, paintings, sculptures, and films. They grant authors the exclusive right to authorize public performance, broadcasting and communication of their works to the public. The duration of a copyright provided for by national law spans in general at least 50 years after the author's death.

- *Geographical indications* are signs used on goods that have a specific geographical origin and possess qualities or a reputation that are due to that place of origin. They may be used for a wide variety of agricultural products, such as ”Tuscany” for olive oil produced in a specific area of Italy, or ”Roquefort” for cheese. Geographical indications may also highlight particular product qualities which are due to human factors found in the place of origin of the products, such as specific manufacturing skills and traditions, for example ”Swiss made” for watches.

- *Industrial designs* are ornamental or aesthetic aspect of useful articles considering shape, pattern or color the article. They recognize and protect the visual appeal of products. Industrial designs can generally be protected if they are new or original. The usual maximum duration of an industrial design is from 10 to 25 years, depending on the country.

Today the protection of intellectual property rights in the international trade is governed by the Agreement on Trade-related Aspects of Intellectual Property Rights, TRIPS WTO (1994). TRIPS agreement was negotiated in 1986-94 and they introduced for the first time intellectual property rules into the multilateral trading system. Is establishes minimum levels of protection that each government has to give to the intellectual property of fellow WTO members.

Table II-1: *Summary of intellectual property rights (WIPO, 2004)*

Right	Description	Example subjects
Patent	• Protects inventions, both products and processes • Exclusive rights to the invention generally for 20 years • Regional validity, differences in legislation	Viagra, Paper clip, Light bulb
Trademark	• Protects words, letters, pictures, shapes, colors etc. • Distinguishes goods or services to consumers • No fixed expiry time (re-registration)	Coca-Cola label, Coca-Cola bottle
Copyright	• Protects books, music, paintings, sculptures, films etc. • Exclusive rights to encourage and reward creative work • Valid at least 50 years after the death of the author	Beatles songs, Harry Potter books, MS Office
Geographical indication	• Protects signs indicating specific geographical origin • Highlights qualities, reputation, manufacturing skills, and traditions specific to the place of origin	Swiss made, Roquefort, Habana
Industrial design	• Protects aesthetic aspects, shape, pattern or color • Right to prevent the manufacture, sale or importation of copies of the protected design	Mobile phone, User interface

II.2 Taxonomy of Illicit Trade

For affected companies, product counterfeiting is only one dimension of illicit trade. Therefore a taxonomy of illicit trade helps understand product counterfeiting in a larger context.

Illicit trade is a root term that brackets several trade-related activities that are either illegal or unauthorized by owners of intellectual property rights. The illicitness of these activities derives from breaches of intellectual property rights or other related trade regulations and therefore the taxonomy of illicit trade closely follows that of intellectual property rights. The dimensions of illicit trade are explained below.

- *Product counterfeiting* means production of any goods (i.e. *counterfeit products*), including packaging, bearing without authorization a trademark which is identical to the trademark validly registered in respect of such goods, or which cannot be distinguished in its essential aspects from such a trademark, and which thereby infringes the rights of the owner of the trademark in question under the law of the country of importation (WTO, 1994, Article 51). Thus the definition covers the illicit manufacturing process but excludes other activities such as parallel importing, bootlegging, and trafficking in stolen products.

- *Product piracy* means production of any goods (i.e. *pirated products*) which are copies made without the consent of the right holder or person duly authorized by the right holder in the country of production and which are made directly or indirectly from an article where the making of that copy would have constituted an infringement of a copyright or a related right under the law of the country of importation (WTO, 1994, Article 51).

- *Illegal product diversion* refers to a situation in which products produced genuinely under protection of intellectual property rights and intended for specific markets are ”diverted” for sales in an alternative market where importing these product is illegal. In many cases product diversion is not illegal but happens without the permission of the intellectual property right holder in the receiving country. These not-illegal cases are referred to as ”parallel trading” or ”gray market” (WTO, 2006) and the activity is in general legal and tolerated within the European Union since it represents free flow of goods. The most common reasons for product diversion are higher sales price and lack of authorized retail in the receiving country.

- *Smuggling* refers to illegal exporting or importing of goods. Smuggled goods can themselves be illegal (e.g. drugs or weapons) or they can be subject to illegal evasion of taxes and duties levied on imported goods (e.g. cigarettes and alcohol). In the former case the smuggled goods can also be illegally diverted.

These four dimensions of illegal trade activities sum up to what is referred to as illicit trade. Companies, industries, and economies are affected by illicit trade through different mixtures of these distinct activities. In practice the boundaries of these activities are often blurred and the problems overlap. For instance, a copied music CD can be in the same time both a pirated and a counterfeit product since it infringes both the copyright of the artistic content as well as the registered trademark on the CD cover. In some cases, counterfeit products are co-mingled with illegally diverted genuine products to lower the chances of detection (e.g. Case study Xerox, CACP, 2009).

For a more detailed analysis of illicit trade, in particular product counterfeiting, also other qualities and mechanisms of the problem need to be defined. These help describe the problem in a more detailed level and they are explained below.

- *Factory overrun* refers to cases in which an outsourced manufacturer exceeds the production quantity allowed by the license contract with the right holder and produces additional products without the consent of the right holder. Even though the functional and visual quality of these products can be identical to that of genuine products, the resulting products are legally considered counterfeits since they are produced without the permission of the right holder.

- *Product tampering* refers to manipulation of a product, including its packaging and relating documents, for harmful or illicit purposes.

- *Non-deceptive counterfeiting*, or perceptive counterfeiting, refers to situations in which counterfeit products are consumed or purchased knowingly.

- *Deceptive counterfeiting*, or non-perceptive counterfeiting, refers to situations in which counterfeit products are consumed or purchased unintentionally.
- *High quality fake* refers to a counterfeit product whose quality is close or even identical to that of genuine products so that it is very hard to distinguish from genuine products.
- *Low quality fake* refers to a counterfeit product that is a poor imitation and thus can be easily recognized as a counterfeit.

II.3 Radio Frequency Identification

Radio frequency identification (RFID) is a promising tool for anti-counterfeiting since it allows scanning multiple products without a line of sight and it will be deployed in many cases anyway. This subsection introduces RFID in the context of other Auto-ID technologies.

The term Auto-ID refers to the process of automatic identification of a physical object. Though Auto-ID technologies are mostly used in an industrial or commercial context, they also benefit normal consumers and citizens for example through telephone cards, bank cards, car immobilizers and contactless keys. The most important Auto-ID technologies are introduced below based on Finkenzeller (2006, p. 2) and summarized in Fig. II-1.

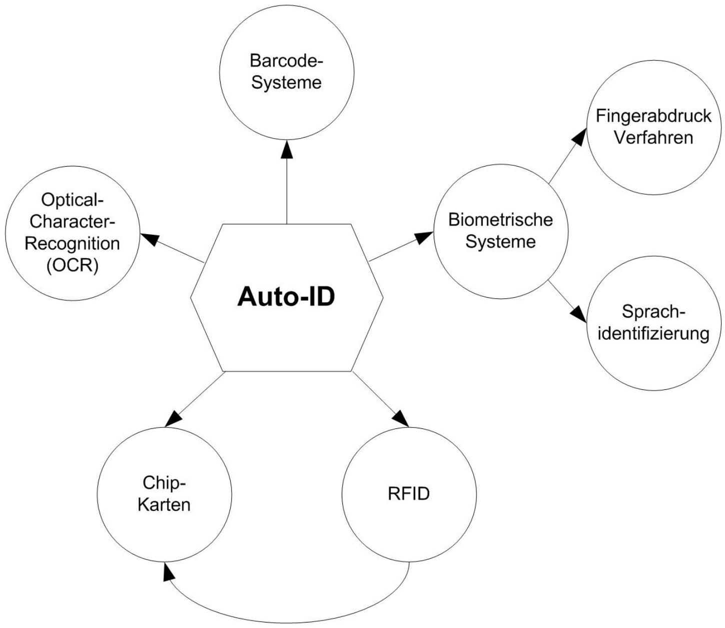


Figure II-1: *Overview of Auto-ID technologies (Finkenzeller, 2006, p. 2)*

The omnipresent barcodes are by far the most common Auto-ID technology today. A typical one-dimensional barcode is a binary code comprising a field of parallel bars and gaps, costs only about one cent or less to print, and it is used to identify virtually any kinds of physical commercial products. The most important barcode standards are the 13-digit European article number (EAN) and the 12-digit universal product code (UPC). UPC was introduced in the USA as early as 1973 and it was followed by the EAN in 1976. Today, the UPC represents a subset of the EAN code and is therefore compatible with it (Finkenzeller, 2006). There are also two-dimensional barcodes that can incorporate a larger amount of data in a matrix form, such as the Data Matrix or the PDF417 barcode. General downsides of barcodes are their relative low storage capacity and the fact that the data cannot be reprogrammed.

Optical character recognition (OCR) is a less frequently used Auto-ID technology. It refers to electronic translation of handwritten, typewritten or printed text. OCR is used for example in various administration tasks to identify paper forms, in postal services, and in banks. Auto-ID also includes biometrics which means identification—and authentication—of people based on fingerprints, voice recognition, and iris scans.

Smart cards are probably the Auto-ID technology most frequently used by consumers and citizens. Smart cards are electronic data storage devices with computing capability (a microprocessor) and they can be found for example in telephone cards and bank cards. Smart cards are often incorporated into plastic cards to give them a practical form factor and they can be protected against unwanted access and manipulation of data. Being based on silicon chips, smart cards provide technically more versatile features compared to barcodes and OCR.

Last, Auto-ID technology family comprises RFID that is a contactless identification technology. Since smart cards can be contactless as well, there is in fact a fine line between smart cards and RFID devices, and in this work wireless smart cards are considered as a subset of RFID devices. Though the history of RFID technology dates all the way back to the Second World War, it is only now finding its place as a ubiquitous Auto-ID technology. RFID is mostly used to track physical objects in logistics and retail, but its possible usage scenarios are versatile spanning from animal tracking to ticketing and mobile payment.

Owing to the way the technology is used, RFID raises often more security and privacy concerns than other Auto-ID technologies. RFID tags are used for example in e-passports (International Civil Aviation Organization, 2006a) to store passenger data, including a biometric feature (e.g. fingerprint or photo). E-passports are designated to facilitate and secure cross-border travel by enabling automated biometric authentication of travelers, but an RFID chip on a passport also raises new security requirements. For instance, these include authenticating the biometric feature, protecting the chip against unwanted access, and authenticating the chip itself.[4] Even though standards exist to address these requirements (International Civil Aviation Organization, 2006b), researchers have demonstrated successful attacks against e-passports due to shortcomings in security concepts and their implementation (cf. subsection III.4).

RFID is also an important enabling technology behind the Internet of Things and sometimes—mistakenly—even used as a synonym for it. The Internet of Things is a vision that combines

[4] E-passports still rely on tens of non-electronic security features to protect them against counterfeiting (International Civil Aviation Organization, 2006a)

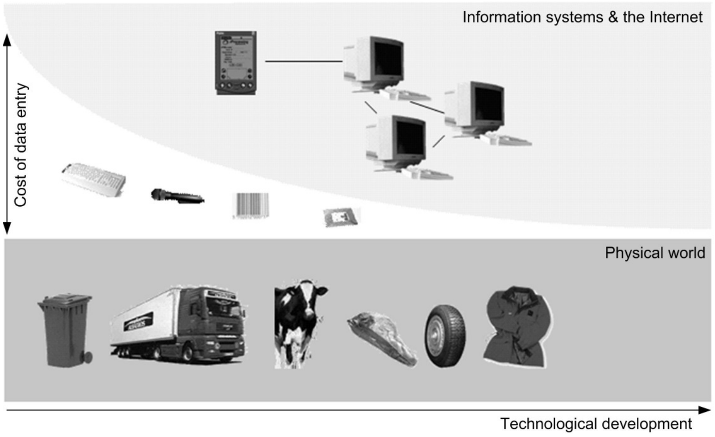


Figure II-2: *Integration of the real world and the virtual world (Fleisch and Mattern, 2005)*

identification, sensing, localization, and communication and networking technologies (Mattern, 2002; Fleisch and Mattern, 2005; Mattern, 2005; Müller, 2009), and it is driven by the decreasing cost of data entry from the physical world, Fig. II-2. In the vision of the Internet of Things, all items have unique identity and potential sensing and actualization capabilities; thus physical objects become smart and they can be automatically managed.

The Internet of Things is strongly destined for industrial usage. Williams (2008) argues that the Internet of Things is shaped and limited by its business cases, in a case to case basis. Fleisch and Tellkamp (2006) argue that the increased level of information system integration, improved data quality, and digital management control loops of the Internet of Things can provide improved processes, enhanced products, and new services. So instead of being a technology-push, the Internet of Things is also a market-pull.

In accordance to the long term vision of the Internet of Things, integration of RFID readers into mobile phones could empower masses of consumers with the ability to interact with products, including authenticating them. Consumers can already interact with products using the mobile phone camera as a barcode reader (Adelmann et al., 2006), and this interaction could be also enabled by Near Field Communication (NFC) technology. NFC operates at HF band and an NFC device can operate either as a reader or a tag[5]. Many mobile phones may support NFC in the future, though the published predictions have been overly optimistic (e.g. 30% of all mobile handsets NFC-enabled due 2011[6]). However, NFC is not compatible with EPC tags that operate at the UHF band, and solving these interoperability problems has already been discussed (e.g. Wiechert et al., 2007).

The following subsections dive into the details of RFID systems.

[5] NFC Forum (2007). http://www.nfc-forum.org/aboutus/

[6] Contactless Payment Comes to Cell Phones (November 2006). Business Week. http://www.businessweek.com/

II.3.1 System components and operating principle

RFID systems comprise tags that are attached to products, readers that read and write data on the tags, middleware that filters and aggregates the low-level data, and applications and services that reside on back-end systems (cf. Fig. II-3). The electromagnetic signals of tags correspond to low-level events (e.g. reader X observed the tag Y at time T) that are translated into high-level events (e.g. product Z was received to the warehouse W at time T) and to what is referred to business intelligence. The system components are detailed below.

- *Tags* or transponders are small electronic devices that are affixed to physical products. They come in various form factors including plastic and glass capsules, chip cards, and ”smart labels”. A tag includes an antenna, an analog radio frequency front-end, and a digital part (processor and memory). At minimum, tags can communicate their ID number but optionally they can also have user memory, password-protected access control, kill-command to protect end user privacy, cryptographic unit for strong challenge-response authentication, and sensors. *Passive* tags get all their energy from the reader field while *active* tags have a battery to power the microchip and send data. *Semi-passive* tags use a battery to power the microchip but they still use energy from the reader field to send data.

- *Readers* or interrogators are responsible of communicating with tags, i.e. reading and writing data on them. A reader device includes one or multiple antennas and can come in various configurations or form factors including a reader gate, a table reader, an autonomous portable reader, and a reader that can be integrated to a mobile device such as a personal digital assistant (PDA) or a mobile phone. A reader gate and a table reader are controlled by a separate computer.

- *Middleware* coordinates multiple readers that occupy the same physical space and transforms raw tag reads into streams of high-level events by filtering, aggregating, and counting them (EPCglobal Inc., 2007). An RFID reader is likely to observe an RFID tag several times when a tagged object passes by the reader, but this information is irrelevant at the application level, and middleware is responsible of formulating one, high-level read event out of the multiple low-level events. RFID middleware systems typically employ a smoothing filter that interpolates for lost readings that happen when a tag is temporally lost whilst it still is in the reader’s field. Using such temporal filtering technique the middleware can find out when a tag enters and leaves its field, based on uncertain reader output.

- *Applications and services* reside on back-end systems and they use and process the high-level RFID read events. Various enterprise applications can be linked to the RFID system including enterprise resource planning (ERP) systems, customer relationship management (CRM) systems, supply chain management (SCM) systems, e-business systems, and web services.

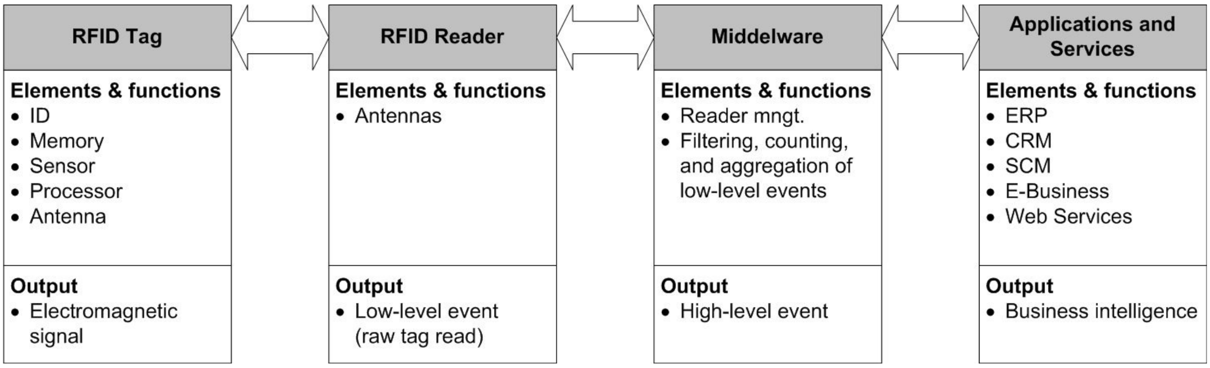


Figure II-3: *Architecture of an RFID system (adapted from Strassner (2005, p. 58))*

RFID tags are powered through two different operating modes: inductive coupling and electromagnetic backscattering (Lampe et al., 2005; Finkenzeller, 2006). Inductive coupling transfers energy to the tag through a magnetic field in the same way than an electronic transformer. The reader's coal generates a changing magnetic field that generates an alternating voltage in the tag's coil, supplying the tag's microchip with power. The power generated by the magnetic field depends on the reader's output power, frequency, and diameter and number of turns of the reader coil. The tag transfers data to the reader through *load modulation* which means coding signals by switching on and off a modulation resistor.

UHF and microwave RFID systems transfer energy through electromagnetic backscattering. The reader's antenna generates an electromagnetic wave that propagates to the RFID tag and generates an alternative voltage in the tag's antenna. The voltage is converted into direct currency to power up the microchip. The tag transfers data to the reader by modulating the reflected electronic field.

II.3.2 Frequency Spectrum

RFID systems operate on different frequency bands. The four major bands are listed below (Hunt et al., 2007; Lampe et al., 2005).

- *Low Frequency* (LF) – 100-135 kHz
- *High Frequency* (HF) – 13.56 MHz
- *Ultra High Frequency* (UHF) – 840.5-955 MHz
- *Microwave* – 2.45 GHz and 5.8 GHz

Operating frequency is a major selection criteria for end user companies who consider investing in RFID. It not only affects the physical properties and operation principles of tags and readers, but also the international compatibility of the system. Moreover, the physical properties of

Table II-2: *Typical characteristics of RFID systems on different frequency bands (Hunt et al., 2007; Lampe et al., 2005; Strassner, 2005)*

	LF	HF	UHF	Microwave
Frequency	100-135 kHz	13.56 MHz	840.5-955 MHz	2.45/5.8 GHz
Coupling method	Inductive	Inductive	Backscatter	Backscatter
Read range	<1.5 m	<1.0 m	<3...7 m	<2.0 m
Example	Animal tracking	ID cards	Pallet tracking	Toll system

tagged products can dictate the choice of frequency band: lower frequencies are less disrupted by products that contain water or metal; for instance, it is possible to integrate an LF tag inside a metal watch and read it through the full-metal watch frame (Cook et al., 2008).

LF tags are mostly used to track animals by implanting encapsulated tags under the animal's skin. These tags are regulated by international standards ISO 11784 & ISO 11785 that do not define anti-collision protocol. HF tags are often used in proximity cards, such as wireless smart cards and e-passports, and important standards in this frequency band include ISO/IEC 14443. UHF tags are often used in logistics applications owing to their elevated read range, and important UHF standards include EPC Class-1 Gen-2 (cf. subsection II.3.5) which has been also approved as the ISO 18000-6C.

HF, UHF and microwave RFID systems operate on industrial, scientific and medical (ISM) radio bands that are reserved by regulatory bodies. Though these bands were originally intended for non-commercial purposes, they are now being used by commercial applications such as WLAN and Bluetooth. The ISM bands are license-free but still subject to regional regulations relating the radiated power and interference.

LF and HF bands are worldwide available for RFID (Lampe et al., 2005), but this is not the case for the UHF band where differences exist. In the US, the UHF RFID band is located at 902-928 MHz. This band is not available in EU because it is occupied by GSM mobile phone systems and so the European UHF RFID devices operate at 865.6-867.6 MHz (EPCglobal Inc., 2009b). To further illustrate the differences, the UHF band is 952-954 MHz in Japan, and 840.5-844.5 MHz and 920.5-924.5 MHz in China (EPCglobal Inc., 2009b). UHF chips can operate on all frequency bands, but the antennas can be adjusted to different optimal frequencies. Moreover, while the maximum allowed transmission power in the UHF band is up to 4 W EIRP[7] in USA, it is 2 W ERP[8] in Europe (ETSI, 2008).

Table II-2 summarizes the typical characteristics of RFID systems.

[7] Equivalent isotropically radiated power

[8] Equivalent radiated power

II.3.3 Tag Memory

Tag memory is closely linked to the chip manufacturing process. A typical RFID tag manufacturing process starts with the design of the application-specific integrated circuit (ASIC), i.e. the chip. Outcome of the design project is a chip mask, based on which a semi-conductor foundry can produce the silicon chips. The chip production process is characterized by the manufacturing precision of the semiconductor manufacturing plant. Currently 120-140 nanometers is considered the state of the art for RFID chips.

Building a modern semi-conductor manufacturing plant is a billion-dollar investment, but older manufacturing technology is much less expensive. A semi-conductor foundry produces wafers that contain several thousands of chips. While chips are on the wafer, they are in an *open test state* and can be contacted through direct connectors instead of the radio frequency interface. After testing and programming, the chips are cut from the wafer and attached to antennas to produce tags (Finkenzeller, 2006).

A tag's non-volatile memory[9] consists of read only memory (ROM) and electrically erasable programmable read only memory (EEPROM). Pure ROM is implemented during the wafer production as arrays of transistors on the silicon chip. Because data is fully incorporated in the chip's physical structure, it can neither be erased nor replaced. Content of ROM is defined by the chip mask and all chips that are manufactured with the same chip mask have identical ROM content. Therefore ROM can only store non-serialized ID numbers. Rewritable non-volatile memory is typically implemented as EEPROM that can be reprogrammed. The memory cell employs two transistors in series, the storage transistor and the access (or select) transistor. The storage transistor has an additional floating gate, located between the channel and the upper gate known as the control gate. The stored memory state of any cell depends upon whether or not electronic charge is present on its floating gate (Haythornthwaite et al., 2004).

EEPROM is more expensive than ROM in terms of cost per one bit of memory, but it provides more flexibility. A *permalock* command that prevents reprogramming of EEPROM is sometimes used to replace ROM memory of RFID chips. For instance, the memory bands that are not meant to be reprogrammed after chip manufacturing can be written while the chips are on the wafer and then permalocked to prevent further manipulation.

The memories of existing EPC Class-1 Gen-2 chips include both EEPROM and ROM or permalocked EEPROM. The latter is used to store transponder ID (TID) numbers that identify the chip type and the possible custom commands and optional features the chip supports (cf. subsection VI.1), and they are written on a dedicated TID memory bank. This number is not meant to be reprogrammed after chip manufacturing. Other memory fields of EPC tags are on EEPROM and they include the EPC memory bank, the user memory bank, and the reserved memory bank for kill and access passwords (EPCglobal Inc., 2005b). The memory banks of EPC Class-1 Gen-2 chips are illustrated in Fig. II-4.

[9] Memory content is not erased when the chip is not powered

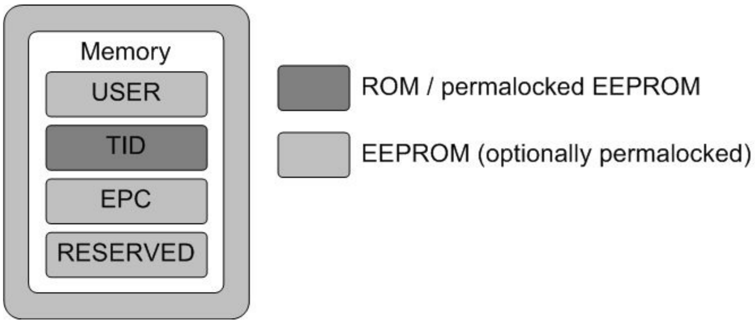


Figure II-4: *Memory map of an EPC Class-1 Gen-2 tag*

II.3.4 Missing Reads

As other Auto-ID technologies, RFID systems are somewhat prone to read errors; the laws of physics can prevent RFID tags being read in certain situations even though a tag is present in the reader field. This creates a *missing read*. Though read errors can occur also with other Auto-ID technologies, they are especially disruptive in RFID systems owing to the bulk mode reading where missing reads can easily go unnoticed (e.g. compared to scanning of single items in the point of sales). As a result, missing reads can severely reduce the potential benefits of adopting RFID (Tellkamp, 2006, p. 47).

Various causes of uncertainty in RFID traces have been discussed in the scientific community. Derakhshan et al. (2007) identify inaccuracy, i.e. missing reads (false negatives) due to imperfect read rates, as one of the primary factors limiting the widespread adoption of RFID technology. Real-world read rates of only 60-70% have been reported (Jeffery et al., 2006), though presenting general numbers for read rate is misleading since the read rate depends on many case-specific factors (cf. Fig. II-5). Researchers in the University of Arkansas measured the read rates of RFID tags in Electronic Article Surveillance (EAS) (Hardgrave and Patton, 2008). Overall, the tested UHF tags and readers performed very well compared to existing EAS systems, especially for reading single tags. When scanning 50 tags passing through a gate, read rates of 95% and more were observed.

Examples from the field show that missing reads can also be eliminated in real-world RFID implementations by engineering solutions in the physical layer. Folcke (2008) describes a commercial ”smart cabinet” application where medical devices (25% of which contained a metal cover) are automatically identified. After the first deployment, the error rate in identification was smaller than 1.5×10^5 (no errors in 65,000 reads). This high level of reliability was achieved by choosing the best frequency for that particular application (125 kHz), by positioning and adjusting the reader antennas, and by choosing the best tag position on the products.

The most common causes for missing reads are summarized in Fig. II-5. Most of these causes can be traced down to the physical layer. Most importantly, these include i) missing reads

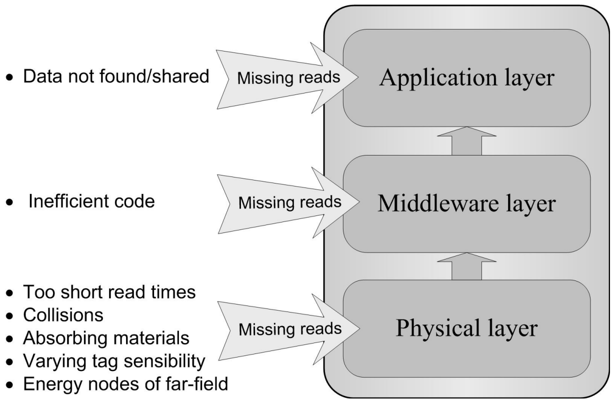


Figure II-5: *Sources of missing reads in RFID systems*

due to too short reading times (the time the tag is in the readers field), ii) collisions in the air interface that collision detection protocol does not catch, and iii) conductive materials that absorb radio waves. Since reading times cannot always be increased due to constraints in business processes (e.g. speeds of conveyor belts and manufacturing lines) and the tags cannot be always chosen to provide the best performance for all products and read locations, the most important root problems cannot be always directly addressed. In addition, when tags are read using the far-field they might be in a node where the field strength is close to zero and thus a tag will not be read. In these cases, moving the tag few centimeters is likely to correct the problem. Furthermore, due to normal variance in tag manufacturing processes, chips and antenna connections have varying impedances which results into variance in tag read range.

Note that bit errors in the data that is read from the tags do not constitute a source erroneous events because of effective error detection coding. For example for UHF tags conforming to the ISO 18000-6C standard air interface, the memory content that is read from the tags is appended with a CRC-16 checksum defined in ISO/IEC 13239 standard. The probability that the CRC-16 checksum does not detect a single bit error in the payload is very small, 2^{-16}.

Also slow or otherwise non-optimal code in the middleware can result into missing reads, even when an antenna has interrogated a tag. In a typical setting, middleware listens to all the antennas of a reader device in a loop. If a tag is present in one antenna's field whilst the middleware is listening to other antennas (e.g. reading other tags), the low-level event might not be captured by the middleware. Moreover, it is theoretically possible that inefficient code in the middleware is too slow to process all the low-level events when multiple tags are scanned.

Last, also problems in the application layer can lead to missing events. In supply chain applications, the high-level data can be gathered and stored in multiple locations, by multiple supply chain partners. In the EPCglobal network (EPCglobal Inc., 2009a), the responsibility to locate data relating to a product is assigned to the EPC Discovery Service (DS). However, it is not yet known how DS can provide 100% reliability without delays in large supply chain networks. In addition, it is likely that all companies do not want to share information with all other companies. As a result, RFID applications might not have access to all relevant data.

In addition to missing reads, RFID traces can be plagued by so called *phantom reads* or *ghost reads* where a reader reports a tag that was was not in its field or did not exist. In a ghost read, the reader receives incorrect data which it interprets as valid data and it results in erroneous trace data, more specifically, in an identifier that is not stored on any tag. In practice, ghost reads can fortunately be nearly eliminated with a combination of correct RFID protocol design, redundant error detection features in the air interface, error protection on the communicated data, as well as other measures, and therefore they are unlikely to appear for instance in the EPC Class-1 Gen-2 protocol (Engels, 2005).

II.3.5 EPCglobal network

The most important standards for networked RFID are overseen by EPCglobal Inc[10], a subsidiary of the global standards organization GS1[11]. The term EPC stands for an *Electronic Product Code*. The development of EPC standards stems from the collaboration of the Auto-ID Center of Massachusetts Institute of Technology (MIT) and the industry. Today EPC standards are supported by major industrial players especially from the retail industry—among the top 30 Fortune 500 companies in 2007 can be found 13 EPCglobal members[12].

EPC is a high-level or ”envelope” identifier format that accommodates existing coding schemes such as the GS1 identification keys[13], i.e. identifiers that denote individual physical items, services, locations, logistic units, returnable containers, etc. These include Global Trade Item Number (GTIN), Global Location Number (GLN), Serial Shipping Container Code (SSCC), Global Returnable Asset Identifier (GRAI), Global Individual Asset Identifier (GIAI), Global Service Relation Number (GSRN), and Global Document Type Identifier (GDTI). Conversion rules specified in the EPC Tag Data Standard define how to map a GS1 key to the corresponding EPC value (EPCglobal Inc., 2006).

EPC infrastructure is defined by the EPCglobal Architecture Framework which is a collection of interrelated hardware, software, and data standards (EPCglobal Inc., 2009a). This framework is sometimes called the ”EPCglobal Network”, though this name is more of an informal marketing term rather than the name of an actual network or system. Being a well-established term in the industry jargon, however, the term EPCglobal Network will be used throughout this thesis. Goals of the EPCglobal standards and the EPCglobal Network are to facilitate the exchange of information and physical objects between trading partners, foster the existence of a competitive marketplace for system components, and encourage innovation.

EPC Information Services (EPCIS) is the primary vehicle for data exchange between end-users

[10] EPCglobal (2009). http://www.epcglobalinc.org

[11] GS1 (2009). http://gs1.org/

[12] CNN Money (2007). Fortune 500—Annual ranking of America’s largest corporations. https://www.money.cnn.com/magazines/fortune/fortune500/2007

[13] GS1 (2009). http://www.gs1.org/barcodes/technical/id_keys#sscc

such as manufacturers or logistic service providers. It encompasses interfaces for data exchange and specifications of the event data itself. EPCIS data is information that trading partners share to gain more insight into what is happening to physical objects in locations inside and outside their own four walls (EPCglobal Inc., 2009a).

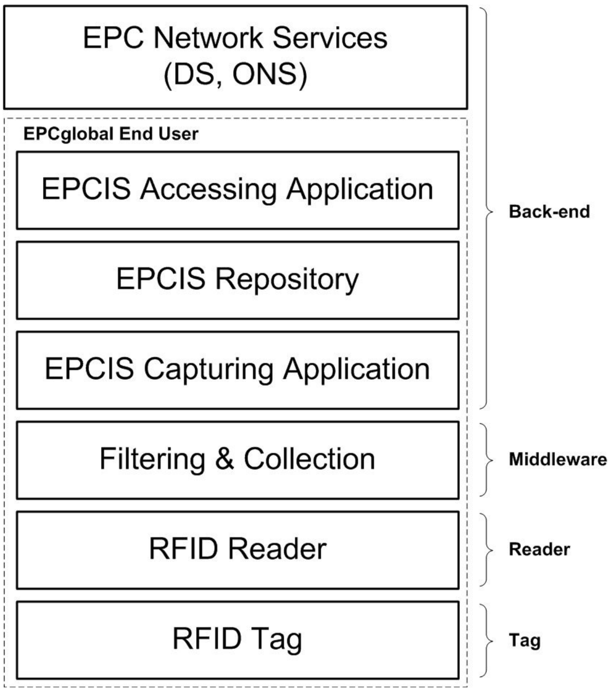


Figure II-6: *Hardware and software roles in the EPCglobal network*

Figure II-6 illustrates the hardware and software roles in the EPCglobal network. The EPCglobal Architecture Framework (EPCglobal Inc., 2009a) defines interfaces between these roles. Definition of these interfaces is still and ongoing task. Standards that are still under development include for example the Discovery Services and HF tag air interface. The hardware and software roles are explained below (EPCglobal Inc., 2009a).

- *Tags* are classified according to their functionalities. Class-1 tags (”Identity Tags”) and Class-2 tags (”Higher-Functionality Tags”) are passive tags with limited features while Class-3 (”Battery-Assisted Passive Tags”) and Class-4 (”Active Tags”) tags have a battery and can form communication channels with each other, or sensor networks.

- *Readers* make low-level observations of RFID tags that are in the read zone.

- *Filtering & Collection* filters and collects raw tag reads over time intervals delimited by events defined by the EPCIS Capturing Application.

- *EPCIS Capturing Application* provides business context by coordinating with other sources of information involved in executing a particular step of a business process. The EPCIS

Capturing Application may, for example, coordinate a conveyor system with filtering & collection events.

- *EPCIS Repository* records EPCIS level events generated by one or more EPCIS Capturing Applications and makes these events available for later query by EPCIS Accessing Applications.

- *EPCIS Accessing Application* is some application specific to a partner end-user, and interested in information about a particular EPC.

- *Object Name Service* (ONS) is a lookup service based on the existing Domain Name System (DNS) that takes an EPC as input and produces as output the address of an EPCIS service designated by the issuer of the EPC. EPCglobal provides the root ONS as a part of the core network services, but it is up to each subscriber to run the local ONS that replies to the lookup requests.

- *Discovery Services* (DS) locate the EPCIS services of all end-users that have information about the object in question and, additionally, provide a cache for some EPCIS data. DS is a very important functionality and the EPCglobal Community is currently drafting requirements for the Discovery standards and services[14].

Multilateral networks for exchange of data among trading partners that the above described standards enable have many requirements for security. EPCglobal Network addresses security in terms of data protection methods and privacy; security features are either built into the standards or use of best practices that are in accordance with the EPC standards are recommended. The security features built into the standards include authentication of end users, services, physical devices, and killing and locking of tags. However, the current security features do not yet cover all the security requirements of the EPC Network. Regarding this thesis, the most significant security gap relates authentication of the tagged objects to mitigate tag copying attack (cf. Fig. I-4). Other open security challenges include authentication of high-level events and management of access rights to the EPC data.

II.4 Security

Though the word *security* is easy to understand as a synonym for *protection* in everyday language, security cannot be analyzed without formal definitions of terms that make all underlying assumptions explicit. Regarding the following definitions of security terminology, this work refers to the ISO/IEC 27000:2009 standard (ISO, 2009) that defines vocabulary for information security management.

[14] This work has been undertaken e.g. in WP2 of the BRIDGE project, http://www.bridge-project.eu

Security always involves an *asset* (”anything that has value to the organization[15]”) that is protected against *threats* (”potential cause of an unwanted incident, which may result in harm to a system or organization”) caused by adversaries. What security means in a given context is defined by the chosen assets and the expected threats, and if either assets or threats are not defined the notion of security remains helplessly vague. Thus the working definition for security used in this thesis is *protection of certain assets against threats of adversaries*.

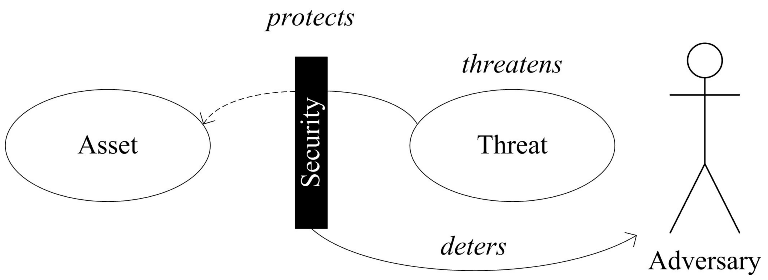


Figure II-7: *General security concepts*

Figure II-7 illustrates the conceptual framework of general security concepts: a threat *threatens* an asset and security *protects* an asset and *deters* the adversary. Deterrence is the indirect effect of security which makes an adversary less willing and thus less likely to attempt to materialize the threat. If the deterrent effect does not exist because the threats are caused by nature or ”bad luck”—and not by an adversary with intentions—one is dealing with *safety* and not security.

Closely relating security, the term *risk* refers to the combination of the probability of an event, e.g. a materialized threat, and its consequence. In the purest sense of the term, risk is a tuple of these two elements and a combination of them into a single element (e.g. high or low) can be done only with assumptions of risk-neutrality (e.g. risk-averse, risk-neutral, or risk-seeking). Moreover, *vulnerability* is defined as a weakness of an asset, policy, guideline, or practice that can be exploited by a threat, and an *attack* as an ”attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset”.

II.4.1 Security Services

Security is provided by *security services* that are different ways to protect assets. The notions of security services are commonly used in the field of information and network security but they can be applied to virtually any security domain. Many textbooks provide definitions for security services (e.g. Schneier, 1996; Kurose and Ross, 2003), sometimes adopting them to a particular application such as communications systems. This work opts for more general definitions based on (ISO, 2009) which defines security services as follows.

[15] Asset can be information, software, physical, service, people, or intangible

- *Authentication* is a provision of assurance that a claimed characteristic of an entity is correct.
- *Confidentiality* is a property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
- *Integrity* is a property of protecting the accuracy and completeness of assets.
- *Non-repudiation* is an ability to prove the occurrence of a claimed event or action and its originating entities, in order to resolve disputes about the occurrence or non-occurrence of the event or action and involvement of entities in the event.
- *Availability* is a property of being accessible and usable upon demand by an authorized entity.

Availability differs from the other four security services by being actually a characteristic of the usability of the application, rather than a direct characteristic of security. Thus, in addition to the common trade-offs between between security, cost, and usability & performance, there are common trade-offs between the security services themselves, usually involving availability. For instance, burying a computer in the bottom of an ocean provides very good confidentiality for the data stored on the hard disk, but the availability of this information becomes very poor.

II.4.2 Cryptography

Cryptography is an irreplaceable building block of information systems security. Even though the development of cryptographic schemes is not in the scope of this thesis, an introduction to cryptography is necessary to understand the related work on RFID security and the concepts that the technical contribution of this thesis seeks to complement.

Cryptography refers to designing ciphers, i.e. algorithms that encrypt and decrypt data. It is the mathematical part of security engineering and closely linked to the theory of authentication. The topic is well covered by several textbooks (e.g. Schneier, 1996; Anderson, 2001a; Kurose and Ross, 2003) and this subsection only introduces the basic concepts that are needed to understand product authentication based on RFID tags that can run ciphers.

Referring to Anderson (2001a) for the terminology, *cryptography* refers to the science and art of designing ciphers and *cryptanalysis* to the science and art of breaking them. The input to an encryption process is called the *plaintext* and the output *ciphertext*, whereas decryption process works inversely. There are a number of *cryptographic primitives* that are basic building blocks for algorithms such as *block ciphers*, *stream ciphers*, and *hash functions*.

A stream cipher's encryption rule depends on a plaintext symbol's position in the stream while a block cipher encrypts several plaintext symbols at once in a block of a certain block size. Block ciphers may either have one key for both encryption and decryption, in which case they are called symmetric (or secret key), or separate keys for encryption and decryption (public and private keys, respectively), in which case they are called asymmetric (or public key). It should not be possible to derive the private key based on a known public key. A hash function (or a one-way function) accepts an input string of any length and outputs a random string of fixed length. The output of the hash function is known as the *hash value*, *message digest*, or simply the *hash*, and for each input string there is only one hash value.

Cryptographic authentication methods are often referred to as *challenge-response* protocols, or simply protocols. They can be motivated by flaws in the unsecure basic authentication method where B wants to prove A that he really is B over an unprotected communication channel (i.e. an adversary can observe the messages):

$$B \rightarrow A : \text{"}\textit{I am B}\text{"}$$
$$B \rightarrow A : \textit{password}$$

The notion $B \rightarrow A$ means that B sends a message to A. The first message is a claim of identity and the second message secret information that A knows that (only) B knows. This basic method is secure only the first time it is used. After that an adversary could have *eavesdropped* the *password* and he/she can impersonate B. Authentication protocol based on symmetric cryptography resolves this vulnerability as follows:

$$B \rightarrow A : \text{"}\textit{I am B}\text{"}$$
$$A \rightarrow B : ch$$
$$B \rightarrow A : E_{A-B}(ch)$$
$$A : D_{A-B}(E_{A-B}(ch)) = ch$$

Here ch stands for a random challenge, E_{A-B} denotes encryption with the symmetric secret key shared by A and B, and D_{A-B} denotes decryption with the same key. Since B can generate a challenge that has never been used before, an adversary who has eavesdropped the past communication cannot fool B by knowing the correct response ($E_{A-B}(ch)$). In the fourth step of the protocol A verifies whether B knows the shared secret key or not.

Ciphers for the calculation of $E_{A-B}(ch)$ include the Data Encryption Standard (DES) that is widely used in banking and has a block size of 64 bits (8 ASCII characters). DES is however being replaced in many applications by the more secure Advanced Encryption Standard (AES) that has twice as big block size (e.g. Schneier, 1996).

Authentication protocol based on asymmetric cryptography differs in the way the verifier A decrypts the response. When E^{-A} denotes encrypting with the secret key (private key) of A, and D^{+A} decryption with the public key of A, the conventional asymmetric authentication protocol can be formalized as:

$$\begin{aligned}&B \rightarrow A : \text{"\textit{I am B}"}\\&A \rightarrow B : ch\\&B \rightarrow A : E^{-A}(ch)\\&A : D^{+A}(E^{-A}(ch)) = ch\end{aligned}$$

Common ciphers for the calculation of $E^{-A}(ch)$ include the RSA algorithm of Rivest, Shamir, and Adleman (Rivest et al., 1978) and Elliptic Curve Cryptography (ECC) (Miller, 1986; Koblitz, 1987). To provide the same level of protection as a symmetric block cipher, asymmetric ciphers are believed to require at least twice the block length. ECC appears to achieve this, for instance a 128-bit ECC scheme could be about as hard to break as a 64-bit symmetric block cipher with a 64-bit key (Anderson, 2001a, 112).

Asymmetric cryptography is also widely used to create *digital signatures*. Like the written signatures, digital signatures attest that the signing person has acknowledged and agreed with the singed document's contents. In addition, a digital signature is linked to the document's content in a verifiable and non-repudiable way. As a result, it is a prove that a document signed by an individual was indeed signed by that individual (authentication), that only that individual could have signed the document (non-repudiation), and that the document has not been changed after signing (integrity). In the physical world, digital signatures are used for instance in digital postal marks or parcels and printed as 2D barcodes (Pintsov and Vanstone, 2001).

A digital signature of a message m is created by encrypting m with one's private key. For example, if A signs m the signature is $E^{-A}(m)$. If the message is long, the encryption operation can be very lengthy. Therefore one typically first calculates a fixed-length "fingerprint" of the message called the *message digest* using a hash function. The message digest of m can be denoted as $H(m)$ and the corresponding signature is then computed as $E^{-A}(H(m))$. To verify a digital signature, one must compare the message digest of the received document to the decrypted digital signature that is of form $D^{+A}(E^{-A}(H(m)))$. In other words, the digital signature is decrypted with the public key of A.

Various algorithms can be used to generate digital signatures. One way how those algorithms vary is the signature length required to provide a given level of security. For instance, a digital signature generated with the RSA algorithm has typically the length of 1024 bits (Boneh et al., 2004; Naccache and Stern, 2001; Pearson, 2005). The level of security of this signature is 80 bits which means that an adversary requires in average about 2^{80} signature generations to find the private key that was used to generate the signature. The same level of security can be achieved also with shorter signature lengths; the Digital Signature Algorithm (DSA) and the Elliptic Curve DSA (ECDSA) provide the same level of security with 320 bit signature length (Naccache and Stern, 2001). Even shorter signature schemes achieving the same level of security have been proposed in research papers, for example, with key lengths of 208 bits (Naccache and Stern, 2001) and 171 bits (Boneh et al., 2004).

Offline Verification of ID Numbers

Public key cryptography can be used together with low-cost RFID technology to enable offline verification of ID numbers. In this context, verification means finding out whether the product ID number has been issued by the authorized party or not, and it can be done without cryptographic computations by the tag.

In this scheme the product ID number consist of two parts: random number ID_{rnd} and its digital signature $E^{-A}(H(ID_{rnd}))$. The authorized party computes the digital signature based on the secret key $-A$. Another party who knows the corresponding public key $+A$ can verify the tag's ID number by decrypting the digital signature, which means computing $D^{+A}(E^{-A}(H(ID_{rnd})))$, and compare it to the message digest $H(ID_{rnd})$. When these numbers match, the product ID number is issued by the authorized party, e.g. the brand owner.

Assuming that ID_{rnd} and the digital signature are of sufficient length, this scheme prevents guessing of product ID numbers and enables offline verifications. Guessing of valid ID numbers can be prevented also with ID_{rnd} alone when there is an online database where the validity of ID numbers can be verified. Even when guessing of ID number is prevented, however, cloning of tags is still possible through skimming and eavesdropping (cf. subsection III.4). Therefore secure product authentication also requires that tag cloning attack is addressed (cf. subsection IV.2). But verification of serialized ID numbers is still a potentially effective way to detect counterfeit products, especially when products are shipped in large lot sizes (cf. subsection V.2.3), and it is therefore proposed as the starting point in a roadmap toward secure authentication of EPC-tagged products (cf. subsection VII.2).

II.4.3 Security Requirements

Securing an existing system that is built without keeping security in mind can be both expensive and inefficient. For example, houses need to be designed with windows and doors that can be properly locked, airports need to be designed with space for security controls, and computer networks need to be designed with suitable places for firewalls, access control, and intrusion detection systems. Therefore security needs to be taken into account already when designing new systems. This can be done by defining security requirements.

Bishop (2003) argues that security requirements define security goals by answering ”what do you expect security to do for you?”. Security requirements are followed by a security policy that answers how the security goals are to be achieved, and by security mechanisms that enforce the policy. Alexander (2003) argues that security differs from all other specification areas in that someone is deliberately threatening to break the system and therefore it needs to be addressed with special methods.

As one possible solution for electing security requirements, Alexander (2003) and Sindre and Opdahl (2005) examine *misuse cases* to derive the functional security requirements of a sys-

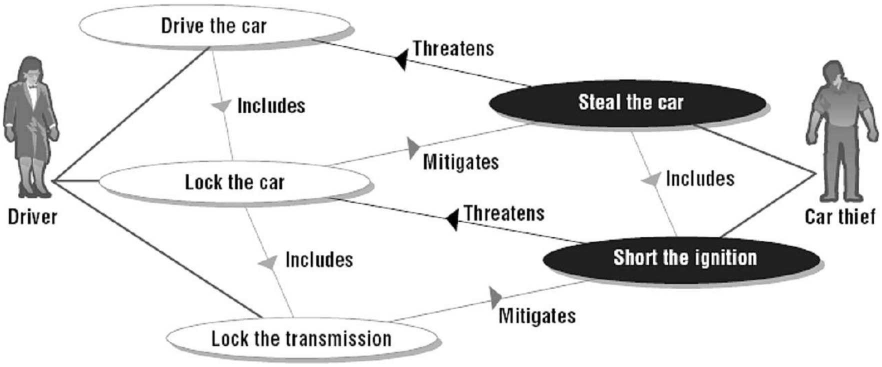


Figure II-8: *Use/misuse case diagram of car's security requirements (Alexander, 2003)*

tem. Use cases (Alhir, 2003) are common in requirements engineering but they offer limited support for electing security requirements because they take into account only the intended use. Extending the use case paradigm with misuse cases of illicit actors enables modeling and analyzing the unintended use as well. Figure II-8 illustrates the resulting use/misuse case diagram that presents the functional security requirements as white ovals. Sindre and Opdahl (2005) propose a process for eliciting security requirements with misuse cases based on identification of critical assets and their security goals, and an analysis of risks and protection costs. This method will be applied to derive the functional security requirements of RFID-based product authentication systems in Section IV.

II.5 Review of Technical Anti-Counterfeiting Measures

RFID is by no means the only technology that brand owners can use in anti-counterfeiting. This subsection reviews existing technical anti-counterfeiting measures.

The core function of technical anti-counterfeiting measures is to enable people distinguish genuine articles from counterfeits. This is achieved through product authentication which can be seen as a tool or a method that verifies a physical products and answers either with a ”green light” (i.e. product is authentic) or a ”red light” (i.e. product is counterfeit). Some techniques can also answer with a ”yellow light” which means that the result is not known for sure and further inspections are needed.

This subsection reviews technical anti-counterfeiting measures by categorizing and listing existing techniques. Most techniques rely on inserting a *security feature* on the product based on which the product can be authenticated. There are various criteria to categorize technical anti-counterfeiting measures including the underlying technology, the underlying reasoning, whether the security feature is machine-readable or not, or how visible the security feature is. The last criteria provides the following commonly-used categorization for security features.

- *Overt feature:* visible to the naked eye, verified with or without a reading device.
- *Semi-covert feature:* visible in certain artificially-reproducible conditions.
- *Covert feature:* not visible to the naked eye, requires a special reading device.
- *Forensic feature:* virtually invisible, part of a product's physical and chemical structure.

This subsection classifies anti-counterfeiting techniques to i) overt and semi-covert labeling approaches, ii) covert and forensic labeling approaches, iii) direct authentication approaches, and iv) serialization and tracing-based approaches (cf. Fig. II-9). RFID-based approaches are excluded from this review and presented in details in subsection III.4.

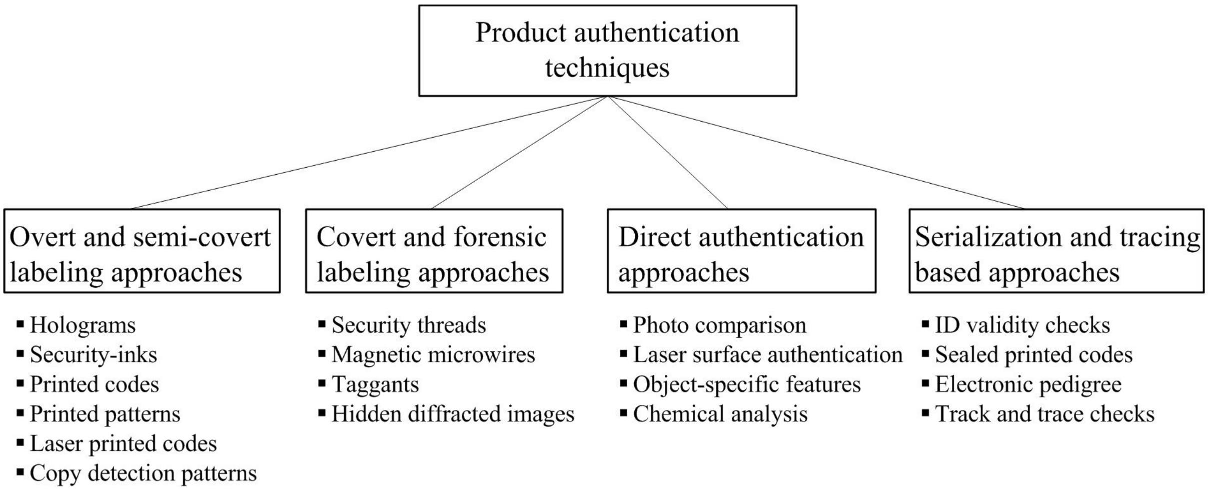

Product authentication techniques
Overt and semi-covert labeling approaches
▪ Holograms
▪ Security-inks
▪ Printed codes
▪ Printed patterns
▪ Laser printed codes
▪ Copy detection patterns
Covert and forensic labeling approaches
▪ Security threads
▪ Magnetic microwires
▪ Taggants
▪ Hidden diffracted images
Direct authentication approaches
▪ Photo comparison
▪ Laser surface authentication
▪ Object-specific features
▪ Chemical analysis
Serialization and tracing based approaches
▪ ID validity checks
▪ Sealed printed codes
▪ Electronic pedigree
▪ Track and trace checks

Figure II-9: *Categorization of product authentication techniques*

II.5.1 Overt and Semi-Covert Labeling Approaches

Various labeling techniques are used to authenticate branded or trademarked products. Labeling-based authentication techniques are based on marking the genuine products with additional physical or chemical security features that cannot be easily reproduced without access to special know-how, materials, or equipment. This makes security feature and thus the product difficult and expensive to forge; a counterfeiter who wants to fool the authenticity check either needs to forge the security feature or remove an authentic security feature from a genuine article and reapply it to a counterfeit article.

Overt security features provide the first level of verification and many of them can be verified by anybody, including consumers and customs officers. Hologram is probably the best-known overt anti-counterfeiting label. Hologram technology took major leaps following the development of the laser in the 1960s and at first holograms used to be very hard to manufacture and easy to verify, being suitable for secure and easy product authentication. Embossed holograms first turned up on credit cards as a security device in the 1980s and today they are used in software and CD packaging, clothing labels, ID cards etc. But holograms are no longer considered secure. Today the technology to manufacture holograms is widely spread and holograms are found in several counterfeit products—even when the genuine articles do not have one—and many consumers cannot tell the difference between the hologram of a reasonable counterfeit and that of an authentic item.[16] For an improved protection, modern security holograms can incorporate a serial number, such as the tesa holospot[17]. Other overt features include color-shifting films that change color when looked from different angles.

Security inks are a common example of semi-covert labeling techniques. Different kinds of security inks can be used to put invisible or color-shifting markings on products that cannot be detected without specific light, such as infra-red or ultra-violet, or chemicals. Security inks are commonly used to authenticate banknotes. Even though security inks can be invisible, they can often be discovered by professional counterfeiters without much trouble.

Copy detectable images (CDI) are computer generated images used to automatically detect copies of documents or products on which they are printed. Examples of CDIs include ”fragile” digital watermarks, sparse patterns of small dots and copy detection patterns (CDP) (Picard, 2001). A CDP is a printed labels of pseudo random noise and it can be incorporated for example in 2D barcodes (Picard, 2004). Since the pattern appears as random variations in color saturation over the label area it is hard to be copied without loosing information. The CDP is verified by comparing an optical image to what the pseudo random noise pattern should be. The technique relies on the fact that if the original optical marker is copied, the resulting noise pattern will be slightly different compared to the original pattern due to imperfect scanning and printing, and this difference can be detected. As a result, CDIs appear very promising for optical document security rendering paper itself a hard-to-copy feature. On the downside, CDIs can hardly be used reliably without a deep understanding of printing processes so they are not plug-and-play solutions (Picard, 2001).

In addition, there are many secure printing techniques developed to authenticate banknotes, passports, and other value documents. These techniques include, for example, watermarks, micro printings and printed codes, printed patterns, and intaglio printing. A watermark is a recognizable image or pattern in paper that appears lighter when viewed by transmitted light and most banknotes have them. Micro printings are very small markings that can only be produced with sophisticated machinery. Printed patterns include for example artificial Moire effect that is interference pattern created when two grids are overlaid at an angle. Security printing technology is based on the concept of using highly defined print lines to create complex designs that are difficult to originate and print. All these techniques increase the barrier to copy banknotes and paper documents, and their copying resistance is characterized by the complexity of machines that are needed to fabricate them. These techniques are normally considered overt

[16] Wired magazine (2007). http://www.wired.com/science/discoveries/news/2007/02/72664?currentPage=all

[17] Tesa Scribos GmbH (2009). http://www.tesa-scribos.com

but if the printings are small enough they can also be considered semi-covert or even covert.

II.5.2 Covert and Forensic Labeling Approaches

Covert and forensic labels are invisible to the naked eye. This makes them less likely to be discovered by counterfeiters but harder to be verified. Covert labeling techniques include for example small security threads that are embedded within the paper fibers and can be completely invisible or have special effects. Another example is MicroWires[18] that are small glass-coated fibers with special magnetic properties which can be verified with a special device. However, covert labeling techniques can be also much less high-tech, such pas printed patterns that reveal a codeword when looked through a special decoder device (Hopkins et al., 2003, p. 254).

Forensic labeling approaches include microscopic taggants[19] that are very small particles used to uniquely mark products, and whose existence on a product can be later verified. There are various techniques how to produce small particles that are suitable for this purpose. Sizes of microscopic taggants are measured in micrometers (one millionth of a meter) but they still can be used to code information on products. The taggants themselves can be sensitive to energy (e.g. infrared radiation) or temperature, which enables different ways of verifying their existence on a product. Combined with unique color coding, microscopic taggants can provide millions of unique ways to mark products.

Taggants are used for instance to authenticate pills. However, if only the existence of a taggant is verified, but not its concentration, then the check might be fooled by pulverizing one genuine pill and mixing it into the compound used to manufacture counterfeit pills. Taggants whose concentration can be verified can be used for example to detect adulterated or diluted versions of branded fuels (Hopkins et al., 2003, p. 254).

II.5.3 Direct Authentication Approaches

In addition to the aforementioned labeling approaches, products can be also authenticated directly based on their physical or chemical features. A rudimentary example of such approaches is comparison of the product under inspection to photos about the visual features of the genuine products. Photo comparison can be applied as a first level verification of products that have a number of details that can be visually verified, for example luxury hand bags. However, the reference photos need to be kept safe from counterfeiters.

One example of direct authentication techniques is laser surface authentication (LSA)[20]. LSA is based on the fact that hard material surfaces consist of unique microscopic 3D surface patterns and a fingerprint of this pattern can be measured from the way the surface reflects light.

[18] Role of Nanotechnology in Brand Protection (2007). Converting Magazine. http://www.convertingmagazine.com/article/CA6479787.html

[19] Microtrace (2007). http://www.microtracesolutions.com/transpondergant.htm.

[20] Protexxion (2007). http://www.bayertechnology.com/eng/press/79_6540.php

LSA measures the reflection pattern by sweeping a laser beam over a surface and compares it to entries in a reference database. Consecutive reads of the same surface do not result into identical feature vectors because of natural variations of the process and therefore the comparison allows a range of variations. This technique makes most surface materials hard to copy without additional labels, but one needs to know which part of the product must be scanned.

Also scientific analysis of physical or chemical properties of the product itself counts as direct product authentication. This is sometimes referred to as *forensic analysis* and it typically takes place in laboratory conditions. The downside of forensic analysis is the low response time which can be up to days.

II.5.4 Serialization and Tracing-Based Approaches

Serialization and tracing-based approaches do not rely on making copying of genuine products harder. Instead, they give unique identity to all genuine products and seek to detect products with copied identifiers. These techniques require that products are serialized and traced. A counterfeiter can usually copy the identifier without much difficulty but there is little he can to prevent the system from trying to detect tags with copied identifiers. In this thesis tracing-based authentication approaches are denoted as *location-based authentication* since these approaches use location information to detect tags with copied identifiers.

Scientific literature recognizes that serialization alone can be a powerful anti-counterfeiting tool. Juels (2006) illustrates this with an example from the art world where a Victorian painter issued serial numbers to his paintings and cataloged them. Juels argues that (partly) because of this reason far less spurious paintings of this particular painter turn up on the market than from other painters. However, the primary business motivation of serialization and tracing-based countermeasures in fighting illicit trade is typically detection of diverted articles and not the detection of counterfeit articles.

The first step in serialization and tracing based approaches is verification that the product under study has a *valid ID number*—i.e. one that is or could have been issued by the brand owner. The database that stores the valid ID numbers is denoted the ”white list” by Koh et al. (2003).

Electronic pedigree, or e-pedigree (e.g. EPCglobal Inc., 2008), is probably the best-known serialization and tracing-based anti-counterfeiting measure. Buyers and sellers of a product must append its pedigree file upon every transaction with digitally signed events. In this scheme, all genuine products must have an valid e-pedigree so a product without one is helplessly suspicious. The pedigree itself is not protected from copying and a counterfeiter can copy the pedigree of a genuine product to go along a counterfeit product. But by signing transactions of the counterfeit product the counterfeiter will face a risk of being caught since there are multiple copies of the same pedigree in circulation. Legislation that mandates the use of e-pedigree for pharmaceutical products has already been accepted in several states in the U.S. (e.g. California, Nevada, Florida) and it is likely that similar regulations emerge in the near future.

Also consumers or end-users are involved with serialization-based approaches. For example Nokia uses holograms and unique ID numbering to allow consumers to verify the authenticity of their batteries. Each genuine battery must contain a unique 20-digit code that can only be revealed by scratching the ink coating that covers the code. A consumer can read the code and enter it using SMS or a web-interface to a service that returns whether the battery is genuine or not based on whether the code has already been used[21].

Also the software industry uses unique ID numbers to authenticate products. Certain software products must be activated using a unique ID number after the installation. When the activation is done in a centralized manner, the system knows whether an ID number has already been used. Consumers can authenticate products also using custom-made paper labels that contain the ID numbers[22]. These paper label are sealed and reading the ID number without opening or damaging the label should not be possible. When a consumer wants to verify the authenticity of a product he needs to open the label and enter the ID number on a website that tells whether the product is genuine or not. Only a registered and unused code will return a positive response.

[21] Nokia (2008). http://www.nokia.co.id/nokia/0,,82227,00.html

[22] Dintag (2008). https://www.dintag.com/

III Related Work

One the one hand, related work on measures against product counterfeiting stems from research on anti-counterfeiting strategies. This is a somewhat sparse stream of scholarly papers that dates back to the end of 1970s and it applies scientific methods to the topic that is otherwise primarily discussed in trade publications and business papers. This research aims at providing guidance for practitioners who have to define anti-counterfeiting strategies and it conceives the use of technical measures as one anti-counterfeiting strategy among others (cf. Fig. I-1).

On the other hand, the vast body of knowledge about security engineering and related fields cover many aspects of technical anti-counterfeiting measures. Though this research only rarely explicitly addresses product authentication techniques, it provides the foundations for understanding and explaining them. Related work on security is categorized to research on level of security, economics of security, and RFID security.

III.1 Research on Anti-Counterfeiting Strategies

In accordance with the counterfeiting literature, this subsection uses the term *anti-counterfeiting strategy* in a lax way to refer to all plans, programs, projects, and countermeasures that affected companies and governments take to fight product counterfeiting and piracy. This research field is closely linked to supply and demand studies of counterfeit trade which contribute to the development of anti-counterfeiting strategies by providing ”tactical” knowledge, and thus these research fields partially overlap. A comprehensive review of counterfeiting literature covering anti-counterfeiting strategies, supply and demand studies, impact analysis, as well as legal issues is collected by Staake et al. (2009).

The earliest scholarly contributions on anti-counterfeiting strategies date back to the end of 1970s and to the beginning of the 1980s, and they focused on describing the problem and outlining the first countermeasures. The following contributions elaborated the countermeasures and discussed company-wide anti-counterfeiting strategies. Since the late 1990s, the contributions have been focusing on evaluation and implementation of anti-counterfeiting strategies. Figure III-1 illustrates a time line of chosen scholarly contributions on anti-counterfeiting strategies.

Kaikati and LaGarce (1980) are among the first to discuss the economic, political, and cultural factors of product counterfeiting and piracy in scholarly journals. The authors argue that narrowed technological gaps between affected economies and others and increased interest in foreign markets are contributing to the increase of product counterfeiting and piracy. In addition to describing the problem, the authors identify four major strategies how companies can react: hands-off strategy (price war against counterfeiters), prosecuting strategy, withdrawal strategy, and warning strategy.

Harvey and Ronkainen (1985) examine the supply side of counterfeit markets by distinguishing different counterfeiting strategies. The authors conclude that increasing company security is a

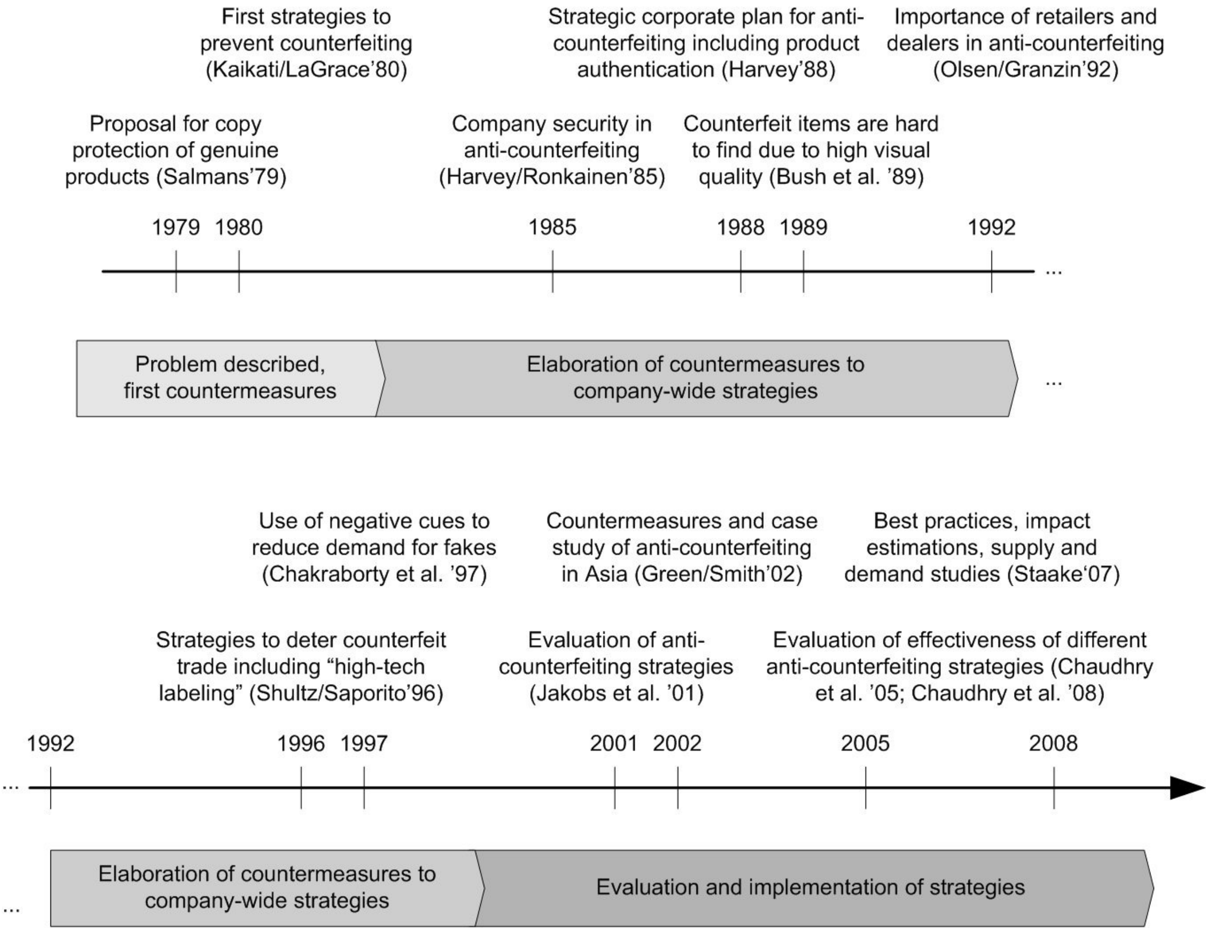

First strategies to prevent counterfeiting (Kaikati/LaGrace'80)
Strategic corporate plan for anti-counterfeiting including product authentication (Harvey'88)
Importance of retailers and dealers in anti-counterfeiting (Olsen/Granzin'92)
Proposal for copy protection of genuine products (Salmans'79)
Company security in anti-counterfeiting (Harvey/Ronkainen'85)
Counterfeit items are hard to find due to high visual quality (Bush et al. '89)
1979
1980
1985
1988
1989
1992
...
Problem described, first countermeasures
Elaboration of countermeasures to company-wide strategies
...
Use of negative cues to reduce demand for fakes (Chakraborty et al. '97)
Countermeasures and case study of anti-counterfeiting in Asia (Green/Smith'02)
Best practices, impact estimations, supply and demand studies (Staake'07)
Strategies to deter counterfeit trade including "high-tech labeling" (Shultz/Saporito'96)
Evaluation of anti-counterfeiting strategies (Jakobs et al. '01)
Evaluation of effectiveness of different anti-counterfeiting strategies (Chaudhry et al. '05; Chaudhry et al. '08)
1992
1996
1997
2001
2002
2005
2008
...
...
Elaboration of countermeasures to company-wide strategies
Evaluation and implementation of strategies

Figure III-1: *Time line of chosen scholarly contributions on anti-counterfeiting*

viable countermeasure against all of counterfeiting strategies. The article also reviews reported cases where counterfeit products (e.g. pacemakers and medicines) have lead to health and security hazards.

Grossman and Shapiro (1988a) discuss product counterfeiting and model the effect of quality and price variations on demand for counterfeits. The authors point out that "*[t]rade in counterfeit products is reaching epidemic proportions*" and that it affects a wide range of consumer and industrial goods. Furthermore, the authors make a difference between deceptive and non-deceptive counterfeiting and discuss the benefits of stricter border inspection policies. The authors also refer to early work of Salmans (1979) about using technical countermeasures to make trademarked products copy-proof against counterfeiters. In another article Grossman and Shapiro (1988b) investigate the positive effects of counterfeiting with respect to the availability of cheaper products to the consumers and analyze policies to combat counterfeiting.

Harvey (1988) proposes a strategic corporate plan to address counterfeiting involving several functions including research and development, distribution networkers, product promoters, legal staff, and investigative team, among others. Harvey promots the collaboration of different roles within a company for effective reactions and suggests that product authentication is one important part of an overall anti-counterfeiting strategy.

Bush et al. (1989) review the negative effects of counterfeiting and discuss possible countermeasures. Like Grossman and Shapiro (1988a) the authors argue that product counterfeiting affects a large variety of different kinds of products. The discussed countermeasures include legal remedies and cooperation through anti-counterfeiting associations, product and packaging changes to distinguish counterfeit products, raising public awareness, and channel monitoring. Moreover, Bush et al. (1989) report results of a survey study suggesting that end-users and channel members have difficulties in detecting counterfeits based on their visual quality. These results represent early evidence for the need of technical anti-counterfeiting measures.

Olsen and Granzin (1992) argue that dealers and retailers—not manufacturers—are in a critical position to engage in countermeasures against counterfeiting. The authors show that the most important factors that influence how willingly channel members assist manufacturers in anti-counterfeiting are salience, perceived seriousness of the problem, and internal acceptance of responsibility. In another article Olsen and Granzin (1993) show that a manufacturer can engender cooperativeness of channel members by nurturing satisfaction and dependence in manufacturer-dealer relationships. Furthermore, management practices that induce higher satisfaction and dependence but lower conflict and control will enhance a manufacturer's ability to gain the help of retailers. In particular, need for senior management's commitment to supply chain security is required in order to gain distributors' assistance.

Shultz and Saporito (1996) analyze the conditions for brand protection focusing on two dimensions: WTO commitment—the extent to which a country is committed to the provisions outlined by WTO agreements, such as TRIPS (cf. subsection II.1)—and product differentiation. The authors propose ten often-cited strategies to deter counterfeit trade in different conditions including: ”do nothing”, ”co-opt offenders”, ”educate stakeholders at the source”, ”don't despise, advertise”, ”investigation and surveillance”, ”high-tech labeling”, ”create a moving target”, ”legislation”, ”coalitions”, and ”cede the industry”. Besides outlining these strategies, however, the article provides no real guidance on how to operationalize them.

Chaudhry and Walch (1996) investigate the legal framework of intellectual property rights and review different anti-counterfeiting strategies with the focus on labeling techniques. The authors conclude that legal remedies have been largely meaningless so far due to lacking enforcement by national governments, and identify security and usability-related shortcomings in what they call anti-counterfeiting labeling tactics.

Chakraborty et al. (1997) examine means of dissuading consumers from knowingly purchasing counterfeit products (non-deceptive counterfeiting). The findings of the presented empirical analysis suggest that by reinforcing the consumers' negative beliefs about counterfeit products brand owners can negatively impact consumers' intentions to purchase them. Such negative beliefs include primarily lower quality and the country of origin of counterfeit products.

Jacobs et al. (2001) discuss different facets of counterfeiting and illicit trade and explore and evaluate different anti-counterfeiting strategies. The authors suggest that proactive methods such as making the product label and packaging difficult to copy as well as proactive marketing may be the most powerful solutions, but provide no empirical evidence to support these claims. Moreover, the authors do not provide strong arguments for or against either strategy. The authors emphasize the role of cost-benefit analysis in a company's anti-counterfeiting strategy, but provide no guidance for conducting it.

Green and Smith (2002) present a detailed case of a major alcoholic beverage producer fighting well-established large-scale counterfeiting in Thailand. The company's anti-counterfeiting strategy consists of identification of illicit channel members, minimizing the risk to the ongoing business, converting counterfeit operators into legitimate businesses, and increasing penalties associated with counterfeiting. The authors report that substantial and long-term execution of this strategy eliminated the problem, though the case raised questions about employee safety and companies' ethical responsibilities.

Hung (2003) examines product counterfeiting in China that is the world's biggest manufacturer of counterfeit products with an estimated 10-20% market share of counterfeit goods sold inside the country. The author analyses the contributing factors behind the status quo and evaluates the profit margins of counterfeit producers, concluding that product counterfeiting is so widespread and deep-rooted in China that it is unlikely to subside in the near future, despite WTO treaties and foreign pressure.

Chaudhry et al. (2005) address the questions of how managers can conceptualize the intellectual property environment and how such environments affect market entry decisions, and present frequently used anti-counterfeiting measures. The authors propose a framework to debate how effective different tactics are in the host country markets, but present no empirical study that instantiates this framework. In another article, Chaudhry (2006) reviews recent trade initiatives against product counterfeiting and piracy. The author points out that published studies provide very little insight into whether anti-counterfeiting tactics are effective or frequently used by firms and concludes that more research is required on how different anti-counterfeiting tactics decrease either the supply or demand of fake products.

Staake (2007) reports extensive studies that provide new insights into the general understanding of supply, demand, and impact of counterfeiting, contributing to the design of anti-counterfeiting strategies. He formalizes the notions of licit and illicit supply chains (cf. Fig. III-2) and provides calculation models for the market share of counterfeit articles, the magnitude of the substitution effect—the extent to which counterfeit articles displace genuine articles—and the impact on reputation and brand value. In addition, the author identifies empirically five categories of counterfeit producers including: "disaggregators" who produce counterfeit goods with low visual quality (hence disasggregating the brand and the product), "imitators" who produce counterfeit articles with high visual quality, "fraudsters" who produce counterfeits with high visual quality but low functional quality, "desperados" who produce low quality products likely to severely endanger their user or consumer, and "counterfeit smugglers" who produce

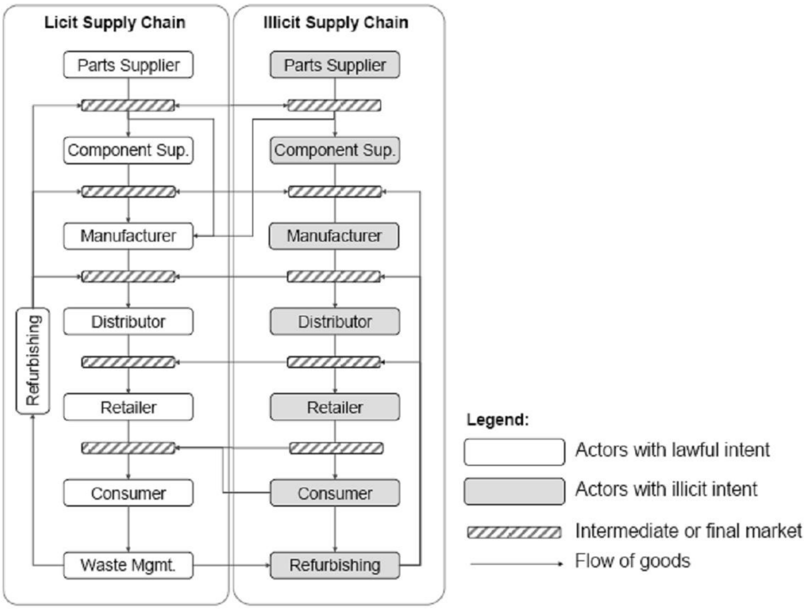


Figure III-2: *The concurrence of the licit and illicit market (Staake, 2007)*

counterfeit products of high visual and functional quality and medium complexity. Staake also investigates the best practices in anti-counterfeiting with a rigorous benchmarking study and outlines a technical solution approach based on RFID.

Chaudhry et al. (2008) evaluate the efficacy of different anti-counterfeiting tactics based on interviews with managers of affected companies. The interviewed managers state that registering of trademarks and patents, encouraging distributors to notify manufacturer, and educating own employees and channel members are the most effective countermeasures. However, the study is conducted with a relative small number of responses (16) and it has a very small response rate (less than 1.6%). Furthermore, due to a shortcoming in the questionnaire design, infrequent use of a countermeasure contributes to inefficiency, which limits the accuracy of the results. Despite these limitations, the study provides meaningful empirical evidence of the importance of communication and collaboration within the distribution channel.

This reviewed stream of scholarly contributions aims at providing guidance for practitioners who define anti-counterfeiting strategies. Though such guidance is partially provided, the contributions are mostly limited to listing what possible countermeasures are without analyzing their efficiency and effectiveness in depth. This research gap has also been found by Staake et al. (2009). Regarding the research question of this thesis (cf. subsection I.3.1), the related work on anti-counterfeiting strategies does not answer in which supply chain locations the authentication technology should be used, nor does it describe the pros and cons of different checking policies (e.g. check all products, check only suspicious products etc.).

Table III-1: *Summary of scholarly contributions on anti-counterfeiting strategies*

Publication	Contribution
Salmans (1979)	Make brand-name products copy-proof
Kaikati and LaGarce (1980)	Hands-off strategy, prosecuting strategy, withdrawal strategy, and warning strategy
Harvey and Ronkainen (1985)	Legal countermeasures, communication, authentication technology
Grossman and Shapiro (1988a)	Border inspection policies and disposition of confiscated counterfeit goods
Grossman and Shapiro (1988b)	Enforcement policy that increases the likelihood of confiscation and imposition of a tariff on low-quality imports
Harvey (1988)	Strategic corporate plan involving most functions e.g. marketing, R&D, lawyers, investigators, counterfeit prevention task force, etc.
Bush et al. (1989)	Legal actions, product and packaging changes, public awareness, channel monitoring
Olsen and Granzin (1992)	Cooperation in marketing channels
Olsen and Granzin (1993)	Cooperation in marketing channels
Shultz and Saporito (1996)	Ten strategies: ”do nothing”, ”co-opt offenders”, ”educate stakeholders at the source”, ”don’t despise, advertise”, ”investigation and surveillance”, ”high-tech labeling”, ”create a moving target”, ”legislation”, ”coalitions”, and ”cede the industry”
Chaudhry and Walch (1996)	Review of anti-counterfeiting strategies and labeling tactics
Chakraborty et al. (1997)	Reducing consumer demand for counterfeits through negative cues
Jacobs et al. (2001)	Communication, legal actions, governmental involvement, direct contact (remove counterfeit goods from shops without bureaucratic formality), labeling, proactive marketing, and piracy as promotion
Green and Smith (2002)	Identification of illicit channel members, minimizing the risk to the ongoing business, converting counterfeit operators into legitimate businesses, and increasing penalties associated with counterfeiting
Hung (2003)	IPR protection in general, government actions
Chaudhry et al. (2005)	Various IPR actions targeted at consumers, governments, distribution channels, international organizations, and pirates
Chaudhry (2006)	Trade initiatives against counterfeiting
Staake (2007)	Technical countermeasures based on RFID
Chaudhry et al. (2008)	Interviews to evaluate various countermeasures including e.g. register trademarks/patents, encourage distributors to notify manufacturer, educate employees about counterfeit goods, educate channel members etc.

III.2 Research on Level of Security

Lord Kelvin said that when you can measure what you are speaking about, you know something about it[1]. Applied to security, this means that being able to evaluate the level of security of countermeasures is a prerequisite for managing them. Moreover, the need of measuring security is not only academic but there is a market need for evaluation of the level of security of commercial products; if consumers and end-user companies are not able to understand and compare the benefits and value of security, they are also not willing to pay for it (Anderson, 2001b; Schechter, 2002).

This subsection reviews how related work addresses evaluation of the level of security in IT systems. In this context, level of security refers to the amount of protection provided to the protected asset against the assumed threat. Since intuition suggests that the level of security can be zero or higher, an ideal metric for the level of security should be on a ratio scale[2] and not on a nominal scale[3].

Related work on computer security risk modeling considers how security measures decrease the exposure to security risks. Hoo (2000) provides a comprehensive review of this research. The roots of these efforts are in the concept of Annual Loss Expectancy (ALE) that is the frequency of security incidents times the consequences that could result from each incident (FIPS, 1979). To give well-grounded estimates of the level of protection, however, ALE and similar risk modeling approaches require impractically large amounts of empirical data. Furthermore, risk modeling approaches do not provide insights to the direct and deterrent effects of security since they only consider the overall effect of security in terms of the number of materialized threats.

There exists a base of scholarly articles and papers that concentrates on examining how to provide security in an abstract and general level. Perhaps most notably, Bruce Schneier argues that security is not a product but a process and it consists of three steps: prevention, detection, and response (Schneier, 2000, 2003) (cf. Fig. III-3). On the one hand, Schneier regards security processes not as a replacement for security products but as a way of using them, and on the other hand as a way of managing the involved risks, as opposite to trying to avoid the threats. Arguing along the same lines, Bishop (2003) states that the level of a security of a system is ultimately defined by its security policy and security mechanisms, or in other words, how the security measures are used in practice. For what comes to the level of security, Schneier's model suggests that the final level of security depends on the output of the overall process of security, but the author does not present a way to quantify it.

Schechter (2004) argues that for any given threat, a system is only as strong as it is difficult for

[1] ”*I often say that when you can measure what you are speaking about, and express it in numbers, you know something about it; but when you cannot measure it, when you cannot express it in numbers, your knowledge is of a meagre and unsatisfactory kind*” (Lord Kelvin, 1883)

[2] On a ration scale, a certain distance along the scale means the same thing no matter where on the scale you are and zero represents the absence of the thing being measured (e.g. 0,1,2,...)

[3] A nominal scale is in essence a list of categories to which objects can be classified (e.g. low, medium, high)

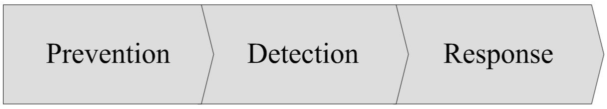


Figure III-3: *The process of security according to Schneier (2003)*

an adversary to succeed in attacking it in terms of time, effort, and other resources required to bypass the safeguards. The author quantifies security through *cost-to-break* which he defines as the *lowest cost to detect and exploit vulnerability in the system* (Schechter, 2002). A practical benefit of cost-to-break is that it allows one to compare the level of security to the value of the protected asset—and when it is more than the financial benefit of a successful attack the system can be considered secure from financially motivated adversaries (who know how much the cost-to-break is). However, one of the difficulties in measuring cost-to-break—and the level of security in general—is that it depends on the adversaries' costs, and also they are not likely to know themselves how much time and resources they would need.

To overcome the above mentioned evaluation problems, Schechter (2004) proposes to evaluate the cost-to-break as the market price to acquire a vulnerability. A market for vulnerabilities was originally proposed by Camp and Wolfram (2000) as an instrument for pricing security and for systematic testing of IT security. An upper bound for cost-to-break could be estimated by offering a reward for the first report of a vulnerability with an exploit, and a lower bound by offering a reward for each and every unique security vulnerability reported, and repairing each one until the reports cease. RSA Security is responsible for one of the earliest attempts to measure cost-to-break by economic means; between 1991 and 2007 the company offered cash rewards for breaking the security of the keys used by its cryptosystem[4]. One downside with the market-based valuation approaches is that comparing the consequences of vulnerabilities in different types of products is difficult (Schechter, 2002).

Schechter and Smith (2003) come up with further metrics for security while examining how much security is enough to stop a thief in the field of computer and information networks. The authors define an economic threat model that assumes an adversary who seeks for financial benefit through single thefts and repeated thefts. The authors show that increasing the probability to detect and patch vulnerabilities has an important decreasing effect on the expected utility of serial thefts; by sharing information on vulnerabilities, companies can increase the chances of detecting serial thieves and thus protect each other from adversaries seeking financial gain.

Schechter and Smith formalize the notions of *serial theft*, where the adversary exploits a single vulnerability one time after another until he is caught or the vulnerability is patched, and *parallel theft*, where the same vulnerability is exploited simultaneously in multiple target systems. The expectation values of a single exploit (E_1) and a serial theft (E_s) are given as follows::

[4] RSA Security (2009). RSA Factoring Challenge, http://www.rsa.com/rsalabs/node.asp?id=2091

$$E_1 = P_s \cdot l - P_c \cdot F \tag{III-1}$$

$$E_s = \frac{P_s \cdot l - P_c \cdot F}{P_d} \tag{III-2}$$

In these formulas P_s is the probability that a single exploit succeeds, l is the value of the loot (i.e. the financial gain from one successful theft), P_c is the probability that the thief is detected, caught and punished when he attempts to exploit the vulnerability, F is the fine that has to be paid when punished, and P_d is the probability that the vulnerability is patched after an exploitation attempt. Moreover, P_s represents the direct effect of security (e.g. attack does not succeed) and E_1/E_s characterizes the deterrent effect of security (e.g. attack does not pay off), but this does not consider the cost-to-break.

Schechter and Smith (2003) also expand Schneier's process of security by taking into account threat modeling, determination of security requirements, and measuring the achieved level of security. The result is an iterative process for securing a system, illustrated in Fig. III-4. In another paper, Schechter (2005) emphasizes the importance of the deterrent effect of security as an important part of its overall impact. The author argues that since a burglars' risk is increased by increasing the probability of getting caught, security systems that provide deterrents are more likely to be effective.

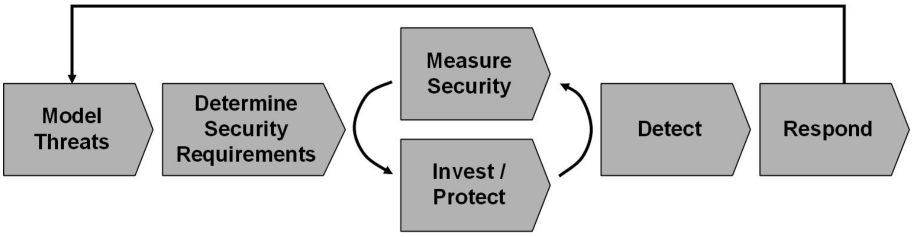


Figure III-4: *The iterative process of securing a system (Schechter and Smith, 2003)*

Sandhu (2003) approaches the problem of finding the right level of security by proposing that the goal in security design should be to achieve *good enough security*, but no more than that. According to the author, security goals are set too high in the academic mind setting to be effective in practice, and the tradeoffs of security, most importantly those with cost, will dominate (cf. Fig. III-5). Therefore the design should allow some margin for security incidents to work well in practice.

Sandhu exemplifies his reasoning with on-line banking, on-line trading, automatic teller machines (ATMs), and GSM phones which all provide sufficient protection for the common users but are not flawless. The author further remarks that these systems' security success is largely unrecognized by the security community. Even though in many cases good enough is achievable at a pretty low threshold, determining how much is good enough is hard, partly because a changing environment makes good enough a moving target.

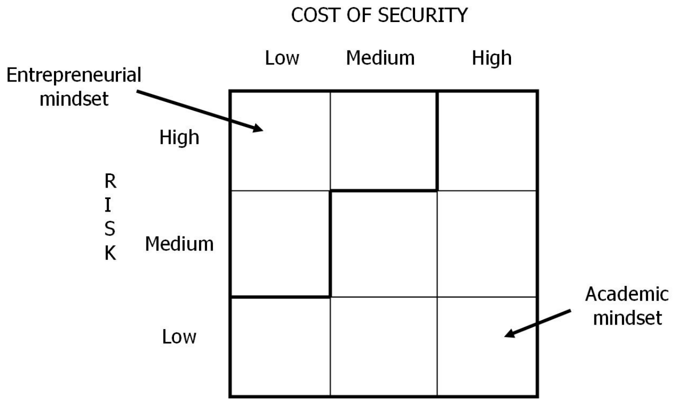


Figure III-5: *Good enough security (Sandhu, 2003)*

Sandhu's paradigm of good enough security is echoed by Schneier (2000) who argues that frauds in the credit card industry or shoplifting in the retail industry do not necessarily mean that the corresponding security measures are completely flawed since in practice security measures do not need to be perfect.

Review of related work on level of security suggests that the level of security is the outcome of the overall process of security which includes both the strength of the security measures and they are used in practice. As a result, multiple metrics are needed. On the one hand, cost-to-break captures the adversary's effort needed to bypass or break a protective measure, but evaluating this metric is not easy and it might require a market-based approach. On the other hand, the probability of detecting an adversary and the related risk of punishment define the deterrent effect of security and for how long a vulnerability can be exploited without detection. In particular, the econometric models of Schechter and Smith (2003) provide very good basis for quantifying the complete process of security in anti-counterfeiting, but these models still need to be extended to take into account the cost-to-break and a counterfeiter's different options (do not forge the security feature, only imitate the security feature, forge the security feature).

Table III-2: *Summary of scholarly contributions on level of security*

Publication	Contribution
FIPS (1979)	Fundamentals of basic computer security risk modeling through the introduction of Annual Loss Expectancy (ALE) concept
Hoo (2000)	Review and analysis of computer security risk modeling research, proposal of new models
Schneier (2000)	Security is a process, not a product, and it applies security measures to manage the involved risks
Camp and Wolfram (2000)	First proposal for a market of vulnerabilities for pricing security and detecting vulnerabilities
Anderson (2001b)	Arguments for a market need for evaluating the level of security
Schechter (2002)	Arguments for evaluating the level of security, formalization of the term cost-to-break (CTB)
Bishop (2003)	Level of security is defined by practice, not theory
Schechter and Smith (2003)	Study of economic threat models to answer how much security is enough to stop a financially motivated thief
Sandhu (2003)	Paradigm of ”good enough security” which states that in the level of security should be good enough, but no more
Schechter (2004)	Detailed analysis of measuring security strength and cost-to-break, proposal to use regression models to estimate CTB
Schechter (2005)	Arguments on the importance of the deterrent effect of security regarding the overall impact of security measures

III.3 Research on Economics of Security

In addition to technical aspects, security encompasses behavioral aspects of individuals and organizations. These aspects are covered by research on economics of security which spun off from information security research in the end of 1990s, and they help explain the link between security of a technical anti-counterfeiting system and the behavior of counterfeiters. Overall, these contributions illustrate the relevance of economic analysis in security applications.

Becker (1968) applied pioneering economic analysis to crime and punishments as a part of his Nobel prize-winning work about the economic way of looking at life. Becker investigated the optimal amount of public expenditures to fighting crimes and optimal punishments that minimize the overall social costs of crime, enforcement, and punishment. Following a prevention, detection, and response paradigm—which was later denoted as the process of security (cf. Fig. III-3)—Becker modeled the expected utility of a crime as the expected value of the crime plus the expected punishment. In particular, the author assumed that offenders are more deterred by the probability of conviction than by the punishment when convicted. Overall, Becker's main contribution was to demonstrate that optimal policies to combat illegal behavior are closely linked to optimal allocation of resources.

Recent work on economics of security argues that security failure is caused at least as often by misaligned incentives as by bad design. Anderson (1993) observes that though UK banks had laxer liability policies regarding ATM-frauds than banks in the USA, they still spent more on security and suffered more fraud than their American counterparts. This was explained by UK banks not taking the problem seriously, leading to an epidemic of fraud.

Varian (2000) discusses misaligned incentives in the anti-virus software market. The author notes that people did not spend as much on protecting their computers as they logically should have, partly because they do not have strong incentives to pay for a software that prevents hackers from using their computers to launch denial of service attacks against large corporations.

Anderson (2001b) analyzes the reasons why the economics of the software industry have not favored secure products. Owing to the combination of high fixed costs and low marginal costs, network externalities, and technical lock-in effects of the software market (Shapiro and Varian, 1998), the optimal competitive strategy focuses on the speed to get to the market rather than on the time-consuming process of writing and testing more secure code. The philosophy of ”we'll ship it on Tuesday and get it right by version 3” is thus a rational response to the market conditions—and the cause of many security incidents.

In addition to the aforementioned market conditions for misaligned incentives, Odlyzko (2003) argues that may players in security markets even have the interest of passing on the costs of security to others, such as from manufacturing companies to their customers, further incrementing the suboptimal allocation of risks.

Anderson (Anderson, 2001b; Anderson and Moore, 2006, 2007) argues that the secure software market is a ”market for lemons”. In a Nobel prize-winning work, economist Akerlof (1970) employed the used car market as a metaphor for a market with asymmetric information. He imagined a town in which good used cars (worth \$2000 each) are for sale, along with the same number of ”lemons” (worth \$1000 each). The sellers know the difference but the buyers do not. Akerlof investigated what the market-clearing price will be. One might initially think \$1500, but at that price no one with a good car will offer it for sale, so the market price will quickly end up near \$1000. Because buyers are unwilling to pay a premium for quality they cannot measure, only low-quality used cars are available for sale.

According to Anderson, the software market suffers from the same information asymmetry; vendors may make claims about the security of their products but buyers have no reason to trust them since they have no means of verifying the claims. In many cases, even the vendor does not know how secure his/her software is. So buyers have no reason to pay more for protection, and vendors are disinclined to invest in it under a price pressure. The same view is also shared by Schneier (2007).

Overall, Anderson argues that a significant difficulty in optimal development of security technology is that economic implications should be integrated into technical designs. If a security technology requires that the party with the least risk makes the greatest investment, that system will fail to be widely adopted because liability should be assigned to the party that can best manage the risk. Anderson (2001b) concludes that information security is currently about power and money, about raising barriers to trade, segmenting markets, and differentiating products.

Security is also characterized by externalities—that is, cases where individuals' or companies' actions have economic side effects on others for which there is no compensation (e.g. Anderson, 2001b; Anderson and Moore, 2006, 2007). These externalities can both increase and decrease the level of security of other systems. Positive externalities are empirically illustrated by Ayres and Levitt (1998) who analyze a car-theft prevention system. The authors found out that once a threshold of car owners had installed the system in a city, auto theft plummeted in the whole city as the stolen car trade become too risky for thieves. These externalities have an impact on the decision of other actors. For instance, airlines may decide not to screen luggage transferred from other carriers that are believed to be careful with security (Anderson and Moore, 2006).

Positive security externalities can also have discouraging effects. Kunreuther and Heal (2003) discuss interdependent security and note that an individual taking protective measures creates positive externalities for others that in turn may discourage them from investment in security.

Camp and Wolfram (2000) analyze information security vulnerabilities as negative externalities, like air pollution: someone who connects an insecure PC to the Internet does not face the full economic costs of that, any more than someone burning a coal fire. Varian (2003) argues that system reliability often depends on the effort of many individuals and formalized three cases—where performance depends on the minimum effort, the best effort, or the sum-of-efforts. These three cases also the ways how externalities affect the achieved level of security. Externalities of security are also discussed in more popular literature by Schneier (2003).

In addition to the aforementioned microeconomic studies on security there are various studies on the investment and management aspects of security technologies. These include approaches based on traditional risk or decision analysis framework where idea is to identify the potential risks, expected losses and their likelihoods, and compute the expected losses (e.g. Finne, 1998; Buzzard, 1999; Hoo, 2000; Longstaff et al., 2000). Though the cost of security technology can be often accurately estimated, it is rarely possible to use completely rational cost-benefit analysis since estimating the expected benefits would require users to have information on precise potential losses from security breaches and the probability of such breaches. Though these approaches are systematic and well-grounded, they require large amounts of data for accurate estimates of threat likelihoods, and provide little guidance to managers about how much and how to invest in security.

Gordon and Loeb (2002) presented a methodologically rigorous economic model to determine the optimal amount to invest to protect a given set of information based on risk analysis. Investments in security are assumed to decrease the probability that an occurred threat is successful according to the law of diminishing returns. The analysis suggest that a firm may often prefer to protect those information sets with middling vulnerability, rather than the most vulnerable (as that may be too expensive), and to maximize the expected benefit, a firm might only spend a small fraction of the expected loss. However, since the model's parameters are hard to evaluate in practice and it does not take into account the deterrent effect of security, the contribution of this work is mostly theoretical.

Geer et al. (2003) argue that information security managers should rely on quantifiable metrics, including: how secure the firm is, is the firm better off than last year, how the firm compares to the peers, is the firm spending right amount of money on security, and what the risk transfer options are. In another paper, Geer (2005) argues that security investment should be measured through a return on security investment (ROSI) analysis. Cavusoglu et al. (2004) propose a quantitative model of the costs and benefits of securing an IT system against internal and external hackers. A model based on game theory is used to estimate the utility of an information breach for a hacker. This approach can be used to optimize certain parameter values, such as how often alarms from the intrusion detection system should be manually inspected. The need for formal methods for security investment analysis is also echoed by practitioners; an empirical study of Gordon and Loeb (2006) demonstrates that security managers apparently do use some form of economic analysis in budgeting for information security, in some cases even with a formal net present value analysis.

Review of related work on economics of security reveals security also needs to take into account behavioral aspects of individuals and corporations including misaligned incentives of different actors, transparency of the level of security of commercial products to avoid a market for lemons, and positive and negative externalities. In addition, many authors argue for the use of quantitative metrics to support investment decisions in security, though the optimal amount to invest in security is hard to define in practice.

Table III-3: *Summary of scholarly contributions on economics of security*

Publication	Contribution
Becker (1968)	Pioneering work on economics of crime prevention and deterrence, application of a prevention, detection, and response paradigm
Akerlof (1970)	Market for lemons, quality uncertainty caused by information asymmetry between the seller and the buyer
Anderson (1993)	Study of the relationship between misaligned incentives (liability) and ATM-frauds in the banking industry
Finne (1998)	Risk-analysis perspective to information security
Ayres and Levitt (1998)	Empirical study illustrating externalities and deterrence of a car-theft prevention system
Buzzard (1999)	Problems of knowing where to invest in computer security
Longstaff et al. (2000)	Hierarchical holographic modeling framework for computer security risk assessment
Varian (2003)	Security problems in anti-virus market resulting from poorly allocated incentives to avoid abuse
Anderson (2001b)	An economic analysis of why information security is not merely a rational risk management task, introduction of microeconomic analysis
Gordon and Loeb (2002)	Methodologically rigorous but somewhat unpractical economic model to determine the optimal amount to invest in security
Geer et al. (2003)	Risk-management approach with dependable, quantifiable metrics in information security
Odlyzko (2003)	Description of ways in which cultural factors can undermine the formal assumptions underlying many security systems
Kunreuther and Heal (2003)	Investigation of interdependent security, identification of discouraging effect of positive externalities
Varian (2003)	System reliability depends on the effort of many individuals: minimum effort, the best effort, or the sum-of-efforts
Cavusoglu et al. (2004)	A quantitative model of the costs and benefits of securing an IT system
Geer (2005)	Arguments for return on security investment analysis
Anderson and Moore (2006)	Review and overview of the economics of information security
Gordon and Loeb (2006)	Empirical study of economic security analysis within companies
Camp (2006)	An assessment of the state of economics of information security
Schneier (2007)	Security is a market for lemons
Anderson and Moore (2007)	Review of research on economics of security

III.4 Research on RFID Security

Before developing product authentication concepts for low-cost RFID, existing RFID authentication concepts and their hardware requirements are reviewed. This review helps answer what are the existing and upcoming approaches to authenticate products tagged with low-cost RFID tags, and where further contributions are still needed.

RFID technology's ability to identify single products without a line of sight has not only enabled new Auto-ID applications—it has also evoked an increased need for security. RFID is used in many applications where cloning and spoofing of tags could be financially lucrative for crackers and criminals while being severely harmful to licit companies, such as access control, ticketing, mobile payment, and anti-counterfeiting. Furthermore, the potential losses are amplified by the high level of automation of RFID. Therefore security is not only added value that RFID can provide vis-a-vis older Auto-ID technologies—it is also a requirement.

RFID security measures address various threats and attacks. The following attacks are gathered from a survey article of Ari Juels who pioneered research on RFID security (Juels, 2006).

- *Clandestine scanning* (sometimes *rogue scanning*) refers to an adversary scanning a legitimate tag, which can lead to *clandestine tracking*.
- *Eavesdropping* refers to an adversary trying to capture the exchange of information between a legitimate reader and tag.
- *Skimming* refers to an adversary reading the contents of a legitimate tag without the consent and permission of the tag's owner.
- *Spoofing* refers to an adversary forging a legitimate tag and masquerading (impersonating) as the legitimate tag to deceive a legitimate reader.
- *Replay* refers to an adversary capturing and repeating (replaying) a data transmission, for example a tag's response to a reader.
- *Denial of service* (*DoS*) refers to harming or destroying the RFID system so that it becomes unresponsive or does not function as expected, such as destroying a tag.
- *Side channel* attack refers to gaining information from the physical implementation of a crypto system, typically from timing and power analysis of a device.
- *Man-in-the-middle* attack (*MITM* or sometimes *relay* attack) refers to an adversary making independent connections with two victims (e.g. a tag and a reader) and relaying messages between them, making them believe they are talking directly to each other.

Research on RFID security primarily revolves around two problems: authenticating RFID tags and providing privacy (Juels, 2006). The former is about techniques to mitigate tag cloning and spoofing and the latter about keeping the identity, location, and belongings of consumers in secrecy, in case it is desired. This review focuses on techniques to authenticate RFID tags.

Clandestine scanning and eavesdropping are enough to copy ID numbers from legitimate tags to forged tags. Clandestine scanning using a sensitive reader equipped with a powerful antenna and output power that exceeds the legal limits can exceed the nominal read range. Kfir and Wool (2005) suggest that the clandestine read range for ISO 14443 tags can be five times higher than their nominal reading range. Once a tag is powered by a legitimate reader, a rogue reader can also eavesdrop the tag emission and capture the tag ID number for cloning. The maximum distance where a tag can be eavesdropped may be larger than the clandestine read range (Juels, 2006). Also the reader-to-tag communication can be eavesdropped, though this channel is less frequently used to transfer tag-specific information. Since the reader transmits at much higher power than the tag, eavesdropping range for the reader-to-tag channel is much greater than for the tag-to-reader channel (Weis et al., 2003).

Many cryptographic protocols have been proposed to protect tags from cloning by carefully using the tags' scarce hardware resources. The principal techniques are tag-to-reader authentication, reader-to-tag authentication, and mutual authentication that incorporates both of them. The typical approach is to have a *secret key* on the tag that cannot be directly read but that can be indirectly verified (cf. Fig. III-6). Contributions in this field aim at providing improvements to the underlying trade-offs between cost, security, and usability & performance (cf. subsection I.2.3).

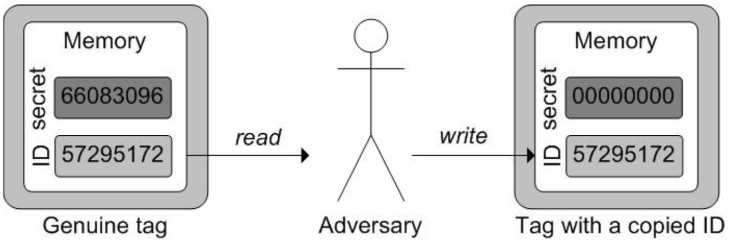


Figure III-6: *Using a secret key to mitigate the tag cloning attack*

Hash-lock of Weis et al. (2003) is one of the first cryptographic protocols for RFID. The principle behind the scheme is that tags cannot be trusted to store long-term secrets when left in isolation. The authors propose a way to lock the tag without storing the access key on the tag but only a hash of the key. The key is stored in a back-end server and can be found using the tag's meta-ID. Unlocking a tag successfully corresponds to authentication. The cloning resistance of this scheme is based only on the locked state of the tags and so the scheme is more suitable for protecting privacy. Henrici and Müller (2004) introduce a randomized version of the hash-lock scheme for increased privacy and scalability.

Avoine and Oechslin (2005) propose another hash-based protocol that provides modified identifiers for improved privacy and that can be applied for authentication. The authors solve scalability issues of the privacy-enhancing scheme of Ohkubo et al. (2003) by introducing a time-memory trade-off. In addition, hash-based RFID protocols for mutual authentication are proposed by Lee et al. (2005), Choi et al. (2005), and Lee et al. (2006). These protocols rely on synchronized secrets residing on the tag and back-end server and they can provide untraceability while increasing the workload of the back-end servers.

The hash-based protocols were developed based on the assumption that a hash algorithm is cheaper to implement on an RFID tag than symmetric or asymmetric ciphers. However, this assumption is proved wrong by Feldhofer (2008) who investigates the power consumption, chip area, and number of clock cycles required by different cryptographic primitives. The results of this study are illustrated in Fig. III-7. For instance, comparison of the hash functions SHA-256 and SHA-1 with the block cipher AES shows that they require more than twice as much chip area. The author argues that this is due to the high number of registers required for the internal state. Also the power consumption in case of SHA-256, which has the same security level, is nearly twice as high while requiring a similar amount of clock cycles.

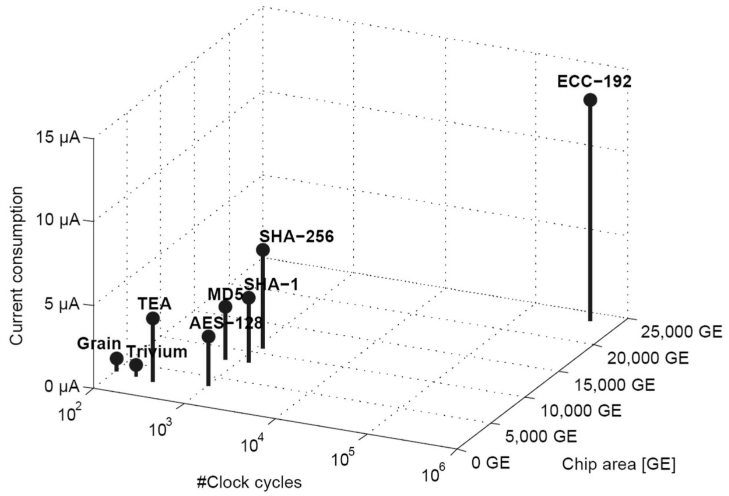


Figure III-7: *Comparison of crypto primitives (Feldhofer, 2008)*

Pearson (2005) proposes RFID-based authentication techniques for the pharmaceutical industry. The model bases on authenticating the products through digital signatures written on tags. By using transponder ID number and a public key, the tag can be linked to the signer of the data in a provable way. To improve the traceability of products, tag memory is also used to store chain-of-custody events.

Juels and Pappu (2003) present an approach to increase tracing and forgery resistance of RFID-enabled banknotes by using digital signatures. The approach uses re-encryption to avoid static identifiers and optical data on the banknote to bind the RFID tag and the paper. Authentication is performed by verifying that the data on the tag is signed with a valid public key. In order to the increase cloning resistance, the authors suggest including some distinctive characteristics of the physical media into the signature (i.e. physical fingerprint of the banknote) and verifying the validity of these characteristics as a part of the authentication process. Zhang and King (2005) enhance the protocol by addressing some integrity issues.

Juels (2004) discusses minimalist cryptography based authentication and proposed a tracking-resistant pseudonym-throttling scheme. The minimalist model assumes a cap on the number of times an adversary can scan a given tag or try to spoof a valid reader. The proposed mutual authentication protocol bases on a list of pseudonyms and keys residing on tag and on back-end server. The protocol needs additional memory on tag and uses a way to update the tag's pseudonym list using one-time pads to resist cloning and eavesdropping. However, the communication cost is relatively high because of the tag data updates.

Juels (2005) proposes another low-cost authentication where the read-protected 32-bit kill passwords of EPC Class-1 Gen-2 tags are used to implement an ad-hoc tag authentication protocol. The protocol bases on the fact that even though the EPC of a transponder can be skimmed, the kill-password remains secret. Cloned tags can be found by testing, without killing the tag, if the kill password matches the original one stored in a database. Furthermore, the protocol supports for mutual authentication. Koscher et al. (2008) demonstrate that implementation of this technique is indeed feasible in deployed tags, but presents some delicate technical challenges.

Also the unique factory programmed read-only transponder ID (TID) number (cf. subsection II.3.3) can increase the cloning resistance of EPC Class-1 Gen-2 tags (EPCglobal Inc., 2005a). TID-scheme is not cryptographically secure but it represents a practical barrier, requiring a chip manufacturer to knowingly write copied TID numbers on their chips or the use of custom-built tags. Koscher et al. (2008) analyze the weaknesses of TID-based tag authentication by discussing the threat of emulating genuine tags with publicly available devices, concluding that the security of the serialized TID-scheme is overly optimistic in the long term. However, the authors do not quantify their estimates for the cost-to-break of the TID-scheme.

Vajda and Buttyán (2003) discuss lightweight authentication protocols for low-cost tags. The proposed set of challenge-response protocols includes simple XOR (exclusive or) encryption with secret keys. Also complex encryption like RSA was proposed, it is not feasible for standard low-cost tags. The cryptographic problem with keys being static in XOR encryption is addressed by re-keying schemes that make use of keys from multiple previous protocol runs.

Juels and Weis (2005) introduce an approach for low-cost authentication based on the work of Hopper and Blum (HB) (Hopper and Blum, 2000). The proposed HB+ protocol makes use of the hardness assumption of statistical ”learning parity with noise” (LPN) problem and can be implemented on low-cost tags, as it only requires bitwise AND and XOR operations and one random ”noise bit” from the tag. The security of HB+ against active adversaries has been discussed in the RFID security community (e.g. Katz and Smith, 2006; Katz and Sun Shin, 2006). The first version of the original protocol (Juels and Weis, 2005) was found to be vulnerable against a realistic active attack (Gilbert et al., 2005). Since then, various proposals to address the security issues have emerged (Piramuthu, 2006; Bringer et al., 2006; Leng et al., 2008; Bringer and Chabanne, 2008; Yoon, 2009; Frumkin and Shamir, 2009).

Tsudik (2006) proposes an authentication protocol called YA-TRAP (Yet Another Trivial RFID Authentication Protocol) which provides tracking-resistant tag authentication through monotonically increasing timestamps on the tag. YA-TRAP requires a pseudo-random number generator (PRNG) from the tag and its basic version is vulnerable to a DoS attack through time stamp desynchronization between the tag and the server. The approach does not require on demand computation for the back-end as a result of a pre-computed hash-table for later tag verification, which means less load for the server than for example in the scheme of Molnar et al. (2005). Chatmon et al. (2006) propose anonymous RFID authentication protocols based on YA-TRAP that provide anonymity for authenticated tags and address some vulnerabilities of the original design, while increasing the server workload.

Dimitriou (2006) proposes a protocol that addresses privacy issues and aims at efficient identification of multiple tags. The enhanced version of the protocol also protects tags against cloning. In this approach, the tags need a PRNG and a pseudo random function for symmetric-key encryption. The protocol is efficient in terms of tag-to-reader transaction and protects the privacy by avoiding transmission of static IDs. However, since the tags share secret keys, compromising one tag may reveal information about others. In another work, Dimitriou (2005) proposes a protocol against traceability and cloning attacks based on refreshing a shared secret between tag and back-end database, requiring hash calculations and a PRNG from the tag.

Duc et al. (2006) propose communication protocol for RFID devises that supports for tag-to-reader authentication based on synchronization between tag and back-end server. The proposed scheme is tailored for EPC Class-1 Gen-2 tags so that it requires only a PRNG on the tag and pre-shared keys. The approach also takes advantage of the CRC function that is supported by Gen-2 tags. The underlying idea is to use the same PRNG with the same seed on both RFID tag and on back-end side and to use it for efficient key sharing. The encryption and decryption can then be done by XORring the messages.

Engberg et al. (2004) propose so called zero-knowledge device authentication as an answer to consumer privacy issues. In their proposal the tag must authenticate the reader before it returns any traceable identifier. The scheme is based on shared secrets and requires hash function from the tag. Also Rhee et al. (2005) propose a challenge-response protocol for users privacy. The proposed protocol does not update the tag ID and therefore can be applied in an environment with distributed databases. The protocol relies on hash calculations by the back-end database, so that the tag ID is the only necessary shared secret between the devices taking part in the authentication. Molnar and Wagner (2004) propose private authentication protocols for library RFID, where the tag and the reader can do mutual authentication without revealing their identities to adversaries. The protocols make use of PRNG residing on the tag.

Molnar et al. (2005) present another privacy enhancing scheme where the protocol takes care of emitting always a different pseudonym. In order to relate pseudonyms and real tag IDs, the authors present an entity called Trusted Center (TC) that is able to decode the tag responses and obtain the tags identity. The authors introduced term ownership transfer that refers to TC giving permissions to only readers of a certain entity to read an RFID tag.

Gao et al. (2005) propose protocols for improved security and privacy of supply chain RFID. In their proposals the tags store a list of licit readers to protect the tags against skimming and therefore need rewritable memory. Other tag requirements include PRNG and hash function. Though the protocol burdens the back-end server with some computational load, the approach is designed to be suitable for a large number of tags. Yang et al. (2005) propose a mutual authentication protocol that provides protection against replay attack and MITM attack even when the reader is not trusted and the communication channel is insecure. This protocol provides privacy protection and cloning resistance with the expense of tag's hash calculations and storing two secrets in the tag and in the back-end server.

In addition to the aforementioned protocols that are tailored for RFID tags, also standard cryptography (cf. subsection II.4.2) have been applied to RFID. Dominikus et al. (2005) discuss symmetric RFID authentication protocols in practice and presented five standard challenge-response protocols for reader, tag and mutual authentication. The design focuses on strong authentication for advanced, about $0.50 tags with available silicon area of 10,000 gates. The presented protocols use AES encryption (and decryption) on tags in such a way that energy constraints of Class-2 RFID systems are met.

Feldhofer (2003) presents a field programmable gate array (FPGA) implementation of standard symmetric two-way protocol as an extinction to the ISO/IEC 18000 standard which describes the communication of RFID tags with a reader on HF band. The author argues that standard protocols within standard communication protocols are important for security and interoperability. In another paper, Feldhofer et al. (2004) present a 128-bit minimalist design for AES that is optimized for low-resource requirements regarding low die size and power consumption. Feldhofer et al. (2005) demonstrate a silicon implementation of the minimalist AES implementation as a proof that *strong cryptography is possible with passive RFID tags*, though the implementation does not include countermeasures against side-channel attacks. The implementation occupies an area of only 0.25 mm^2 which compares roughly to 3400 gate equivalents.

Bailey and Juels (2006) concentrate on integrating common cryptographic standards into RFID by proposing techniques to create RFID tags that are compliant with the EPC Class-1 Gen-2 tags, but offer cryptographic functionality of standards like ISO 7816-4 that defines general command and response frames for challenge-response protocols. The proposed protocols make use of AES on the tag and can be used for mutual authentication. In particular, the authors define a 32 or 64 bit ”one-time password” that could be included in transmitted EPC data.

Also asymmetric encryption has been applied on RFID. Most contributions focus on Elliptic Curve Cryptography (ECC) which allows for less computationally intense encryption for resource-limited devices. Wolkerstorfer (2005) presents a new ECC architecture which show that the implementation of ECC on RFID tags seems to be viable by respecting the strict power and area constraints of tags. Kumar and Paar (2006) provide further evidence that ECC could be possible on RFID. Batina et al. (2006) describe an FPGA-based implementation of ECC demonstrating that ECC protocols could be implemented an RFID tag requiring between 8500 and 14000 gates, depending on the implementation characteristics. Finally, Hein et al. (2008) demonstrate that *ECC is ready for RFID* by presenting a hardware implementation in silicon.

Even though the reviewed authentication protocols can provide significant improvements to a tag's cloning resistance there remain many ways to attempt a tag cloning attack. The goal of these attacks is to crack the tag's secret key and they include side channel attack (e.g. Kasper et al., 2009), reverse-engineering and cryptanalysis (e.g. Bono et al., 2005; Bogdanov, 2007; Courtois et al., 2008), brute-force attack, physical attacks (e.g. Weingart, 2000), and different active attacks against the tag (e.g. Gilbert et al., 2005). In addition, shared secrets-based product authentication approaches are always vulnerable to data theft where the secret PIN codes or encryption schemes of valid tags are stolen or sold by insiders.

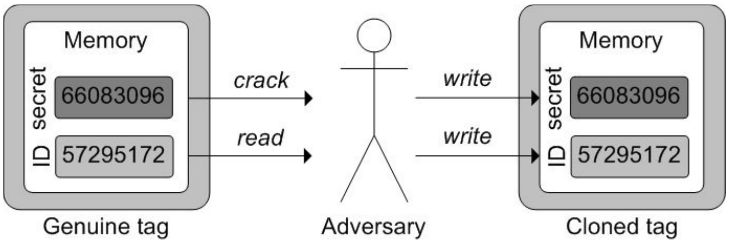


Figure III-8: *Cloning a protected tag by cracking the secret key*

Successful attacks are also conducted against RFID tags of e-passports. The security firm Riscure demonstrated that Dutch passports are vulnerable to a brute force that can be conducted in a few hours on a standard computer, allowing the attacker to read sensitive information on the chip (Witteman, 2005; Juels et al., 2005). Furthermore, it was demonstrated that the e-passport's RFID tag's secret key can be retrieved by a side channel attack and statistical analysis, allowing the attacked to clone the chip. Also shortcomings in the inspections have been reported. In 2008 Jeroen van Beek demonstrated that not all passport inspection systems check the cryptographic signature of a passport chips, opening a possibility for unnoticed tampering of e-passport data (van Beek, 2008).

Ranasinghe et al. (2004) present a way to implement challenge-response protocols on RFID tags that does not need cryptographic primitives like AES and ECC. These proposals are based on a physical unclonable function (PUF) which allows calculating unique and random responses for challenges using only some hundreds of logical gates. A possible early candidate for a PUF is proposed by Lee et al. (2004), based on natural manufacturing variations of integrated circuits. In order to make the use of eavesdropped responses infeasible, several challenge-response pairs have to be stored in a database.

Also Tuyls and Batina (2006) propose PUFs to increase tags resistance against physical and logical cloning attacks, estimating that an anti-clone tag could be built with about 5,000 logical gates. Since then, *PUF has successfully been designed and implemented on HF RFID tags* using 0.18 μ technology by Devadas et al. (2008) who argue that their implementation requires less transistors than existing low-cost AES implementations. Low-cost implementations of PUFs are also studied by Guajardo et al. (2009).

Danev et al. (2009) propose several techniques for the extraction of RFID physical-layer fingerprints—modulation shape and spectral features of the signals—based on which RFID tags could be authenticated. Tests conducted with 50 RFID smart cards of the same manufacturer and type demonstrated that the technique could correctly identify an RFID tag based on its physical-layer fingerprint with a reliability of 95.6-97.6%. Though the remaining error rates still cause many classification errors in big tag populations, the investigation shows that in principle standard RFID tags can be authenticated also by measuring their physical properties.

In addition to the above reviewed approaches that aim at making cloning of tags hard, the authentication problem can also be solved by a system that reliably detects copied tags. Takaragi et al. (2001) propose methods to check of validity of serialized ID numbers. The system should signal an alarm when it detects an alleged counterfeit chip, identification numbers transmitted at the same time from different locations, or any other predefined abnormality. Though this can detect cloned tags in certain cases, the authors do not detail how to do it in practice. Koh et al. (2003) propose a simple method to secure pharmaceutical supply chains by using an authentication server that publishes a *white list* of genuine products' ID numbers; if a product's ID number is not on that list it is not genuine.

Johnston (2005) proposes a call-in numeric token (CNT) technique that lets consumers to call to a service and tell the unique ID number (token) of their product. Though the author does not present the CNT technique for RFID-tagged products, the principle also applies to RFID. If a predefined number N of callers already have expressed the same number, the ID number is *black listed* and the service responds that the product under study is cloned; otherwise the service responds that the product is genuine. The method assumes that the genuine product is called for the first N times and all resulting inquiries result from counterfeits. This method can detect if the same ID number is used in a large number of counterfeit products but leads to less reliable results with smaller numbers of clones.

Staake et al. (2005) discuss the potential of track and trace based product authentication approach within the EPC network (cf. subsection II.3.5) and bring forth some of its vulnerabilities. The authors point out that some scenarios where the cloned transponders cannot be detected by a track and trace based plausibility check due to missing visibility. Lei et al. (2005) present a way to authenticate products by photographing and decoding pseudo-random 2D barcodes on mobile phones, but the presented system is vulnerable to cloning of the codes. Mirowski and Hartnett (2007) present an implementation of an intrusion detection system for RFID that detects cloned tags in an access control application. The developed system can detect most cloned transponders that enter the system by searching for deviations from the expected behavior, but the method is prone to false alarms.

Review of the related work on RFID security shows how modest RFID devices have given rise to a complex melange of security problems. Many cryptographic tag authentication protocols have been proposed based on low-cost primitives (e.g. variants of HB+ and YA-TRAP), symmetric cryptography (AES), or asymmetric cryptography (ECC). Also standard cryptography with AES and ECC has been demonstrated on silicon in a way that complies with the rigid chip size and energy consumption requirements of passive UHF tags, but these approaches have not yet been elaborated into market-ready products that also address side-channel attacks. In addition to cryptography, an approach based on physical unclonable functions (PUFs) has been demonstrated on HF tags and it will compete against cryptographic approaches in the future RFID security market—with an apparent cost advantage. However, since cryptographic approaches require changes in the tag hardware, the state of the art does not solve authentication of existing low-cost tags. Also security through detection of cloned tags has been discussed within the research community, though the contributions in this field are scarce. The state of the art merely outlines the related challenges and possible solutions for detection of cloned tags, without detailing feasible solutions and evaluating their the level of protection.

Table III-4: *Summary of scholarly contributions on RFID security*

Publication	Contribution
Weingart (2000)	Physical attacks against smart cards
Takaragi et al. (2001)	Methods to check of validity of serialized ID numbers
Weis et al. (2003)	Hash-lock scheme for privacy and tag authentication
Ohkubo et al. (2003)	Privacy-enhancing scheme using hash function
Juels and Pappu (2003)	Protocol to authenticate banknotes with digital signatures
Vajda and Buttyán (2003)	Lightweight authentication protocols for low-cost tags
Koh et al. (2003)	Method to secure supply chains by detecting invalid ID numbers
Feldhofer (2003)	FPGA implementation of standard symmetric authentication protocol
Henrici and Müller (2004)	Improved hash-lock scheme
Juels (2004)	Minimalist cryptography based tag authentication
Molnar and Wagner (2004)	Privacy protocols for library RFID application
Feldhofer et al. (2004)	Design for minimalist AES implementation on RFID
Ranasinghe et al. (2004)	PUF-based authentication of RFID tags
Lee et al. (2004)	Proposal for a PUF for RFID tags
Avoine and Oechslin (2005)	Improved hash-lock scheme
Lee et al. (2005)	Hash-based mutual authentication protocol
Choi et al. (2005)	Hash-based mutual authentication protocol
Pearson (2005)	Digital signature scheme for the pharmaceutical industry
Zhang and King (2005)	Enhanced banknote authentication scheme
Molnar et al. (2005)	Pseudonym protocol for RFID tag ownership transfer
Juels (2005)	Protocol based on kill passwords of EPC Gen-2 tags
Juels and Weis (2005)	Low-cost authentication protocol HB+
Dimitriou (2005)	Lightweight protocol against traceability and cloning attacks
Gilbert et al. (2005)	Active attack against HB+ protocol
Rhee et al. (2005)	Privacy protocol for distributed databases
Gao et al. (2005)	Protocols for improved security and privacy of supply chain RFID
Yang et al. (2005)	Mutual authentication protocol against replay and MITM attacks
Dominikus et al. (2005)	Design of symmetric RFID authentication protocols based on AES
Feldhofer et al. (2005)	Demonstration of an AES implementation on silicon
Wolkerstorfer (2005)	ECC implementation architecture for RFID tags

(continues)

Bono et al. (2005)	Reverse engineering and cryptanalysis against RFID
Staake et al. (2005)	Track and trace based product authentication in the EPC network
Johnston (2005)	Method to detect cloning of product ID numbers
Lei et al. (2005)	System to scan and encode 2D barcodes with a mobile phone
Witteman (2005)	Security issues of e-passports
Juels et al. (2005)	Security issues of e-passports
Lee et al. (2006)	Hash-based mutual authentication protocol
Tsudik (2006)	YA-TRAP protocol requiring a pseudo-random number generator
Chatmon et al. (2006)	Improved version of YA-TRAP protocol
Juels (2006)	A comprehensive research survey of RFID security and privacy
Katz and Smith (2006)	Security analysis of HB+ protocol
Katz and Sun Shin (2006)	Security analysis of HB+ protocol
Dimitriou (2006)	Privacy protocol based on symmetric-key encryption
Piramuthu (2006)	Improved HB+ low-cost protocol
Bringer et al. (2006)	Improved HB+ low-cost protocol
Duc et al. (2006)	Protocol based on synchronization between tag and back-end
Bailey and Juels (2006)	Integration of common cryptographic standards into RFID
Kumar and Paar (2006)	Investigation of ECC on RFID tags
Batina et al. (2006)	FPGA-based implementation of ECC
Tuyls and Batina (2006)	Study of PUF-based authentication of RFID tags
Mirowski and Hartnett (2007)	Intrusion detection system for RFID access control application
Koscher et al. (2008)	Review investigation of EPC tag security
Leng et al. (2008)	Improved HB+ low-cost protocol
Bringer and Chabanne (2008)	Improved HB+ low-cost protocol
Hein et al. (2008)	Implementation of ECC for RFID tags in silicon
Devadas et al. (2008)	Hardware implementation of PUF on an HF RFID tag
Yoon (2009)	Improved HB+ low-cost protocol
Frumkin and Shamir (2009)	Improved HB+ low-cost protocol
Kasper et al. (2009)	Side channel attacks against RFID
Danev et al. (2009)	Tag authentication based on physical-layer fingerprints
Guajardo et al. (2009)	Study of low-cost implementations of PUFs

IV The Process of Securing a Supply Chain with RFID

The related work on security suggests that security is not a product but a process that combines preventive, detective and reactive countermeasures (Schneier, 2000, 2003). This view is also echoed by the notion of *layered security*, or *in-depth defense*, where security is provided not by one but by several measures that sequentially come into play as the adversary approaches his or her goal. However, this process view is not shared by the managerial research on anti-counterfeiting strategies (cf. subsection III.1) that approaches technical, organizational, and legal countermeasures as distinct silos, often separated by the organizational boundaries of the involved functions within affected enterprises.

To bridge this gap between security literature and managerial research on anti-counterfeiting strategies, this section investigates what is the overall process of securing a supply chain against counterfeit products. A supply chain is understood as a system of companies involved in moving a product to the final customer. The different companies, or supply chain players, involve manufacturers, distributors, wholesalers, logistics service providers, and retailers or other end points where the products are sold or consumed. In addition, customs can be a part of the supply chain. The overall goal of the involved companies is to supply products to customers while trying to minimize stocks and out-of-the-shelf situations.

This section is structured in three parts. First, the general product authentication process is systematically defined. Second, an analysis of security requirements of RFID-based product authentication systems is presented. And third, a process view to supply chain security is provided to illustrate how state-of-the-art supply chain best practices and mass serialization-based product authentication concepts weld together into one integrated process.

IV.1 Product Authentication Process

IV.1.1 Definition

This thesis refers to an identity-based definition of product authentication that distinguishes between a product's *identity* and *identifier*. Identity is something unique that all individual products have, even products that can be considered identical such as cans of soft drink. A product's identity is the ”soul” of a product and remains the same throughout the product's lifetime—independent of how the product is labeled or tagged. A product's identifier, on the other hand, is a name or a reference to a product's identity. These definitions ensure that changing a product's RFID tag or barcode label does not change its identity.

An RFID-tagged product is identified by reading its identifier and authenticated by verifying the claimed identity. Product authentication can thus be defined as follows:

Product authentication = Product identification + Verification of the claimed identity

This definition conforms to the definition of authentication of Kurose and Ross (2003, p. 620) which says that ”*authentication is the process of proving one's identity to someone else*”, and to the general definition of ISO (2009) which says that ”*authentication is a provision of assurance that a claimed characteristic of an entity is correct*”.

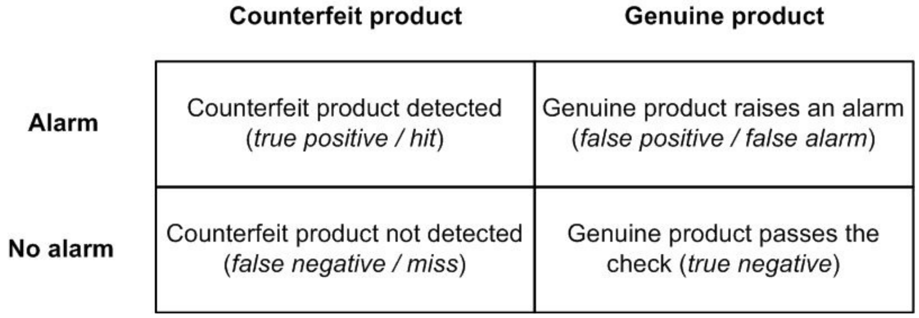
An identifier can be either in *product class-level*, and define what kind of a product its bearer is (e.g. GTIN, cf. subsection II.3.5), or in *serial-level*, and define which unique instance its bearer is (e.g. serialized GTIN). As defined in subsection I.3.3, this work assumes that RFID-tagged products bear serial-level identifiers. When a product has only a product class-level identifier, product authentication refers to verification that a product under study really belongs to this class of products, for instance, it really is a can of soft drink. When a product has a serial-level identifier, product authentication refers to verification that a product under study really is the unique article it claims, for instance, can of soft drink number 50001.

When a product's unique identity is linked to additional product information, product authentication can also help answer whether a product is diverted from an authorized distribution channel, expired, recalled, stolen, has a valid warranty, etc. Like this product identification and authentication can be used to fight also other aspects of illicit trade such as theft and illegal diversion (cf. subsection II.2).

IV.1.2 Security in Product Authentication

Verification of identity always deals with uncertainty. Therefore uncertainty is inherent in product authentication and different product authentication techniques can be seen as tools to minimize it. The remaining uncertainty is closely linked to the achieved level of security.

Owing to the inherent uncertainty, a product authentication process has four possible outcomes. These are illustrated in the decision matrix, Fig. IV-1. Favorable outcomes for the brand owner are that a counterfeit product raises an alarm (*true positive*) and that a genuine product passes the check without one (*true negative*). On the flip side, a counterfeit product can pass the check without raising an alarm (*false negative*) and a genuine product can raise an alarm (*false alarm*).



	Counterfeit product	**Genuine product**
Alarm	Counterfeit product detected (*true positive / hit*)	Genuine product raises an alarm (*false positive / false alarm*)
No alarm	Counterfeit product not detected (*false negative / miss*)	Genuine product passes the check (*true negative*)

Figure IV-1: *Possible outcomes in product authentication (decision matrix)*

The different outcomes of a product authentication process can be used to derive performance metrics. The probability that a counterfeit product is detected in a check, denoted $P_{reliability}$, characterizes the level of security of the check, and the false alarm rate, denoted P_{fa}, represents a cost factor since it invokes additional inspections. These metrics can be defined as follows:

$$P_{reliability} = \frac{\text{number of true positives}}{\text{number of counterfeit products}} \quad \text{(IV-3)}$$

$$P_{fa} = \frac{\text{number of false alarms}}{\text{number of genuine products}} \quad \text{(IV-4)}$$

Figure IV-2 (left) illustrates how the level of confidence can evolve in an example product authentication process. A product authentication process can consist of multiple checks and if a product passes a check, the level of confidence that the product under study is what it claims increases. Since perfect security does not exist under practical assumptions, a 100% confidence level cannot be achieved. Uncertainty is also present on the other side of the scale; if a product fails a check, it can still be what it claims if the check result was a false alarm. The precise mechanisms of checks are investigated in the following subsection by deriving the functional security requirements of product authenication.

Different ways to verify a product's claimed identity lead to different levels of confidence with varying effort. This principle is often employed in practice by first verifying an overt security feature (e.g. a hologram), then a semi-covert or a covert feature (e.g. color-shifting ink), and last a forensic feature (e.g. molecular markers) (e.g. Case study Johnson & Johnson, CACP, 2009). The incremental check process manages the trade-off between security and effort to check a product and improves the efficiency of checks (i.e. time is not wasted on checking forensic features when overt features are enough).

Another way to increase the efficiency of checks is *screening*. It refers to applying some predefined criteria to select products that have an elevated likelihood of being counterfeit. For instance, customs use risk management techniques to identify the most suspicious consignments for physical inspections. Screening effectiveness can be expressed as the increase of likelihood that a product which did not pass the screening test is a counterfeit compared to a product that passes the test (cf. subsection V.2.1). Screening criteria can be derived from past enforcement statistics based on variables such as country of origin, completeness of documentation, and the nature of goods, but also more mundane criteria are employed to reflect inspectors' personal experience, such as if a parcel is dirty or not.

Though screening can help inspectors detect more counterfeit articles given a fixed number of checks, it can also limit the achieved level of confidence ($P_{reliability}$) of the product authentication process. For instance, if only dirty parcels with incomplete paperwork are verified, a counterfeiter only needs to use clean parcels with complete paperwork to avoid authenticity checks. This is illustrated in Fig. IV-2 (right). To avoid counterfeiters from exploiting fixed screening criteria, the screening process should be dynamic and include a random element so that any product that passes through a check point might be checked.

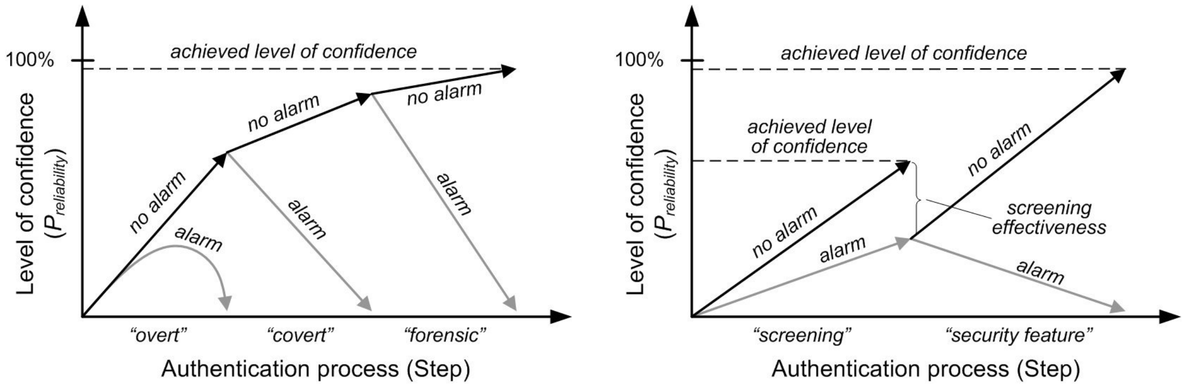


Figure IV-2: *Illustration of the level of confidence and verification steps in a product authentication process without (left) and with (right) a screening process*

IV.2 Security Requirements for RFID-Based Product Authentication

The most important technical qualities of a product authentication system can be characterized by its security requirements. This subsection presents how secure product authentication can be achieved with RFID by deriving the non-functional and functional security requirements of RFID-based product authentication systems.

IV.2.1 Non-Functional Security Requirements

Non-functional security requirements are prerequisites for a secure RFID-based product authentication system, and they do not define the system's functionalities.

1. *Product tagging:* Each genuine product needs to be tagged and the tags need to work. Since products that cannot prove their identity are considered counterfeits, a missing or a broken tag imply that the product is not genuine.

2. *Data sharing:* Product authentication techniques often require sharing of reference data. In particular, location-based product authentication is possible only if the locations of genuine products can be traced.

IV.2.2 Functional Security Requirements

Functional requirements state the functionality of a system and they can be modeled with use cases (e.g. Alhir, 2003). A use case models a basic functionality of the system and it includes actors who interact with the systems. To derive the functional security requirements for RFID-based product authentication, we apply the use and misuse case methodology of Sindre and Opdahl (2005). Requirements are elicited with the following five steps and the resulting set of requirements is presented in Fig. IV-4.

1. Identify critical assets in the system,
2. Define security goals for each asset,
3. Identify threats to each security goal,
4. Identify and analyze risks for the threats, and
5. Define security requirements for the threats to match risks and protection costs.

The use case under study is product authentication by a licit actor (e.g. a sales clerk, customs officer, private investigator, pharmacist, or consumer). The misuse case is an attack where the illicit actor attempts to fool the authenticity check and make a counterfeit product pass the check as a genuine product.

Chain of Trust in RFID-Based Product Authentication

This subsection identifies critical assets and defines security goals by defining the general chain of trust in RFID-based product authentication process.

Links in the chain of trust are identified by studying information flows. The starting step in all RFID-based product authentication approaches is identification where the reader interrogates the tag and the tag answers by transmitting its identifier (e.g. EPC). All RFID-enabled product authentication approaches are considered: product authentication based on object-specific features, tag authentication, and location-based product authentication.

In product authentication based on object-specific features, the testing equipment measures the product's feature value (i.e. the product's physical/chemical fingerprint) and transmits the measured value to the product authentication application. The product authentication application can be considered a software agent that makes the final decision whether a product is authentic or not and it resides in the internal IT systems of the company providing the authentication service (e.g. the brand owner). In order to draw the final decision, the product authentication application compares the measured feature value to reference information, that is, the feature value of the genuine product. This corresponds to verification of the claimed identity. If the two values do not match within an interval of tolerance, the product under study is not the genuine one. A close match between the measured and the reference feature value can be considered to result into a high level of confidence and vice versa.

In product authentication based on tag authentication, the tag proves its identity by showing with an authentication protocol that it knows a certain secret key (cf. subsection III.4). These protocols can be regarded as challenge-response pairs transmitted over the radio frequency interface between the reader and the tag. To know the correct response for a certain challenge, the product authentication system needs reference information which typically is the tag's secret key. In this approach, verification of identity deduces to comparing binary keys and thus

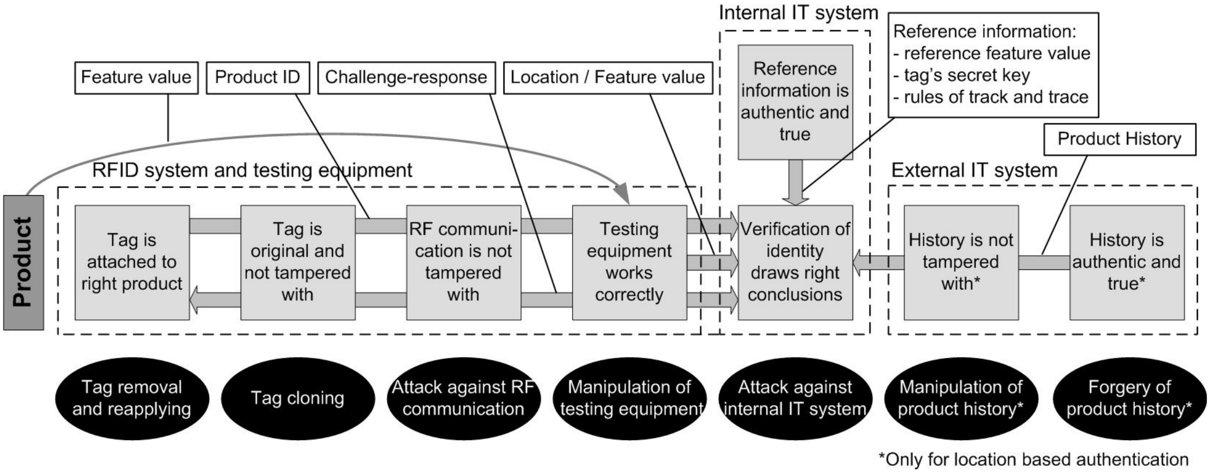

Internal IT system
Reference information:
- reference feature value
- tag's secret key
- rules of track and trace
Feature value
Product ID
Challenge-response
Location / Feature value
Reference information is authentic and true
Product History
RFID system and testing equipment
External IT system
Product
Tag is attached to right product
Tag is original and not tampered with
RF communi-cation is not tampered with
Testing equipment works correctly
Verification of identity draws right conclusions
History is not tampered with*
History is authentic and true*
Tag removal and reapplying
Tag cloning
Attack against RF communication
Manipulation of testing equipment
Attack against internal IT system
Manipulation of product history*
Forgery of product history*
*Only for location based authentication

Figure IV-3: *The chain of trust (rectangles) and threats (ovals) against RFID-based product authentication system. The arrows indicate information flows.*

the result is also in binary form. Furthermore, to move from tag authentication to product authentication, one also needs to establish whether the tag is attached to the right product.

In location-based product authentication, the testing equipment sends time and location where the product has been observed to the product authentication application. The observed location of the product under study is compared with the trace (history) of the genuine product (cf. subsection VI.3). Since products move across organizational boundaries of supply chain partners, the trace is retrieved from an external IT system like the EPCglobal network (cf. subsection II.3.5). To authenticate a product, verification of identity needs to know the set of rules and constraints that the observations must comply to. These rules represent reference information and they can define, for example, the allowed order and time frames of location observations. If the observed location is plausible, the product under study is what it claims. Verification of the claimed identity can optionally yield a level of confidence.

In order to guarantee the integrity of the previously mentioned information flows, one has to be able to trust that the tag is attached to the right product, that the tag is original and not tampered with, that the radio-frequency communication is not tampered with, that the testing equipment works correctly, that the reference information is authentic and true, that the product history is authentic and true, and that the product history is authentic and not tampered with. Finally, the verification of identity needs to draw the right conclusions based on the evidences. The resulting chain of trust is illustrated in Fig. IV-3 where arrows indicate information flows.

Threats in RFID-Based Product Authentication

Each step in the chain of trust is a possible point of attack against the product authentication system. The corresponding threats against the product authentication process are identified and evaluated below and illustrated as black ovals in Fig. IV-3.

1. *Tag removal and reapplying:* Removing and reapplying a tag from a genuine product to a counterfeit one can fool the product authentication application. Without special techniques that bind the tag and the product either logically or physically, only the tag will be authenticated but not the product. Many RFID tags are adhesive labels that are easy to removing and reapplying.

2. *Tag cloning:* Tag cloning attack refers to cloning a genuine tag and attaching the cloned tag to a counterfeit product. Definition of tag cloning means depends on the functionalities of the tag; if the tag only stores static, non read-protected data, then a successful tag cloning attack only requires reading all this data and rewriting it on an empty tag. This is easy to do for unprotected tags that only store a rewritable ID number. If the tag also has a secret key, however, then tag cloning requires cracking this key which can be very hard (cf. subsection III.4).

3. *Attack against RF communication:* Also an attack against the radio frequency (RF) interface can fool the product authentication system. In this case, the product does not have a copied tag that would pass the check and the adversary conducts a replay attack by hiding a replay device close to the reader device, or together with the counterfeit product, to replicate a genuine tag. A replay device is basically an RF tape recorder that can scan and then replicate tags, and building such a device requires only little money or expertise (Westhues, 2005, pp. 291-300)[1]. Even complex protocols can be vulnerable to relay attacks where the adversary resides between the genuine tag and the reader.

4. *Manipulation of testing equipment:* The testing equipment includes the RFID reader and, for object-specific features approach, a device that can measure the physical or chemical features of the product under study. Compromising the testing equipment can be used to fool the check, for example by hard-wiring it to let all products pass the check. In a more complicated attack, it could try to claim a wrong location to the product authentication application, for example, the known location of the genuine product to fool the location-based plausibility check.

5. *Attack against internal IT system:* The most important functionalities and data of a product authentication system reside in the internal IT system of the company that provides the authentication service. These comprise the reference information of genuine products and the part of the system that draws the final conclusion about the authenticity of a product. Possible attacks comprise data theft to steal the secret keys and encryption schemes and manipulation of the product verification software.

6. *Manipulation of product history:* The trace, or history, of a product can either move together with the product as a pedigree (e.g. Pearson, 2005), reside in distributed database

[1] Also the tag impersonation device mentioned in subsection VI.1.3 can be seen as an attack against RF communication

of all the custodians of the product (e.g. Staake et al., 2005), or reside in one central database. In all these cases the trace of a genuine product can be vulnerable to manipulation. Manipulation can fool location-based authentication by adding bogus events to ”relocate” the genuine product, by removing existing events, and by modifying time and location of existing events.

7. *Forgery of product history:* Also the creation of a falsified history from scratch can threaten location-based product authentication.

Risks in RFID-Based Product Authentication

This subsection analyzes risk corresponding to the above identified threats. Risk assessment is needed to evaluate which threats are most serious and therefore require most attention.

In general, risks can be assessed by evaluating the *exposure* (or consequence) and *uncertainty* (or likelihood) of known threats (Holton, 2004). In this analysis the consequence corresponds to the number of products that are compromised, that is, how many counterfeit products can fool the authenticity check after a successful attack. This is either a single product (1), multiple but limited number of products (N), or an unlimited number of products (∞). The likelihood of a threat is commonly measured by the frequency of incidents. Since RFID-based product authentication is still rather immature, the threats have not (yet) realized in such an extent that counting them would provide statistically reliable likelihood estimates. Therefore the threat likelihoods are evaluated in terms of how easily the corresponding attach could be conducted, in a rough nominal scale *low-medium-high*.

Manipulation of existing trace events on a server would require an attack against the location where these events are stored (e.g. EPCIS) or an attack against the communication channel through which the events are transferred. Authentication of end users and services is addressed by the EPCglobal network architecture (EPCglobal Inc., 2009a) and secure communication channels can be established using standard communication protocols. As a result, these attacks do not appear particularly likely. Assuming that the history that is written on a tag is digitally signed with a sufficient key length, also manipulation of existing events on tags appears unlikely. However, an insider in the supply chain who has his own EPCIS could manipulate a product’s trace in a rather straight forward way by publishing forged events. Like this an illicit actor could make a genuine product appear virtually anywhere and inject a counterfeit product with the same identifier in the same location. A successful attack could compromise one or multiple products.

Forgery of a complete product history requires a successful impersonation or infiltration of the brand owner’s server where the events are stored. One potential attack tries to redirect ONS or DS queries to a phony server masqueraded as an authorized EPSIS, publishing forged histories of counterfeit products. Injecting forged manufacturing events into a manufacturing database is considered substantially harder. A successful forgery attack could compromise multiple, even an unlimited number of products. However, database and network authentication mechanisms can be considered good enough so that when properly employed, this threat is not particularly likely to succeed.

Attacking the RF communication is complex and requires hiding special equipment in the proximity of the authenticating reader device. Doing this is hard in practice since the authentication takes place in a controlled environment, most often inside the licit supply chain (cf. subsection VII.3), and under the supervision of authorized personnel. Therefore the likelihood of such an attack is considered low. Similarly, since the testing equipment for object-specific features is handled by authorized personnel, we conclude that manipulation of testing equipment is also not likely. When succeeded, however, both these attacks would compromise all products that pass through the compromised check point.

Attacks against the internal IT systems have the potential to compromise an unlimited number of products, making it especially interesting point of attack. It is likely that the internal IT system running the product authentication service needs to provide an online interface for remote parties. As for other online systems, it is assumed that by using standard network security techniques and secure communication channels this risk can be effectively mitigated, though not completely eliminated.

Low-cost tags provide only limited protection against tag cloning attacks (cf. subsection III.4). To clone a large amount of tags, illicit actors could target consignments inside the licit supply chain or employ social engineering. Overall, the likelihood of cloning attacks against low-cost tags is evaluated high. The use of more expensive cryptographic tags significantly increases the counterfeiter's barrier to clone genuine tags, though also cryptographic schemes can be broken (e.g. Bono et al., 2005; Bogdanov, 2007; Courtois et al., 2008). Furthermore, if cloned tags cannot be detected, cloning one genuine tag compromises an unlimited number of products since a counterfeiter can copy the same tag on multiple counterfeit products without an increased risk of getting caught.

Removal and reapplying of genuine tags is perhaps harder to be completely prevented than tag cloning, but it is more costly for the counterfeit player in larger scales. Tag removal and reapplying is somewhat similar to removal and reapplying of price tags of consumer goods which is an existing threat in the retail industry. When an RFID tag authenticates high-value items such as airplane spare parts or expensive drugs, even the removal and reapplying of a small number of tags can be financially interesting for counterfeits. If a counterfeiter cannot get genuine tags from inexpensive sources, such as diverted genuine packages from scratch or repackaging, he would need to buy genuine products to get the genuine tags. This would be financially unattractive for the counterfeiter. Therefore tag removal and reapplying is partly limited by the extent in which counterfeiters can easily obtain inexpensive genuine tags.

The lack of binding between the tag and the product is especially problematic in the pharmaceutical industry where the RFID tag is never attached to the drug product itself (tablet, ampule, vial, etc.) but on the secondary or tertiary packaging (blister package, carton package, etc.).

Not only is it easy to disassociate the tag from the drug product it authenticates by changing the contents of the package, but it also is a common practice in the industry when the products are repackaged. Drug products are repackaged for example in order to change the language of the package and instructions as the products move to another country. Repackaging of drug products is legal in Europe and in the U.S. but illicit actors can use it to inject counterfeit products to the market by including counterfeit products among the unpackaged genuine products.

Table IV-1 summarizes the risks against RFID-based product authentication systems.

Table IV-1: *Risk assessment against RFID-based product authentication systems*

Threat	Consequence	Likelihood	Risk
Tag cloning (low-cost tags)	∞	High	High
Tag removal and reapplying	1	High	High
Manipulation of product history	N	Medium	Medium
Attack against internal IT system	∞	Low	Medium
Forgery of product history	∞	Low	Medium
Manipulation of testing equipment	N	Low	Low
Attack against RF communication	N	Low	Low

Resulting Functional Security Requirements

Security goals and threats against RFID-based product authentication are presented in Fig. IV-4 as a use/misuse-case diagram. In general, the diagram shows that security officers of affected companies have much more than the tag cloning attack to worry about.

The functional security requirements of RFID-based product authentication systems comprise the security goals that mitigate the above identified threats. If a threat is not mitigated, the system has a vulnerability that can be exploited with a low cost-to-break and a low probability of getting caught. Assuming that the non-functional security requirements (cf. subsection IV.2.1) are satisfied and that an adversary will break through where the barrier is the lowest, *the level of security of a product authentication system is equal to the level of protection provided by the weakest functional security requirement.*

The diagram how that different product authentication approaches are affected by different threats and that there are three different combinations of security goals that mitigate all threats. These correspond to three different approaches how tag cloning attack can be addressed. Assuming that other threats than tag cloning are mitigated, the level of security ($P_{reliability}$) of these three product authentication approaches can be defined as follows:

- Product authentication based on prevention of tag cloning (tag authentication): $P_{reliability} = Pr(\textit{the security feature is not cloned})$.

- Product authentication based on detection of cloned tags (location-based authentication): $P_{reliability} = Pr(\textit{the cloned tag is detected})$.
- Product authentication based on object-specific features (direct authentication): $P_{reliability} = Pr(\textit{the object-specific feature is not cloned})$.

When ID number copying is mitigated by tag authentication, the illicit actor still can attempt physical attacks against the tag memory, data theft from internal IT system, side channel attacks, and cryptanalysis and reverse engineering. The licit actor can respond by physically securing the tag memory, by securing the internal IT system against key theft, by securing the tag against side channel attacks, and by using secure protocols and long-enough keys. This war of escalation is apparent in the use/misuse-case diagram. The other two approaches to mitigate tag cloning attack are detection of cloned tags and verification of object-specific features.

The threat of tag removal and reapplying must be mitigated either by preventing tag removal (e.g. with secure tag integration), detecting tag removal (e.g. with a seal), or by verifying the object-specific features to assure that a tag is attached to the right product. One practical way to prevent the removal tags is to integrate the tag in such a way that the chip will detach from the antenna when the tag is removed. This method is applied for example in perfume bottles where the tag resides between the bottle top and the glass bottleand if the bottle top is removed, the antenna will stay attached to the glass bottle while the chip comes off with the bottle top.

Attack against internal IT system, manipulation of testing equipment, and attack against RF communication needs to be mitigated by securing the internal IT systems from outsider and insider attacks, by guaranteeing the integrity of the testing equipment and by securing the verification environment, respectively. Last, the threat of manipulation of product history must be mitigated by guaranteeing the integrity of the history, and the threat of forgery of product history must be mitigated by guaranteeing authenticity of the history.

The presented security requirements analysis helps understand the threats and risks of potential adversaries as well as the required security goals and how they are interconnected. On the flip side, the use/misuse-case diagram does not model the attack sequence and the sequence in which preventive and detective measures affect the attacks. In addition, the and/or relationships among threats and among security goals are not explicitly marked in the diagram to show which goals replace each other, though these relations are explained in the text. And last, even though the analysis of chain of trust provides an insightful view of possible attacks, adversaries can potentially still come up with other ways to fool the system not covered by this analysis.

IV.3 Integrated Process of Securing a Supply Chain from Counterfeits

This subsection shows that product authentication is not a distinct measure to secure a supply chain from counterfeit products, but rather a part of an integrated process that also comprises several organizational and legal measures. In accordance with the related work (cf. subsection

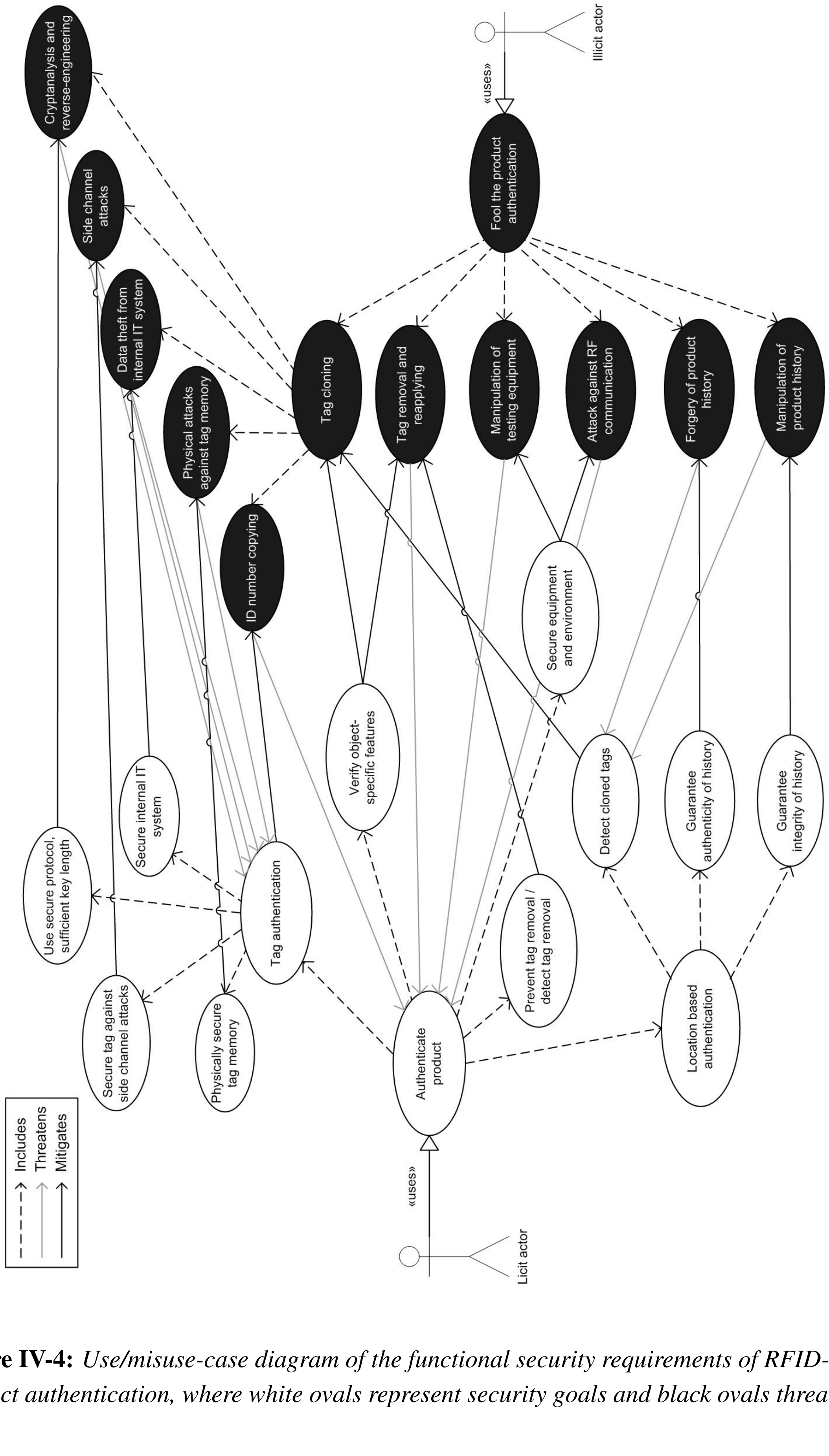

Cryptanalysis and reverse-engineering
Side channel attacks
Data theft from internal IT system
Physical attacks against tag memory
ID number copying
Tag cloning
Tag removal and reapplying
Manipulation of testing equipment
Attack against RF communication
Forgery of product history
Manipulation of product history
Fool the product authentication
«uses»
Illicit actor
Verify object-specific features
Secure equipment and environment
Detect cloned tags
Guarantee authenticity of history
Guarantee integrity of history
Use secure protocol, sufficient key length
Secure internal IT system
Tag authentication
Prevent tag removal / detect tag removal
Secure tag against side channel attacks
Physically secure tag memory
Authenticate product
Location based authentication
«uses»
Licit actor
Includes
Threatens
Mitigates

Figure IV-4: *Use/misuse-case diagram of the functional security requirements of RFID-based product authentication, where white ovals represent security goals and black ovals threats*

III.2), the achieved level of security as well as a counterfeiter's expected payoff from illicit activities are determined by this overall process.

IV.3.1 Assumed Technical Solution

A technical solution is assumed based on low-cost RFID. Each genuine product has an RFID label that stores a unique serial number. Reader devices can read the serial number and verify from a "white list" if the serial number is *valid*, i.e. one that could be found on a genuine product. In addition, the genuine products can have hard-to-copy security features for an increased cloning resistance, such as security printings, holograms, or cryptographic RFID tags (cf. subsection III.4). The brand owner and other licit actors can check the serial numbers and additional security features to detect counterfeit products in the protected supply chain. To make it hard for the counterfeiter to obtain valid serial numbers, the brand owner can issue randomized serial numbers and remove serial numbers of products that are sold or consumed from the "white list". In addition, the brand owner applies organizational and legal anti-counterfeiting measures (cf. Fig. I-1).

IV.3.2 Process Model for Countermeasures

The integrated process of securing a licit supply chain from counterfeit is constructed by first identifying the counterfeiter's course of action and then identifying which preventive, detective, and responsive countermeasures illicit actors can apply to mitigate these actions. The counterfeiter's actions correspond to threats that are each mitigated by a process of security.

The counterfeiter's course of action includes i) obtaining counterfeit products, ii) obtaining tags with valid serial numbers, and iii) selling the counterfeit product to the licit supply chain. Obtaining valid serial numbers is in fact not a mandatory step for the counterfeiter, but not doing it enables the counterfeit product to be easily detected based on invalid serial numbers. A more detailed action sequence could be envisioned for the counterfeiter including for example integration of tags to counterfeit products, but this could introduce unnecessary complexity.

The organizational and legal countermeasures are taken from the state-of-the-art anti-counterfeiting best practices and mapped to the integrated process of securing a supply chain. The current best practices are taken from the following studies:

- No trade in fakes supply chain tool kit of the U.S. Chamber of Commerce and the Coalition Against Counterfeiting and Piracy (CACP, 2006),
- Benchmarking study of anti-counterfeiting best practices by Staake (2007), and
- Intellectual property protection and enforcement manual of the Coalition Against Counterfeiting and Piracy (CACP, 2009).

Figure IV-5 illustrates the resulting integrated process of securing a supply chain that combines mass serialization-based technical countermeasures, as well as organizational and legal measures. This model shows how a supply chain is secured through three processes (1.1 - 1.3, 2.1 - 2.3, 3.1 - 3.3) that each make it hard for the counterfeiter to achieve his goals. *Security is thus not only a process, but a combination of multiple prevent-detect-respond processes.* The resulting overall process has two effects:

- *Direct effect of security:* Counterfeit products in the licit supply chain are detected.
- *Deterrent effect of security:* Counterfeiting becomes financially uninteresting for potential counterfeiters.

By revealing a broad set of possible points of intervention for licit actors, the model gives a comprehensive view of the available measures that licit actors can apply to secure a supply chain from counterfeits. In addition, the model explains the goals and cause-effect relationships of different countermeasures and provides the basis for quantifying the achieved level of security and the financial impact on counterfeiters (cf. Section V).

Countermeasures presented in this model are limited to those that directly mitigate the supply of counterfeit product so the model does not address mitigation of the demand side or the prerequisites for countermeasures like registration of trademarks and copyrights. In addition, the model does not show the actors involved in different countermeasures and therefore it is not a complete guide to company-wide anti-counterfeiting measures. Nevertheless, it is the first explanatory models of how a supply chain is secured with a combination of technical, organizational, and legal measures and it can furthermore applied to both licit and illicit supply chains. The different steps in the overall process are detailed below.

Step 1.1: Prevent Counterfeiters from Obtaining Counterfeit Products

The first step in the overall process of securing a supply chain is to make it hard for the counterfeiters to obtain counterfeit products with adequate functional and visual quality. Though complete prevention is often not realistic, there are ways how brand owners can prevent counterfeiters from exploiting certain loopholes which can make acquisition of counterfeit products considerably easier. Precise blueprints of the genuine product should not be disclosed in public. The brand owner can audit manufacturers and subcontractors who provide semi-finished or finalized products to ensure that they are not selling components to illicit manufacturers or running ”third shifts” to produce *factory overruns* (cf. subsection II.2).

In addition, manufacturers should verify the legitimacy of customers and distributors who might seek to purchase genuine products in bulk only in order to blend counterfeit products among them. This can be enforced through guidelines and training the sales force so that suspicious buyers can be identified based on factors such as unusual large volume, cash payment for a very expensive order, order of products that do not fit the customer's line of business, and vague delivery dates and suspicious delivery destinations.

Production waste, damaged or unusable inventory, or other inferior goods discarded by the brand owner are possible sourcing channels for counterfeiters and should therefore be properly handled by establishing policies of proper disposal. Last, the use of seals on containers and smaller consignments can prevent theft, which, combined with re-labeling (e.g. marking a later expiry date on perishables, a higher concentration of active ingredient on drugs, or a higher performance on electronic appliance), can also become sources of counterfeit products.

Step 1.2: Detect Counterfeit Products Outside the Licit Supply Chain

Private investigations can be used to detect counterfeit products in a market and to track down their source. Other methods include sampling and mystery shopping where example articles are bought from suspicious sources to verify the origins of the sold goods. In addition, brand owners can monitor e-commerce channels including dedicated websites for counterfeit products or ”replicas” as well as Internet auction sites. Last, verifying the integrity of seals on containers and consignments helps detect if genuine merchandise is stolen to source counterfeiters.

Step 1.3: Respond to Counterfeiting Cases

Infringing products that are detected outside the licit distribution channel should be confiscated based on IP right violations. Customs is a critical stakeholder when it comes to supporting seizures and the counterfeit products should be properly disposed of with the help of the manufacturer. In order to have the right to seize suspected counterfeit articles, European customs need to have an *application for action* (European Commission, 2003) from the corresponding IP right owner within the region, though customs can also initiate a so called ex officio procedure to seize the products temporarily if such an application has not yet been filed. To demonstrate to those engaged in counterfeiting activities that they are at risk no matter what the level of sales activity, the offenders should be prosecuted even on small counterfeiting cases.

In addition, especially large brand owners can respond by ending business relationships with offending parties in case such relationships have been established. Brand owners can also employ ”strict liabilities” for instance by including provisions in purchasing contracts to hold sellers responsible for fraudulent goods. However, care must be taken for the response to be conducted in a legally correct manner; for instance, if private investigators become too aggressive in seizing alleged counterfeits, the investigator and his client may face claims for wrongful seizure to recover lost profits and cost of lost material (Hopkins et al., 2003, p. 241).

Step 2.1: Prevent Counterfeiters from Obtaining Valid Serial Numbers

If authentication technologies represent significant barriers to counterfeiters, it can be expected that counterfeiters attempt to obtain valid features that make fake products pass authenticity checks. In one ruthless example, armed robbers broke into a factory in the United Kingdom in November 1997, tied up three employees, and made off with 200,000 Microsoft Certificates of Authenticity (Hopkins et al., 2003, p. 262). In a similar manner, once valid serial numbers become a prerequisite for counterfeit goods not being detected in checks, counterfeiters will have strong incentives to obtain them. This is a potential lever through which brand owners can make life harder for counterfeiters.

To prevent a counterfeiter from obtaining valid serial numbers, the brand owner should minimize the size of the name space of valid serial numbers. The first measure is to hold a ”white list” of serial numbers that have been assigned to genuine products (Koh et al., 2003), such as a manufacturing database. If the validity of serial numbers needs to be verifiable without a network connection, the serial numbers can include digital signatures (cf. subsection II.4.2). Valid serial numbers should also be unpredictable to make it unfeasible for a counterfeiter to guess them. And third, a serial number that becomes invalid (e.g. when the product is sold or disposed) should be put on a ”black list” of numbers that are no longer valid (or removed from the ”white list”). These three measures keep the space of valid serial number in minimum size and unpredictable for counterfeiters.

Furthermore, the databases where the serial numbers are stored should be secured against data theft. In case subcontractors label genuine products, the number of valid serial numbers delivered to the subcontractors should be restricted and controlled to decrease the risk of high-quality factory overruns. In order to prevent removal and reapplication of valid tags (or labels) from genuine products and their packaging, waste management of disposed products should be taken care of. Institutional and industrial users such as hospitals represent a critical point for secure waste management. Last, secure tag-product integration can also prevent the removal of labels with valid serial numbers for illicit purposes.

Step 2.2: Detect Copied Serial Numbers

Detecting that a valid serial number has been copied to counterfeit products is important to prevent further counterfeit products with the same number from entering the secured supply chain. The use of copied serial numbers can be detected by analyzing the track and trace data for inconsistencies, such as repeated sales event. (Subsection VI.3 details a probabilistic method for detection of cloned serial numbers based on machine-learning techniques.) In addition, in case there is an increased risk that a consignment is subject to clandestine scanning for tag cloning purposes in a certain supply chain route, a ”logger tag” could be used to register and detect the clandestine communications. Note that this ”logger tag” approach is specific to RFID and cannot be used with barcodes.

Step 2.3: Respond to Copying of Serial Numbers

After copying of valid serial numbers has been detected, the copied numbers should be put on a ”black list” to prevent their use in counterfeit products. Second, the possible supply chain routes or regions where the serial numbers have been copied can be analyzed to help pinpoint illicit actors.

Step 3.1: Prevent Counterfeit Products Being Sold to the Licit Supply Chain

Measures to prevent counterfeiters from selling fake products to the protected supply chain comprise securing legitimate inputs and vendor audit. These measures are important especially in the retail-level but they can be applied also to acquisition of raw materials and components. Buyers should be guided how to assess the legitimacy of the supplier, and risk management can be utilized to identify businesses that have an augmented probability of engaging in trade with counterfeit products.

In addition, also technical measures can prevent counterfeit products from being sold to the licit supply chain. For example, assuming that all genuine products must comply to certain tag integration constraints that pose technical challenges (e.g. RFID tag integration inside a metal object, a barcode label sealed with a secure seal, etc.), the technical hurdle itself can be enough to prevent the counterfeiter from obtaining a good that could be sold as a genuine product.

Step 3.2: Detect Counterfeit Products Sold to the Licit Supply Chain

Product authentication can be used to detect counterfeit products as they enter—or after they have entered—the licit supply chain. The assumed product authentication process consists at least of checking whether the product under study has a valid serial number, and potentially of other checks that can detect copied serial numbers. In addition to authentication of single products, consignments can be verified by checking that all goods in a case/pallet are in original packaging and have the same lot numbers and different serial numbers (cf. subsection V.2.3).

In contrast to the detection of counterfeit products outside the licit supply chain (Step 1.2) and detection of copied/copying of serial numbers (Step 2.2), detection of counterfeit products inside the licit supply chain can reach a 100% detection rate. Furthermore, serialization based product authentication enables countermeasures 2.1 - 2.3 explained above. Therefore product authentication is a particularly important step in the overall process of securing a supply chain from counterfeits. Product authentication inside the licit supply chain can also be conducted through sampling and ”mystery shopping” if the checks need to be conducted without the consent of the seller. These usage scenarios are detailed in subsection VII.3. In addition to conducting authenticity checks by themselves, brand owners can help customs detect counterfeit products by providing information, equipment, and training.

Step 3.3: Respond to Counterfeiting Cases

The responsive measures in case a counterfeit product is detected in a licit supply chain are basically the same than those when counterfeit products are detected outside the licit supply chain (Step 1.3). They include confiscation of the illicit products, secure disposal of the seized goods, finding the source of illicit products, prosecuting the offenders, ending business relationships as well as applying strong liabilities.

In addition to these responsive measures that directly affect the counterfeiter's payoff, the response process includes measures that minimize the losses to the licit players. These include informing and warning those who are affected by the counterfeit products and adjusting the anti-counterfeiting strategy. Overall, it is recommended that the process for dealing with counterfeiting cases is well established and formalized in affected companies to enables swift responses as well as gradual improvements.

Lessons for Anti-Counterfeiting

- Product authentication is a process that inherently deals with uncertainty. The achieved level of security of this process is characterized by the level of confidence in the result when a product passes the check/checks.
- Screening can increase the effectiveness of scarce authenticity checks, but predictable or otherwise faulty screening criteria can limit the achieved level of security.
- The most important risks that product RFID-based authentication systems need to mitigate are those of tag cloning and tag removal and reapplying.
- There are three distinct approaches to mitigate the risk of RFID tag cloning: prevention of tag cloning, detection of cloned tags, and verification of object-specific features (i.e. direct authentication).
- A supply chain is secured from counterfeits by a process that consists of technical countermeasures (i.e. serialization and product authentication), organizational countermeasures, and legal countermeasures.

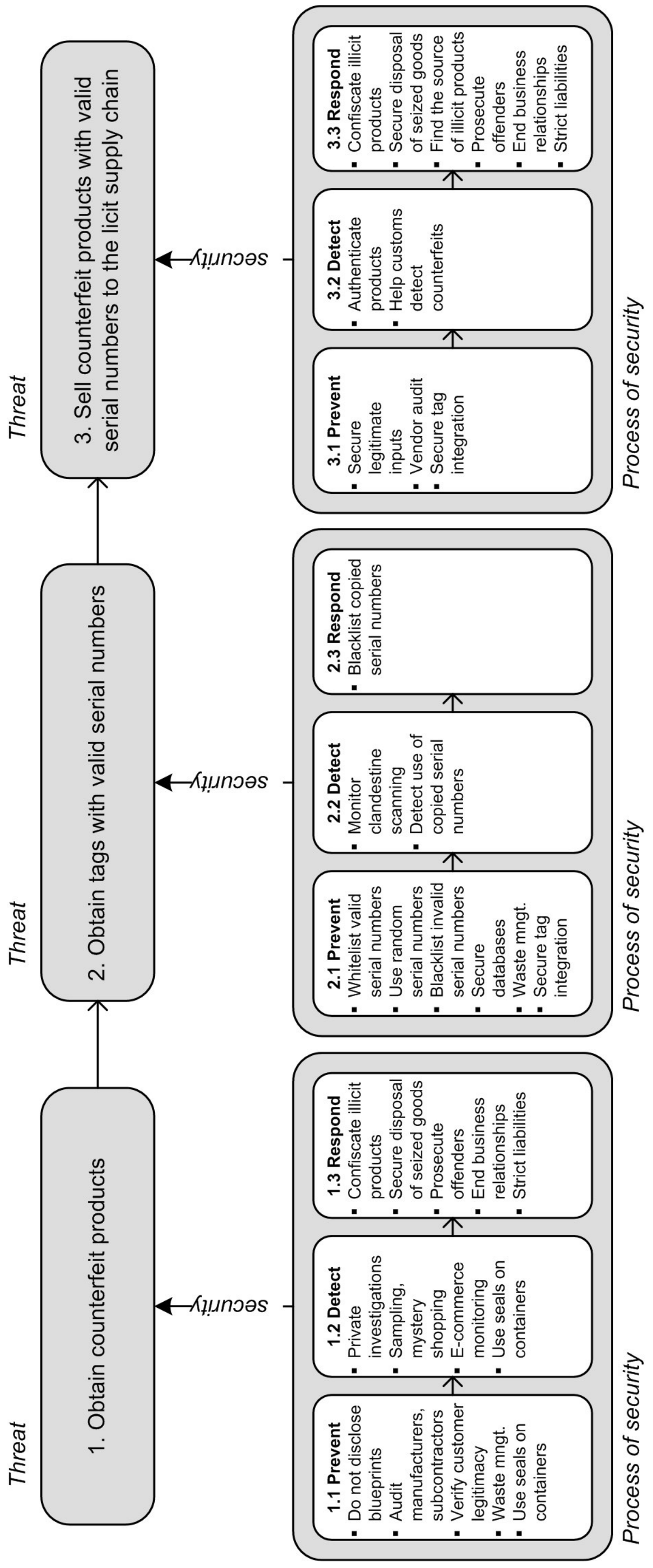

Threat
1. Obtain counterfeit products
Threat
2. Obtain tags with valid serial numbers
Threat
3. Sell counterfeit products with valid serial numbers to the licit supply chain
security
security
security
1.1 Prevent
▪ Do not disclose blueprints
▪ Audit manufacturers, subcontractors
▪ Verify customer legitimacy
▪ Waste mngt.
▪ Use seals on containers
1.2 Detect
▪ Private investigations
▪ Sampling, mystery shopping
▪ E-commerce monitoring
▪ Use seals on containers
1.3 Respond
▪ Confiscate illicit products
▪ Secure disposal of seized goods
▪ Prosecute offenders
▪ End business relationships
▪ Strict liabilities
Process of security
2.1 Prevent
▪ Whitelist valid serial numbers
▪ Use random serial numbers
▪ Blacklist invalid serial numbers
▪ Secure databases
▪ Waste mngt.
▪ Secure tag integration
2.2 Detect
▪ Monitor clandestine scanning
▪ Detect use of copied serial numbers
2.3 Respond
▪ Blacklist copied serial numbers
Process of security
3.1 Prevent
▪ Secure legitimate inputs
▪ Vendor audit
▪ Secure tag integration
3.2 Detect
▪ Authenticate products
▪ Help customs detect counterfeits
3.3 Respond
▪ Confiscate illicit products
▪ Secure disposal of seized goods
▪ Find the source of illicit products
▪ Prosecute offenders
▪ End business relationships
▪ Strict liabilities
Process of security

Figure IV-5: *The integrated process of securing a supply chain against counterfeit products*

V The Economics of Security in Anti-Counterfeiting

Economic models can evaluate the effect of security on financially motivated thieves such as counterfeiters. The assumption that counterfeiters are financially motivated and conduct some form of cost-benefit analysis before engaging in illicit activities is rather strong, but already used in economic analysis (e.g. OECD, 1998) and repeatedly confirmed by discussions with brand protection experts. The potential of economic analysis in anti-counterfeiting is thus based on the fact that product counterfeiting is a business. As a comparison, economic modeling might be less useful in general IT security since computer crackers are partly motivated by intellectual challenges, fame, and reputation.

This section presents an economic analysis of security in anti-counterfeiting based on a model how a product authentication system affects the payoff of a counterfeiter who wants to sell counterfeit products to a licit/illicit supply chain. This model provides the basis for evaluating the economic effects of security on a counterfeiter. The presented analysis framework models security far beyond the cost-to-break that has a somewhat dominant role in current security models (cf. subsection III.2).

As argued in subsection IV.3, the ability to detect counterfeit products is the direct effect of security that a product authentication system has on a supply chain. Furthermore, detection of counterfeit products is an important factor behind the deterrent effect of a product authentication system on a potential counterfeiter. Therefore this analysis focuses on explaining what are the different mechanisms how licit and illicit actors—brand owners and counterfeiters—can influence detection of counterfeit products.

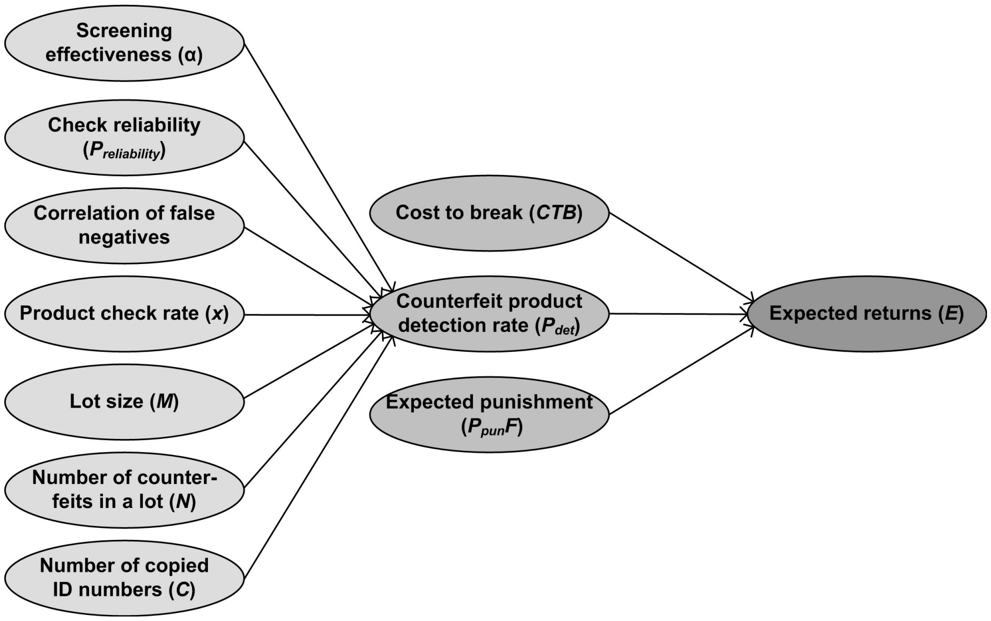

Screening effectiveness (α)
Check reliability ($P_{reliability}$)
Correlation of false negatives
Product check rate (x)
Lot size (M)
Number of counter-feits in a lot (N)
Number of copied ID numbers (C)
Cost to break (CTB)
Counterfeit product detection rate (P_{det})
Expected punishment ($P_{pun}F$)
Expected returns (E)

Figure V-1: *Different effects defining counterfeit detection rate*

Table V-1: *Summary of symbols and definitions used in this section*

Symbol	Description
P_{det}	Probability that a counterfeit product is detected
P_{check}	Probability that a counterfeit product is checked
$P_{reliability}$	Probability that a counterfeit is detected when checked
E	Expected net value of injecting one counterfeit article to a licit supply chain
E_s	Expected net value of a serial theft
CTB	Cost-to-break preventive security measures
P_{pun}	Probability that the counterfeiter is punishment if a counterfeit product is detected
F	Value of the fine paid upon punishment
L	Profit from selling one counterfeit article as a genuine product (*loot*)
M	Lot size
R	One over the ration of counterfeit products (every R^{th} article is counterfeit)
x	Product check rate
N	Number of counterfeit products in a lot of counterfeit products
C	Number of different serial numbers in a lot

The change in a counterfeiter's payoff characterizes the *deterrent effect* of the process of security. However, even when the expected return of injecting counterfeit products into a licit supply chain is negative and thus a losing proposition for counterfeiters, deterrence itself does not guarantee that counterfeiting never happens. Therefore it is important to know the the *direct effect* of security that is characterized by the achieved counterfeit product detection rate (or the average counterfeit product detection rate across different counterfeit product categories). This is an intuitive metric for the effectiveness of the process of security.

Figure V-1 presents the overall model behind the presented analysis. From right to left, the model explains how expected returns from counterfeiting depend on the process of security, and how counterfeit product detection rate depends on a number of tactical mechanisms such as the check success rate and lot size. The strategic level on the right formalizes the economic reasoning of how to win the war against counterfeiters who inject fake products to licit supply chains, and the tactical level on the left formalizes the individual effects of mechanisms that licit and illicit actors can apply. Furthermore, though security is provided by multiple prevent-detect-respond processes as shown in subsection IV.3, this section shows how the effect of subsequent processes of security can be modeled with only one prevent-detect-respond process.

This section first studies the formulas that define a counterfeiter's expected return from injecting counterfeit articles to a protected supply chain. Then the different tactical mechanisms how licit and illicit actors can influence counterfeit product detection rate are analyzed. The results are summarized as lessons for anti-counterfeiting and theoretical implications are discussed.

V.1 How to Affect a Counterfeiter's Payoff

This subsection first builds upon the work of Schechter and Smith (2003) to model the payoff of a counterfeiter who wants to inject a counterfeit product to a supply chain, and then studies the strategic conditions under which a a supply chain can be considered secure from counterfeiting.

V.1.1 Quantifying the Effect of Security

The overall effect of the assumed technical, organizational, and legal anti-counterfeiting measures, as defined in subsection IV.3.1, is first modeled. In order to succeed and generate a profit, the counterfeiter needs to i) obtain counterfeit products, ii) obtain tags with valid serial numbers, and iii) sell the counterfeit product to the protected supply chain. Countermeasures affect each step in this course of action by making them costly to execute and by introducing a chance of failure and a risk of being detected and punished.

A counterfeiter's payoff is affected by multiple prevent-detect-respond processes. This is illustrated in Fig. V-2. The overall effect of all security measures can nevertheless be modeled with only one prevent-detect-respond process (i.e. process of security) when a counterfeiter's cost and risk to obtain counterfeit products and forged labels (denoted as $Cost_1$ and $Cost_2$ in Fig. V-2) are added to the cost-to-break of selling a counterfeit product to the protected supply chain (denoted as CTB_3 in Fig. V-2). The theoretical implication of this observation is that CTB should be expanded to include also the risk factors of adversaries' steps that precede the actual threat (here: the risk of being punished for producing/buying a counterfeit product).

Let CTB denote the cost-to-break of selling a counterfeit product to the protected supply chain (including the above mentioned $Cost_1$ and $Cost_2$), P_{det} the probability that a the counterfeit product is detected, P_{pun} the probability that the counterfeiter is punished when a counterfeit product is detected, F the value of the fine paid upon punishment (including cost of seized goods), and L the profit from selling one counterfeit article as a genuine product (the loot). These symbols are presented in Table V-1. A counterfeiter's expected payoff E from selling a counterfeit article (or a consignment of counterfeit articles[1]) to the protected supply chain can now be presented based on Schechter and Smith (2003) as follows:

$$E = (1 - P_{det})L - P_{det}P_{pun}F - CTB \tag{V-5}$$

In the case of a serial theft, the counterfeiter continues to inject counterfeit articles to a licit supply chain until a counterfeit article is detected. The model assumes that repeating the theft is no longer possible after the detection of the first counterfeit article, for instance because the illicit trader's reputation or shipping route has been compromised, or the used serial number(s)

[1] To calculate the effect of injecting multiple counterfeit products instead of only one, L and CTB should be multiplied by the number of counterfeits in the consignment and P_{det} should be corrected to represent the probability that the counterfeit consignment is detected (subsection V.2.1 presents how to calculate the new P_{det}).

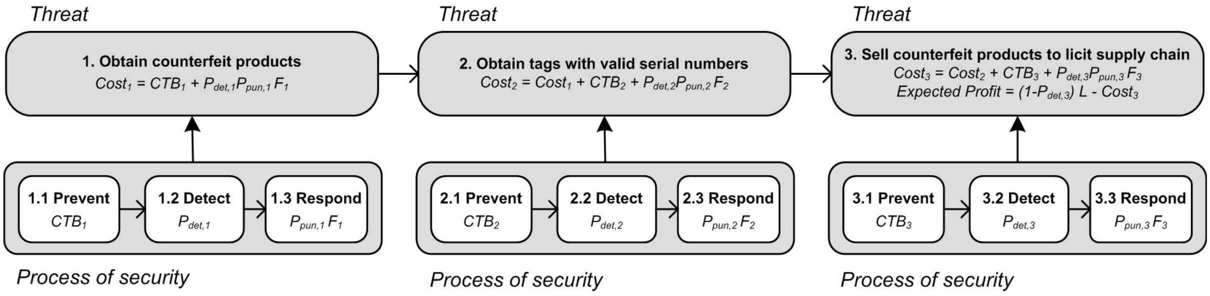

Threat
1. Obtain counterfeit products
Cost1 = CTB1 + Pdet,1Ppun,1 F1
Threat
2. Obtain tags with valid serial numbers
Cost2 = Cost1 + CTB2 + Pdet,2Ppun,2 F2
Threat
3. Sell counterfeit products to licit supply chain
Cost3 = Cost2 + CTB3 + Pdet,3Ppun,3 F3
Expected Profit = (1-Pdet,3) L - Cost3
1.1 Prevent
CTB1
1.2 Detect
Pdet,1
1.3 Respond
Ppun,1 F1
2.1 Prevent
CTB2
2.2 Detect
Pdet,2
2.3 Respond
Ppun,2 F2
3.1 Prevent
CTB3
3.2 Detect
Pdet,3
3.3 Respond
Ppun,3 F3
Process of security
Process of security
Process of security

Figure V-2: *Quantifying the process of security*

are blacklisted. Furthermore the model assumes that P_{det} is constant after each injected counterfeit article. Though this assumption holds true for prevention-based security measures such as cryptographic RFID tags, the probability of detecting cloned RFID tags is not constant but increases if the same serial number is repeatedly used in multiple counterfeit products. Therefore this analysis assumes for now that a counterfeiter does not use the same serial number in multiple products (subsection V.2.3 presents an exception to this assumption). The expected net value of a serial theft, E_s, can then be expressed as follows:

$$\begin{aligned} E_s &= \frac{(1-P_{det})(L-CTB) - P_{det}(P_{pun}F+CTB)}{P_{det}} \\ &= \frac{(1-P_{det})}{P_{det}}(L-CTB) - (P_{pun}F+CTB) \end{aligned} \tag{V-6}$$

V.1.2 Three Strategies for Security

Equation V-5 shows that theoretically there are three distinct strategies to make counterfeiting a losing proposition ($E < 0$):

- *Prevention-strategy* relies on making cost-to-break higher than the loot value ($CTB > L$). This strategy assumes that a counterfeit article cannot be successfully injected without breaking the preventive security measure, i.e. paying the CTB is mandatory to obtain the L.

- *Detection-strategy* decreases the chances of obtaining the L with a high P_{det}, rendering E close to zero also when CTB and $P_{pun}F$ are zero.

- *Deterrence-strategy* relies on a high expected punishment $P_{pun}F$ through an active use of legal countermeasures (fines, prison sentences etc.). This strategy also assumes a high-enough detection rate P_{det}, otherwise the risk factor remains small for the counterfeiter.

The prevention-strategy works only if a counterfeit product cannot be successfully injected to the protected supply chain without paying the CTB, e.g. without forging the hard-to-copy security feature. In practice this means that security features need to be verified (i.e. products are authenticated), so the P_{det} needs to be high-enough for a successful prevention-strategy. Also the deterrence-strategy needs a high-enough P_{det} to be effective. Moreover, studies on supply of crime suggest that the probability of being detected and convicted has a bigger deterrent effect than the size of the punishment (Becker, 1968). Last, detection-based strategy shows that also P_{det} alone without any CTB and $P_{pun}F$ can render a counterfeiter's expected returns close to zero. In short, investigation of Equation V-5 and the three strategies for security reveals that *counterfeit product detection rate has a crucial role in decreasing a counterfeiter's returns.*

Moreover, Equation V-6 shows that P_{det} is a crucial factor also in cutting down the expected returns from a serial theft by revealing that increasing P_{det} has a higher-than-linear decreasing effect on E_s for low values of P_{det}. This effect is highlighted in the second form (second line) of Equation V-6, where the factor $(1 - P_{det})/P_{det}$ corresponds to the average number of times counterfeit article can be injected to the protected supply chain without being detected. For instance, for detection rates of 1%, 5%, and 10% this number is 99, 19, and 9, respectively.

V.1.3 How Much Security is Enough to Stop a Counterfeiter

Empirical observations shows that counterfeiters often do not try to forge the security features of genuine products, but they rather only imitate or even ignore them. Thus, counterfeiters have different *strategic options* to react to countermeasures. To answer how much security is needed to secure a supply chain from counterfeiters, all these strategic options need to be considered.

A counterfeiter's strategic options include i) injecting counterfeit products without the security features of genuine products, which is less expensive and more risky, ii) injecting counterfeit products with forged security features, which is more expensive and less risky, and iii) injecting counterfeit products with imitated security features, which places somewhere in between.

The conditions for security can be now derived directly based on the rational choice theory which assumes that people make decisions about how they should act by comparing the costs and benefits of different courses of action (e.g. Becker, 1968, 1976). Thus, *a supply chain can be considered secure against financially motivated risk-neutral counterfeiters if counterfeiters' all strategic options yield less than their opportunity cost.*

From an affected brand owner's point of view, the expected returns for a counterfeiter should be lower than the opportunity cost to target another company. For the society, however, this is not a solution since the harms are merely transferred to other licit businesses. From a societal point of view, the expected returns for a counterfeiter should thus be lower than the opportunity cost of engaging in legal business. Indeed, past counterfeiters can become future competitors or even partners (Hopkins et al., 2003). Note that deterring a new counterfeiter is easier than deterring a counterfeiter who has already targeted the brand. This is due to lock-in effects and the counterfeiter's switching costs.

Note that the aforementioned condition for a secure supply chain is only theoretic and can be

Table V-2: *Summary of a counterfeiter's strategic options*

Counterfeit product type	CTB	P_{det}	$P_{pun}F$	E
A: *Without security feature*	CTB_a	$P_{det,a}$	$P_{pun,a}F_a$	E_a
B: *With imitated security feature*	CTB_b	$P_{det,b}$	$P_{pun,b}F_b$	E_b
C: *With copied security feature*	CTB_c	$P_{det,c}$	$P_{pun,c}F_c$	E_c

only used as a general guideline; in particular, social scientists have discovered many cases where the assumptions behind the rational choice theory are not realistic. Relaxing those assumptions into a more realistic direction increases the needed level of security before a supply chain can be considered secure. In general, due to information asymmetries and bounded rationality[2] (Simon, 1955; Kahneman, 2003), E is not precisely known by counterfeiters. Counterfeiters can also be risk-preferrers who are not deterred by $P_{pun}F$ to the full extent (Becker, 1976). It is also known that individuals tend to value losses higher than gains, and out-of-pocket losses higher than opportunity costs (Kahneman, 2003). Moreover, the expected punishment in Equation V-5 is not constant but depends on the extent of the criminal activities and should thus be adjusted from case to case. Further studies are needed to assess the impact of these effects on the theoretical condition for a secure supply chain.

Table V-2 illustrates how a counterfeiter's strategic options can be analyzed (the letter subscripts denote the counterfeit product type). In general, $CTB_a < CTB_b < CTB_c$ and $P_{det,a} > P_{det,b} > P_{det,c}$, which means that counterfeiters pay for a decreased P_{det}. Analysis of counterfeiter's strategic options not only reveals how much security is needed but also what kind of security. In particular, making cost-to-break of the security feature higher than the loot value (here: $CTB_c > L$) only makes option C financially uninteresting ($E_c < 0$) but it does not secure the supply chain. Securing the supply chain also requires low E_a and E_b.

V.2 How to Affect the Detection Rate

After synthesizing existing knowledge on strategic-level effects of the process of security, this subsection investigates tactical-level effects that define the counterfeit product detection rate. These effects are summarized in Fig. V-3 and they have an important effect on the achieved effectiveness of a technical anti-counterfeiting measure. Besides screening effectiveness (cf. subsection IV.1) these effects have not been addressed in past studies. The following subsections investigate the mechanisms that define the P_{det} by focusing on the non-linear relation between P_{det} and the check rate.

[2] i.e. rationality of individuals is limited by the information they have, the cognitive limitations of their minds, and the finite amount of time they have to make decisions

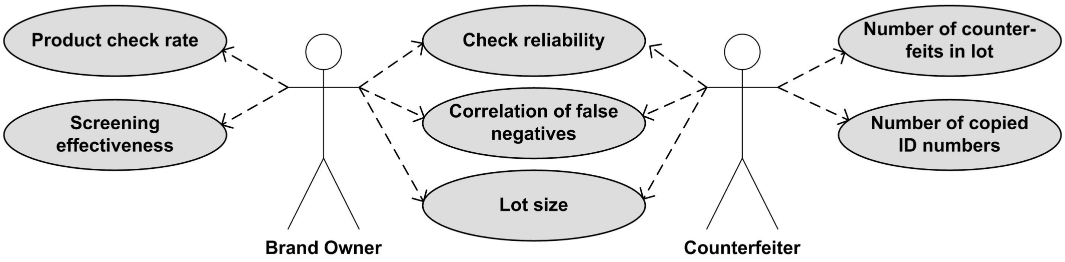


Figure V-3: *Illustration of the different ways how the brand owner and the counterfeiter can influence the counterfeit product detection rate*

V.2.1 The Effect of Lot Size and Co-Mingling

Products are not shipped individually but in lots or consignments. This has an important effect on P_{det} and as a result P_{det} is not a linear function of the check rate. When one counterfeit article is detected in a consignment, it can be assumed that the whole consignment is thoroughly inspected and all counterfeit products in the consignment are detected. This can greatly increase the effectiveness of checks. Moreover, counterfeit products are sometimes mixed, or *co-mingled*, among genuine products to decrease their chances of being detected, for instance by hiding counterfeit products under a layer of genuine products (e.g. Case study Xerox, CACP, 2009).

Let us investigate the following three cases. Randomly chosen samples of products that flow through a check point in the supply chain are authenticated. The ratio of authenticated products is denoted the check rate x which is one independent variable defining the P_{det}. In all these cases, in average $1/R$ of all products are counterfeits, and M denotes the lot size.

- *Case I:* Genuine products and counterfeit products flow in a supply chain individually without being aggregated to consignments ($M = 1$).
- *Case II:* Genuine products and counterfeit products flow in a supply chain in lot sizes $M > 1$. A consignment of counterfeit products contains counterfeit products only—in other words one in every $R \cdot M$ consignments, in average, contains counterfeit products only.
- *Case III:* Genuine products and counterfeit products flow in a supply chain in lot sizes $M > 1$. A consignment of counterfeit products contains N counterfeit products and $M - N$ genuine products that are co-mingled.

In *Case I*, x percent of products are authenticated and as a result $P_{det} = x$ percent of counterfeit products are detected in the check point:

$$P_{det} = x \tag{V-7}$$

In *Case II*, we assume that the authenticity checks are equally distributed among all consignments so that if L products in one consignment are authenticated, no less than L and no more than $L+1$ products are authenticated in other consignments. Also, if one counterfeit product is detected in a consignment, all counterfeit products in the consignment are detected. When $0 < x < 1/M$, one product is authenticated in $x \cdot M$ percent of the consignments and rest of the consignments flow through the check points without being checked. Thus, $x \cdot M$ percent of counterfeit products are detected. When $x \geq 1/M$, at least one product in every consignment is authenticated and thus all counterfeit consignments are identified and all counterfeit products are detected:

$$\begin{aligned} P_{det} &= x \cdot M, \text{ when } 0 \leq x < 1/M \\ P_{det} &= 1, \text{ when } 1/M \leq x \end{aligned} \tag{V-8}$$

In *Case III*, counterfeit consignments are less likely to be detected than in Case II since only N of the M products are counterfeits. When n products in a consignment are authenticated, the probability of detecting at least one counterfeit product is given by the hypergeometric distribution which describes the number of successes in a sequence of n draws from a finite population of M without replacement[3]. The probability of drawing exactly k counterfeit products in n draws from a population of M products with N counterfeits is given by:

$$HG(X = k) = \frac{\binom{N}{k}\binom{M-N}{n-k}}{\binom{M}{n}} \tag{V-9}$$

The probability of detecting that a consignment contains counterfeits when inspecting n randomly chosen products in a consignment containing counterfeits, denoted P^n_{det}, is given by:

$$P^n_{det} = \Pr\left(\text{at least 1 counterfeit detected}\right) = 1 - HG(X = 0) \tag{V-10}$$

Since each counterfeit consignment has the same number of counterfeit products, by detecting P^n_{det} percent of counterfeit consignments, in average P^n_{det} percentage of counterfeit products are detected. As a result, authenticating n products in every consignment leads to the following detection rate:

$$P^n_{det} = 1 - \frac{\binom{N}{0}\binom{M-N}{n}}{\binom{M}{n}} = 1 - \frac{\binom{M-N}{n}}{\binom{M}{n}} \tag{V-11}$$

The final form is achieved by marking $\binom{N}{0} = 1$. The check rate x is obtained from the number of checked products per consignment: $x = n/M$.

[3] Without replacement: a subject is not returned to the population after a draw

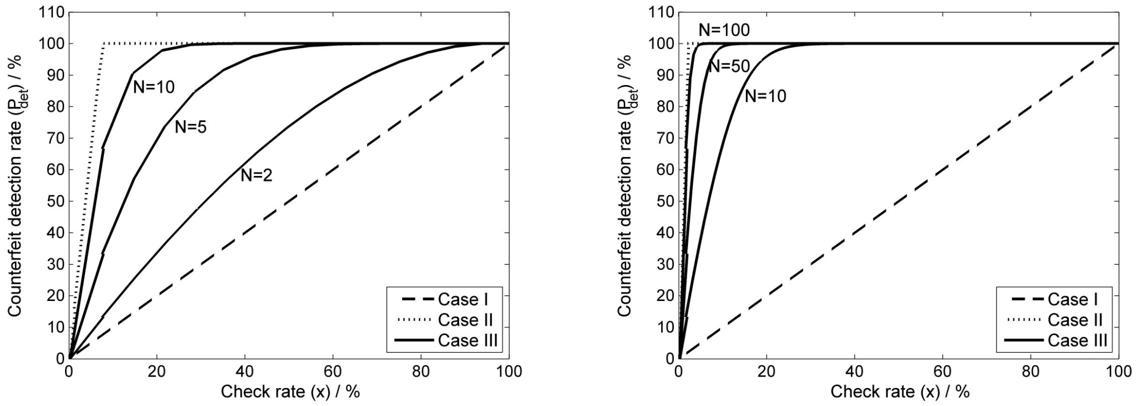


Figure V-4: *The effect of lot size and co-mingling on counterfeit product detection rate for lot sizes* $M = 15$ *(left) and* $M = 150$ *(right) (*$R = 100$*)*

Screening effectiveness (cf. subsection IV.1) represents the ability to select suspicious consignments based on risk analysis. This effect can be included in the formula of the achieved detection rate by multiplying the detection rate with a linear multiplicand (α), provided that the counterfeit consignment check rate does not exceed one (i.e. $\alpha \cdot x \cdot M \leq 1$). Staake estimates that risk analysis increases customs' ability to select suspicious consignments by a factor of 1.5 ($\pm 50\%$), i.e. $\alpha \approx 1.5$ (Staake, 2007, p. 57).

So far the additional checks that are conducted to investigate the whole lot when a counterfeit product is detected are not considered in the check rates of Cases II and III. In Case II, when $0 < x < 1/M$, the effective check rates are obtained by increasing the additional checks to x in the following manner. The effective check rate denoted as x' is given as:

$$x' = x + P_{det} \cdot (M - x \cdot M)/(M \cdot R) \qquad \text{(V-12)}$$

In a similar way, in Case III the effective check rate x' is given as:

$$x' = x + P_{det} \cdot (M - n)/(N \cdot R) \qquad \text{(V-13)}$$

The detection rates in Cases I-III, given by Equations V-7, V-8, and V-11, and taking into account the check rate corrections of Equations V-12 and V-13, are illustrated for $R = 100$ in Fig. V-4. Foremost, the figure demonstrates that increasing the lot size greatly increases P_{det}. In other words, a small lot size is a friend of the counterfeiter and a high lot size a friend of the brand owner. Indeed, the use of small lot sizes has been reported as a typical counterfeiter shipment strategy (Staake, 2007). A counterfeiter can counter this effect by co-mingling counterfeit products with genuine products (N approaches 1), which makes the P_{det} curve approach Case I where all products flow individually. But this is expensive for the counterfeiter since it forces him to dilate his profits by buying and selling genuine goods.

This numeric example illustrates that *lot size is a critical driver of the counterfeit product detection rate*. When counterfeit products are packed in consignments, a check rate x leads to the detection rate of $P_{det} > x$. *Counterfeiters can offset this effect by co-mingling counterfeit products with genuine products*. This reduces P_{det} but it is costly for the counterfeiter.

V.2.2 The Effect of Imperfect Inspections

The analysis of lot sizes presented above assumes that inspections are perfect, which means that every inspected counterfeit article is detected (i.e. $P_{reliability} = 1$). However, perfect security is a utopia or requires conditions that are impossible to fulfill in practice and thus no check can guarantee a 100% level of confidence (cf. Section IV); for example high-quality fakes can pass inspections as genuine products. Moreover, detection-based measures only rarely reach perfect detection rates since high detection rates tend to increase false alarm rates. Thus it is assumed for now that $P_{reliability} < 1$.

The effect of this assumption is analyzed for Case III detailed above. The probability that a counterfeit consignment is detected no longer equals the probability that at least one counterfeit product is inspected. When I is the random variable of the number of inspected counterfeit products when a counterfeit consignment is inspected, the probability that a counterfeit consignment is detected when n products are inspected among M products that contain N counterfeits, denoted P^n_{det}, can be expressed as follows:

$$\begin{aligned} P^n_{det} &= \sum_{i=1}^{N} \left[\Pr\left(I = i | n, M, N\right) \cdot \Pr\left(\text{at least 1 counterfeit detected } | I = i\right)\right] \\ &= \sum_{i=1}^{N} \left[Ins(i, n, M, N) \cdot Det(i)\right] \end{aligned} \tag{V-14}$$

The function Ins in Equation V-14 is the probability that i counterfeit products are inspected when n products are selected from a lot of M containing N counterfeits, and it can be expressed with the hypergeometric distribution (Equation V-9). The function Det stands for the effect of imperfect inspection rates and is thus a function of $P_{reliability}$. Two cases can be distinguished.

In the first case, $P_{reliability}$ is an *independent variable* for all counterfeit products within one consignment, which means that each counterfeit product in a consignment is independently detected with the same probability when checked. In this case, Det function depends on the number of authenticated counterfeit products i and Equation V-14 can be rewritten as follows:

$$P^n_{det} = \sum_{i=1}^{N} \left[\frac{\binom{N}{i}\binom{M-N}{n-i}}{\binom{M}{n}} \cdot \left(1 - (1 - P_{reliability})^i\right) \right] \tag{V-15}$$

In the second case, $P_{reliability}$ is a *dependent variable* and perfectly correlated among all counterfeit products within a consignment. It means that there is no random element in the authen-

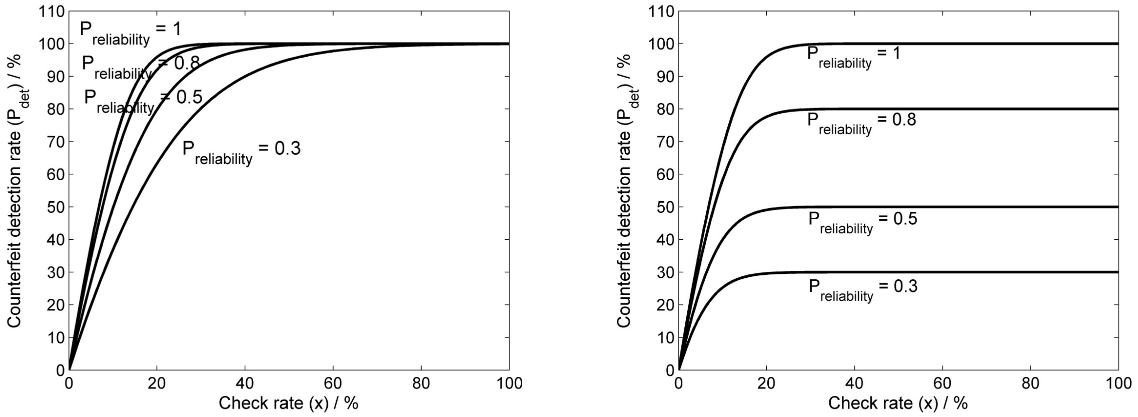


Figure V-5: *The effect of imperfect inspections on counterfeit product detection rate for independent (left) and dependent (right) check errors ($R = 100$, $M = 200$, $N = 150$)*

ticity check result between different counterfeit goods that belong to the same consignment; all counterfeit products in a same consignment either pass or do not pass the authenticity check. For instance, for RFID this could mean having the same secret key in all cryptographic RFID tags. In this case, Equation V-14 can be rewritten as follows:

$$P_{det}^{n} = \sum_{i=1}^{N} \left[\frac{\binom{N}{i}\binom{M-N}{n-i}}{\binom{M}{n}} \cdot P_{reliability} \right] \tag{V-16}$$

Figure V-5 (left) illustrates the effect of imperfect inspections in the case of independent check errors (Equation V-15) among counterfeits in the same consignment ($R = 100$, $M = 200$, $N = 150$). The numeric example shows that *decreasing the inspection success rate has a clear decreasing effect on the overall counterfeit product detection rate*. This negative effect of inspection errors is linear when one product per consignment is inspected, and smaller than linear in higher inspection rates. Fortunately this *negative effect can be effectively countered by increasing the inspection rate*, and even small inspection success rates can yield high detection rates when the check rate is increased far enough. This is a somewhat brute-force strategy, but nevertheless an effective way to counter the effect of imperfect checks.

Figure V-5 (right) illustrates the effect of imperfect inspections in the case of dependent and perfectly correlated check errors (Equation V-16) in the same consignment. This example demonstrates the linear negative effect of decreasing $P_{reliability}$. In this case the negative effect cannot be offset by increasing the detection rate.

From the brand owner's point of view, in the optimal case the false negatives are independent among all products in a consignment so that the possible false negatives can be offset simply by verifying more products. The dramatic negative effect on counterfeit detection rate can be explained as a *class-break* (Schneier, 2003) where the exploitation of one vulnerability can compromise multiple subjects. The lesson for the anti-counterfeiting is to *avoid class-breaks*, otherwise increasing the number of authenticated samples will not increase the changes of detecting a counterfeit consignment.

V.2.3 The Effect of Number of Copied Identifiers

This subsection investigates the situation where a counterfeiter has less valid serial numbers at his disposal than the number of products in one consignment. This can be a realistic assumption for higher lot sizes when the serial numbers are issued randomly. The validity of serial numbers can be verified online from a ”white list” Koh et al. (2003) or offline with a digital signature (cf. subsection II.4.2). Let us investigate the case where a consignment of M counterfeit products has only $C < M$ different valid serial numbers (i.e. there are multiple counterfeit articles with the same serial number). The inspection consists of reading the serial numbers of n randomly chosen products per consignment and an alarm is triggered if the same serial number is observed twice.

The probability of detecting a counterfeit consignment in this case is derived from series $s = s_1, s_2, ..., s_M$ which represents the probabilities that a new (not previously observed) serial number is observed each time when a new product is randomly chosen from the consignment. For mathematical simplicity, it is assumed that each of the C copied ID numbers is copied to the same number of counterfeit products in the consignment ($M \, mod \, C = 0$), this number being M/C. Drawing a new serial number decreases the number of remaining unobserved serial numbers by M/C in each draw while decreasing the number of remaining products by one. The n^{th} element of series s can therefore be expressed as:

$$\begin{aligned} s_n &= \frac{M - \frac{M}{C}(n-1)}{M-n+1}, \text{ when } 1 \leq n \leq C \\ s_n &= 0, \text{ when } n > C \end{aligned} \tag{V-17}$$

Values of s are naturally zero when the number of verified products exceeds the number of different ID numbers. Now the probability of detecting the counterfeit consignment in an inspection can be expressed as:

$$P_{det}^{n} = 1 - \prod_{i=1}^{n} s_i \tag{V-18}$$

Equation V-18 yields accurate estimations when $M \, mod \, C = 0$, but it can be used to give approximative estimations also when C is not a factor of M (e.g. a lot of 100 counterfeit products has 40 different ID numbers). Last, the check rate needs to be corrected to take into account the additional verifications that happen when a counterfeit consignment is detected:

$$x' = x + P_{det}^{n} \cdot (M - \frac{n}{M})/(N \cdot R) \tag{V-19}$$

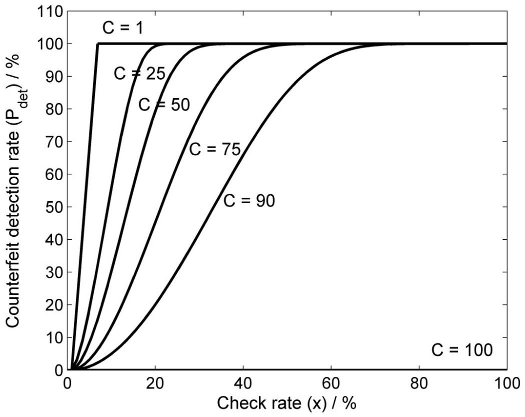


Figure V-6: *The effect of the number of copied identifiers (C) in a consignment on counterfeit product detection rate ($M = 100$, $R = 100$)*

The dynamics of Equation V-18 are illustrated in Fig. V-6 for different values of C, when $M = 100$ and $R = 100$. On small product check rates of about 2-3% C needs to be about 50 for a counterfeit product detection rate of about 2%. In other words, a small check rate allows the counterfeiter to use same serial numbers in multiple products of the same consignment without a considerable risk of being detected in the described inspection. When the check rate increases tenfold to about 20-30%, however, having even a small number of duplicated codes in a consignment becomes risky for the counterfeiter. With these elevated check rates, the benefits of ”recycling” same serial numbers are small for a counterfeiter compared to the involved risk, and the risk of detecting duplicated use of the same serial number increases. As a conclusion, mass serialization will pose challenges to counterfeiters and potential serialization errors can be used to detect counterfeits, even when the check is conducted without a network connection.

V.3 Summary and Guidelines

Counterfeit product detection rate is a good metric for the effectiveness of a technical anti-counterfeiting system since it represents the direct effect of security and is a defining variable behind the deterrent effect of security. This analysis shows that counterfeit product detection rate is not a linear function of the check rate but it follows a law of diminishing marginal utility, which suggests that the good enough security paradigm (Sandhu, 2003) holds true for what comes to the check rate. Overall, check rates of some tens of percents appear high-enough to detect the majority of counterfeit products flowing through a check point.

Moreover, brand owners (and counterfeiters) can affect the detection rate through multiple levers that are illustrated in Fig. V-7. The practical consequences are presented as guidelines for the anti-counterfeiting in the information box below.

The economic conditions for considering a supply chain secure from financially motivated

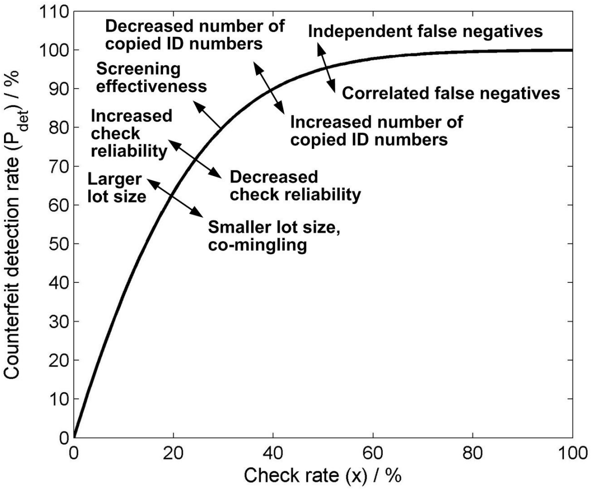


Figure V-7: *Illustration of mechanisms that define the counterfeit product detection rate*

counterfeiters need to include making injection of all kinds of counterfeit products a losing proposition for counterfeiters. The theoretical implication is that the payoffs of adversaries all strategic options need to be considered. In particular, this means that having a security feature the cost-to-break of which is greater than the illegal profit from selling a counterfeit article is an insufficient condition for securing a supply chain, since selling counterfeit articles that do not have security features or that have imitated security features might still be profitable.

The second theoretical implication of this analysis is showing that even though security is provided by multiple subsequent prevent-detect-respond processes, the overall effect of the countermeasures can still be modeled by one process of security where the cost-to-break is extended to include the risk factors of the early countermeasures. In practice this can mean, for example, that the cost-to-break of robbing a bank should include the risk of being punished from buying an illegal handgun. Overall, this supports the existing view that evaluating the cost-to-break is hard and impractical (e.g. Schechter, 2004).

Though the presented econometric study provides various insights to technical countermeasures, the presented models are only simplifications of parts of the problem and they do not provide an integrated view of all the involved dynamics. To evaluate the overall detection rate that takes into account all the presented effects, the distinct effects should be integrated. The formulas of check rates do take into account the increased workload due to inspection all products in detected counterfeit consignments, but they nevertheless do not represent the complete effort to conduct the authenticity checks. The overall check rate itself does not take into account the fact that checking 10 products in 1 consignment is easier than checking 1 product in 10 consignments. A more realistic understanding of the involved effort can be obtained by calculating the number of samples that are authenticated in each consignment.

Lessons for Anti-Counterfeiting

- *Product check rate:* Increasing the available resources for authenticity checks is a straightforward way to increase the counterfeit product detection rate. Increased check rates increase the counterfeit product detection rate according to a law of diminishing marginal returns.

- *Screening effectiveness:* Risk analysis can increase the effectiveness of checks by targeting suspicious consignments, but the screening process should also contain a random element so that it cannot be bypassed (cf. subsection IV.1).

- *Lot size:* High lot size is a friend of the defender since it allows detecting multiple counterfeit products based on only a few authenticated products. Small lot size decrease the chances of detecting counterfeits as well as the value of the confiscated merchandise. Moreover, small lot sizes make it easier for counterfeiter to bypass off-line checks that look for repeated use of same copied ID numbers within consignments.

- *Number of counterfeits in a lot (co-mingling):* Counterfeiters can offset the effect of high lot sizes by co-mingling counterfeit products with genuine products, but this dilutes the profits from counterfeit products.

- *Check reliability:* Though the ideal goal is that 100% of inspected counterfeit products are detected, the effect of false negatives can be offset by increasing the product check rate if the false negatives are not correlated (cf. below). Moreover, a 100% check reliability should not come at the expense of smaller check rates (cf. subsection VII.1).

- *Correlation of false negatives:* In the optimal case for the brand owner, false negatives are independent among all products in a consignment so that checking additional counterfeit products increases the probability of detecting the counterfeit consignment. Dependent false negatives can be avoided by using unique security features in all products, i.e. unique serial numbers and secret keys.

- *Number of copied ID numbers:* When the validity of serialized ID numbers can be verified, valid ID numbers can become a scarcity for the counterfeiter and use of the same serial number in more than one product within a consignment can be detected.

VI Product Authentication Concepts for Low-Cost RFID

The review of related work on RFID security in Section III shows that secure product authentication with low-cost RFID has not yet been solved. Even though secure tag authentication based on strong cryptography and physical unclonable functions (PUFs) have been demonstrated on passive RFID devices with minimal hardware implementations, these approaches will not solve product authentication for low-cost RFID because of the following reasons:

- Though the implementations are minimalistic, they still increase the chip area by some thousands of gate equivalents (Feldhofer, 2008), which currently increases the chip cost. (However, this increase might become negligible in the future due to advances in chip manufacturing.)
- Being a specialized product, these chips will have a cost disadvantage compared to simpler chips due to smaller economics of scale (e.g. the non-recurring engineering costs need to be depreciated by a smaller volume).
- Being a specialized product, chip and tag manufacturers can ask higher price premiums from these chips than from more simple chips (i.e. the profit margin is higher).

To authenticate products based on low-cost RFID, the research community has discussed approaches based on detection of cloned tags. These approaches are technically simple to implement since they do not require additional tag hardware resources, but actual contributions in this field are scarce and mostly limited to concept proposals. Only Mirowski and Hartnett (2007) detail a system that detects cloned tags based on RFID traces, but the system is prone to false alarms and does not fully exploit the location and time information of RFID traces.

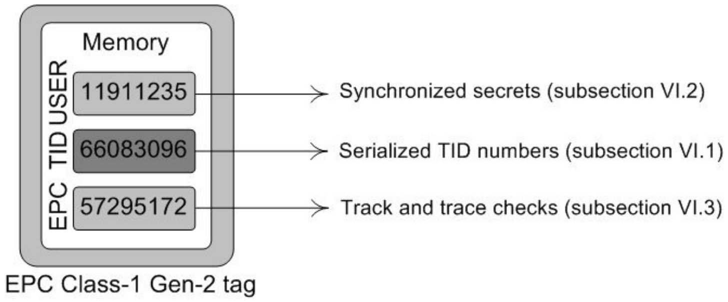

Memory
EPC
TID
USER
11911235
66083096
57295172
Synchronized secrets (subsection VI.2)
Serialized TID numbers (subsection VI.1)
Track and trace checks (subsection VI.3)
EPC Class-1 Gen-2 tag

Figure VI-1: *Overview of the evaluated product authentication concepts*

This section investigates product authentication concepts that are available for existing low-cost RFID tags (cf. Fig. VI-1). First, tag authentication based on transponder ID (TID) numbers is evaluated. This is an existing concept that is already used in practice[1], but its security has

[1] RFIDJournal (2008). http://www.rfidjournal.com/article/articleview/2075/1/9/

not yet been formally analyzed. The contribution of this section is to evaluate the cost-to-break of TID-based tag authentication. Then, two new product authentication concepts are presented and evaluated. They include an approach to detect tag cloning based on synchronized secrets and an approach to detect cloned tags from incomplete RFID traces. To demonstrate the practical relevance of these approaches this section focuses on EPC Gen-2 tags, though both developed concepts can be implemented with all RFID tags that have a unique identifier and rewritable memory. Overall, these three contributions are based on three conference papers published in 2009 (namely: Lehtonen et al., 2009d,c,b) and the practical findings of each study are summarized as guidelines in the end of the corresponding subsection.

VI.1 Tag Authentication Based on Serialized TID Numbers

Though transponder ID (TID) numbers of RFID tags were originally introduced to identify the chip model, serialized TID numbers are currently advertised as security features of UHF chips. Serialized TID numbers do not provide any cryptographic protection, but they do introduce a practical hurdle against adversaries who want to clone RFID tags today. Furthermore, serialized TID numbers are important for end-users who want to protect their current passive UHF tags from cloning since strong tag authentication measures are not yet commercially available on that frequency range.

On the one hand, serialized TID numbers can be a big headache for RFID crackers who want to clone tags. While a tag's EPC number can be easily reprogrammed, changing the write-protected TID number is considerably harder. As a result, chip manufacturers advertise the serialized TID numbers as security features of Gen-2 chips.

On the other hand, the use of serialized TID numbers as security features represents a big opportunity for RFID crackers. In contrast to cryptographic tags, serialized TID numbers do not provide any logical or mathematical barriers against tag cloning. For instance, there is nothing that prevents an adversary from reading the serialized TID number of a tag and transmitting this number to a reader to impersonate this tag. In addition, if chips with programmable TID numbers became commercially available, cloning serialized TID numbers will become as easy as cloning EPC numbers.

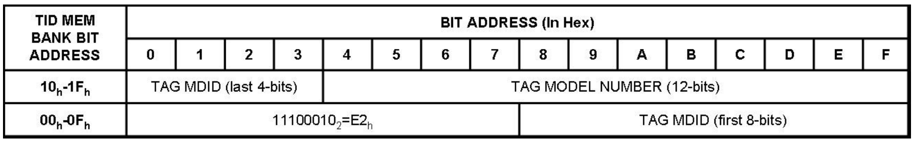
Despite these obvious vulnerabilities of the TID scheme, it would nevertheless be incorrect to claim that serialized TID numbers do not provide any protection against tag cloning and impersonation; since RFID tags with programmable TID numbers are not available in the market today according to the best of the author's knowledge, it is currently not easy for an adversary to obtain a passive RFID tag with a wanted serialized TID number. Because of this dilemma, end-users have a reason to be confused about the usefulness of serialized TID numbers in security applications. To support potential end-users, this subsection evaluates the effort to bypass the TID check based on the known vulnerabilities.

VI.1.1 Technical Primer

TID Standards

The purpose of the TID memory bank of EPC tags (cf. Fig. VI-1) is to identify the chip type and the possible custom commands and optional features the chip supports. This can be done without unique identification of the chip and thus the EPC TID number format does not require serialization of the TID numbers. When the TID number is appended with a unique serial number, such as in the ISO TID format, it also identifies the unique chip.

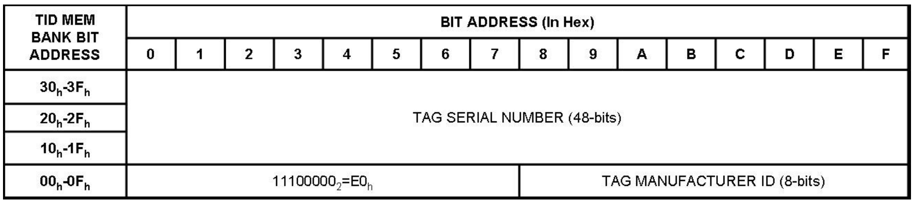
TID numbers begin with an 8-bit ISO/IEC 15963 Allocation-Class (AC) identifier (EPCglobal Inc., 2005b). The ISO/IEC 15963 standard describes the mechanism to guarantee uniqueness of the TID numbers and presently four organizations have been assigned an AC identifier (Främling et al., 2007). The allocation-class identifier for EPCglobal is $11100010_2 = E2_h$.[2] For tags whose AC identifier is $E2_h$, the EPC Gen-2 standard requires that the TID memory be comprised of a 12-bit Tag Mask-Designer Identifier (Tag MDID) and a 12-bit Tag Model Number. According to the Gen-2 air interface specification (EPCglobal Inc., 2005a), the TID memory may also contain tag and vendor-specific data such as the serial number. The content of the TID memory bank defined by existing EPC standards is illustrated in Fig. VI-2.



TID MEM BANK BIT ADDRESS	BIT ADDRESS (In Hex)															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
10_h-$1F_h$	TAG MDID (last 4-bits)				TAG MODEL NUMBER (12-bits)											
00_h-$0F_h$	11100010_2=$E2_h$								TAG MDID (first 8-bits)							

Figure VI-2: *TID memory structure in the EPC standards (EPCglobal Inc., 2005b)*

For tags whose AC identifier is $E0_h$, the ISO/IEC 15963 requires that the TID memory comprise of an 8-bit tag manufacturer ID and a 48-bit tag serial number. Furthermore, the standard requires that the TID memory be permalocked. The ISO TID structure is illustrated in Fig. VI-3.



TID MEM BANK BIT ADDRESS	BIT ADDRESS (In Hex)															
	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
30_h-$3F_h$	TAG SERIAL NUMBER (48-bits)															
20_h-$2F_h$																
10_h-$1F_h$																
00_h-$0F_h$	11100000_2=$E0_h$								TAG MANUFACTURER ID (8-bits)							

Figure VI-3: *TID memory structure in the ISO standards (EPCglobal Inc., 2005b)*

The upcoming EPC Tag Data Standard (v. 1.5) is likely to make locking the TID numbers mandatory and define a way to specify serialized TID numbers. This is likely to be done with

[2] Subscripts 2 and h stand for binary and base-16 (*hexadecimal*) number formats, respectively

an extended tag identification number (XTID) that extends the current EPC TID format with an 48-bit (or more) serial number and information about key features implemented by the tag. Though chip manufacturers can still opt for a non-serialized version of the TID within this scheme, the new standard is presumed to foster the adoption of serialized TID numbers.

Tag Memory

TID numbers can be written on Read Only Memory (ROM) and Electronically Erasable Programmable Read Only Memory (EEPROM) (for more details of tag memory cf. subsection II.3.3). EEPROM is re-programmable by design but it can be protected from rewriting by implementing a *permalock* command. This can be done in different ways. For example, the chip's write command might work only while the chip is on the wafer in the test state, and once the the chip is physically altered to end the test state (e.g. by breaking a connector, by burning a fuse etc.), the write commands are no longer executed by the chip's internal logic. These ways can be used only by the chip manufacturer. Another way is to make use of a lock-bit that can only be flipped once. All read commands to a certain part of the memory first check whether the corresponding lock-bit is flipped and get executed only if the memory is still open (e.g. Sandvos and Alton, 1996). This enables a permalock command that can be used at any time during the chip's lifetime.

VI.1.2 TID-Based Authentication

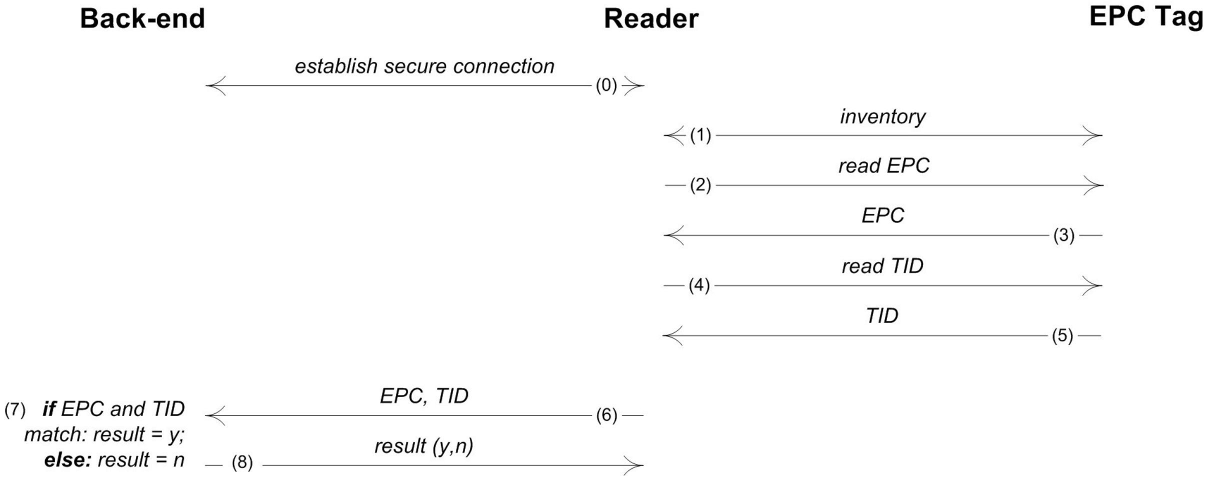


Figure VI-4: *TID-based authentication protocol for EPC tags*

The TID-based tag authentication protocol (in short: the TID check) between an EPC-tag, a reader, and a back-end goes as follows (cf. Fig. VI-4). To initiate the communication, the reader and back-end need to establish a secure connection channel (0) through mutual authentication and encryption, so that the reader knows that he is communicating with the authorized back-end and that the integrity of the messages is provided. When a tag enters the reader field, the reader first performs the inventory command (1) to learn which tags are in its field and then reads the tag's EPC number (2-3) and TID number (4-5). The reader sends the EPC and TID numbers to the back-end (6) which verifies if they match (7) and responds whether the tag passed the check or not (8).

VI.1.3 Vulnerabilities in TID-Based Authentication

This subsection analyzes the known vulnerabilities of the TID check. These vulnerabilities spur from Koscher et al. (2008) and from a general understanding of the tag manufacturing process, subsection II.3.3, and they are illustrated in as a misusecase diagram in Fig. VI-5.[3] The effort to exploit different vulnerabilities is evaluated in monetary terms or other resources as far as it makes sense and can be done under general assumptions.

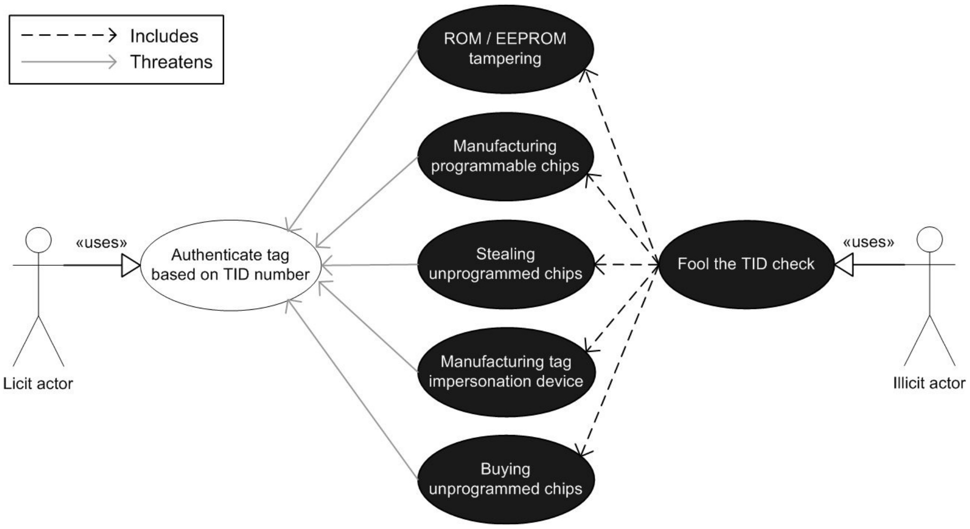

Includes
Threatens
ROM / EEPROM tampering
Manufacturing programmable chips
Stealing unprogrammed chips
Manufacturing tag impersonation device
Buying unprogrammed chips
«uses»
Authenticate tag based on TID number
Licit actor
Fool the TID check
«uses»
Illicit actor

Figure VI-5: *Vulnerabilities of TID checks*

EEPROM and ROM tampering

One way to clone tags with serialized TID numbers, in theory, is to purchase standard tags and to manipulate the content of their TID memory. Even though standard tags' TID memory banks are write-protected (cf. subsection VI.1.1), there are ways to bypass this protection. TID memory bank can be implemented both as EEPROM and ROM, ROM being a possible memory structure only for the non-serialized parts of TID numbers. Both these memories are vulnerable to physical tampering if suitable equipment and knowledge are available.

Tampering of EEPROM and ROM has been discussed in the field of smart card security. The general rule is that the more sophisticated the chip structure is (e.g. higher manufacturing

[3] This analysis focuses on tag authentication so tag removal and reapplying attack is not considered here

precision), the more expensive the equipment needed to tamper with it. The difficulty in these techniques is that the adversary needs to know or find out which parts of the physical chip (e.g. transistors) to tamper with, and the attacks can also damage nearby portions of the integrated circuit.

The cost of equipment to manipulate ROM memory starts from tens of thousands of dollars. Specialized failure analysis laboratories can provide pieces of the necessary physical analytical services at rates around USD 400 per hour (Asanghanwa, 2008). For example, an electron beam of a conventional scanning electron microscope can be used to read, and possibly write, individual bits in ROM and EEPROM. To do this, the surface of the chip must be first exposed, usually via chemical machining (Weingart, 2000). Single bits in a ROM can be overwritten using a laser cutter microscope and EEPROM can be altered using two microprobing needles (Anderson and Kuhn, 1997).

Focused Ion Beam (FIB) is perhaps the most powerful equipment to analyze and tamper with the structure of integrated circuits. FIB tools are scientific instruments that resemble a scanning electron microscope and they are used, for example, to locate failure sites within EEPROM memory microcircuits (Haythornthwaite et al., 2004). FIB can be used to modify the hardware circuitry in different ways as it can change a hardwired ROM cell and in principle also modify an EEPROM cell. This technique corrupts the EEPROM cell forever, which means that rewriting is no longer possible, though this might not be a problem for an d. In some cases, FIB can also restore test circuitry in smart cards by restoring a fuse that has been blown to physically prevent access to the test state (Poll, 2007). According to Kömmerling and Kuhn (1999), using laser interferometer stages, a FIB operator can navigate on a chip surface with 0.15 μm precision. Using laser-interferometer navigation or infrared laser imaging it is possible to locate individual transistors. Modern FIB workstations cost less than half a million USD and are available in over hundred organizations (Kömmerling and Kuhn, 1999).

Security of TID numbers can also be investigated by drawing an analogy with the MAC (Medium Access Control) addresses of network cards. The MAC address is a unique 48-bit integer that identifies all network cards. Hardware manufacturers purchase blocks of addresses from the IEEE Registration Authority and assign unique addresses to their cards. Every company is responsible for ensuring that every manufactured unit gets a unique address (Grand, 1998).

There are various motivations to rewrite MAC addresses of network cards. Licit reasons for rewriting it include replacing a broken network card by a new one without having to reconfigure the networking software which is not always easy or possible. However, also illicit reasons exist, for example, bypassing a mechanism that limits the use of software to authorized network cards, bypassing a restriction of Internet service providers that limit the use of a connection to one computer, and falsifying the source of Internet traffic.

Most network cards store the MAC address in a separate EEPROM chip that can be removed and reprogrammed using off-the-shelf EEPROM programmer kits. There also exist software-based solutions to rewrite the MAC addresses of network cards (Grand, 1998). In addition, it is possible to buy network cards with fully programmable MAC addresses[4]. Furthermore, in some cases it is enough to change the MAC address in higher levels of communication protocols for a successful spoofing attack.

From a technical point of view, rewriting the MAC address of a network card appears to be easier than rewriting the TID number of an RFID tag. First, reprogramming the memory where the MAC address is stored is substantially easier than tampering with the memory on RFID tags IC when the MAC address is stored in a separate EEPROM chip that can be connected to a programming kit. Second, there are ways to program MAC addresses based on software, whereas mechanisms to rewrite TID number should not exist after TID memory has been permalocked. Third, compared to manufacturing RFID tags with programmable TID numbers, manufacturing network cards with programmable MAC addresses appears easier since it can be done using standard components. The promising result is that TID numbers seem to offer greater protection against rewriting than MAC addresses, as well as less licit reasons for doing it.

Manufacturing Programmable Chips

If any existing chip manufacturer would sell UHF chips with programmable (unlocked) TID memory, the security of the TID checks would be completely undermined; an adversary could simply buy an empty chip and write the wanted TID number on it. Current EPC standards do not require permanently locked TID memory banks, but according to the best of the authors' knowledge all available EPC chips have their TID memory locked (cf. review of chip manufacturers below). Chips with programmable TID numbers would cause discontent among companies who use TID as a security feature. It appears that the current UHF chip manufacturers recognize their responsibility in securing the TID scheme and that they act accordingly. However, it is possible that such chips will be provided to the market if they will be—for any reason—demanded by the market.

Overall, nothing would prevent a semi-conductor foundry from manufacturing fully programmable chips and a chip manufacturer from selling them. This can be seen as somewhat analogous to what happened with MAC addresses of network cards, though it must be noted that there are good *licit* reasons for network cards with programmable MAC addresses, whereas there are no known licit reasons for RFID chips with programmable TID numbers.

In addition to existing chip manufacturers also a new entrant could start producing and selling chips with programmable TID numbers. According to expert interviews, the biggest effort in manufacturing such chips is in the IC design that includes both an analog radio-frequency part and a digital part. The IC design projects of modern Gen-2 chips cost several millions of dollars and can last two to three years. However, these projects include many activities that would not be necessary for a manufacturer of programmable chips, perhaps most importantly optimization of the chip size and price. According to expert estimates, the minimum effort to

[4] e.g. from http://www.sdadapters.com

make an IC design is in the range of hundreds of thousands of dollars in general. There are at least tens of semi-conductor foundries who could produce the chips, though the potentially small production volumes would increase the price per chip.

We derive a rough estimate of what programmable chips could cost in small quantities. Chip manufacturers sell modern Gen-2 chips around EUR 0.05 - 0.07 apiece today and the total price of the resulting RFID label would be around EUR 0.15 - 0.20 (in volumes of tens of thousands). This chip price includes the chip manufacturer's variable manufacturing cost per chip, fraction of the fixed costs like IC design (depreciation), and the chip manufacturer's profit. When manufacturing programmable chips in smaller quantities, the fixed costs (e.g. IC design and configuring wafer production line) are divided by a much smaller number of chips. In addition, assuming a less optimized IC design, the price per chip could be 10 to 100 times bigger than that of the most popular UHF chips, and the resulting price of a single programmable RFID label would be around EUR 0.60 - 7.15.

Stealing Unprogrammed Chips

In theory, a wafer could be stolen early enough in the manufacturing process by an adversary who wants to write specific TID numbers on the chips. However, also this would require an investment in equipment to write the chips and since this approach is not easily scalable, it would be hard to obtain the volumes that would justify the investment. Furthermore, wafers are high-value articles that are tracked and traced both inside and outside the factories (e.g. when transported from semi-conductor fabrication plant to the chip manufacturer) and therefore stealing them would neither be easy nor go unnoticed. The risk of stealing unprogrammed chips can therefore be considered low.

Tag Impersonation Device

Another option to bypass the TID check is to build a device that effectively emulates or imitates an RFID tag, without the need for IC manufacturing. This kind of device could fool the inspections if the impersonation device is not seen during the check. This could be done in practice, for example, when pallets or cases of goods are verified by distributors or customs and the impersonation device is hidden inside the package. In addition, in case when the tag is not a label but a hard tag (encapsulated tag), the spoofing device could be built inside it (cf. Fig. VI-7). These kinds of encapsulated tags are used in applications requiring longer life cycle for the tag or tolerance for harsh conditions.

Achieving adequate functionality and performance for such a device is possible even with moderate effort and costs and without special equipment. Moreover, the effort can be further decreased by using a RFID tag hardware and software developer platforms such as the WISP[5].

[5] Intel (2009). http://www.seattle.intel-research.net/WISP/

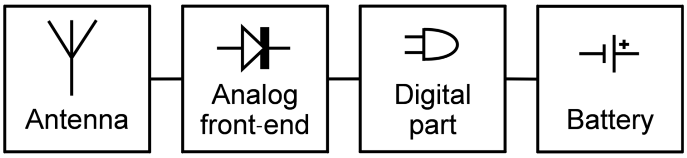


Figure VI-6: *Block diagram of semi-passive impersonation device*

To evaluate and illustrate the feasibility of an attack based on a tag impersonating device built from the scratch, an implementation of a semi-passive RFID tag is presented. This implementation and the corresponding evaluation are done by Antti Ruhanen as a part of the work in BRIDGE project WP4 (security work package)[6]. A generic block diagram of a tag impersonation device is illustrated in Fig. VI-6. The hardware blocks are described below.

- *The antenna* can be a simple half-wave dipole. It can be easily fabricated by anyone.
- *The analog front-end* should be capable to detect the reader signal and to create backscatter modulation during reply. As the receiver does not need to be very sensitive or frequency selective, fairly unsophisticated structures can be used. A simple rectifier, envelope detector, and a comparator are enough (Aigner et al., 2008). More complex and better performing front-end designs can be found in the literature (e.g. Barnett et al., 2007). Backscatter modulation can be done with a single transistor.
- *The digital part* implements the actual communication protocol. The protocol description is publicly and easily available and protocol emulation can be implemented by using a microcontroller or a Field Programmable Gate Array (FPGA). This is the most challenging part and will be discussed later. The chip used for protocol emulation is also the most expensive component of such impersonation device.
- *The battery* provides operating power for the digital part and the battery voltage can also be utilized to make the front-end more sensitive.

Implementing the protocol without prior knowledge requires a serious effort, but the communication protocol is open and standardized which makes it easily available for anyone and, demonstrably, the protocol emulation can be done (e.g. it is done by Aigner et al., 2008; Mitsugi, 2006; SecureRF Corporation, 2007). For example, the Gen-2 protocol has been successfully implemented as a part of the RFID security research in the BRIDGE project in a microcontroller (Aigner et al., 2008). The used microcontroller is a very lightweight and inexpensive controller with a 8 MHz clock rate. Due to the slow clock rate, all mandatory data rates are not supported by the prototype. The cost of the microcontroller is only few euros and the total bill of materials is less than 10 euros. The prototype is demonstrated in Fig. VI-7.

[6] BRIDGE (2009). http://www.bridge-project.eu/index.php/workpackage4/en/

Implementation of the protocol with supporting functions is mainly done in the C language. The total amount of source lines of code within the protocol implementation is around 2300. By using a basic COCOMO-model (*The COnstructive COst MOdel*[7]) with embedded project coefficients, the estimated effort for the implementation is around 10 man months. These numbers roughly reflect the required effort for software based protocol implementation with a microcontroller.

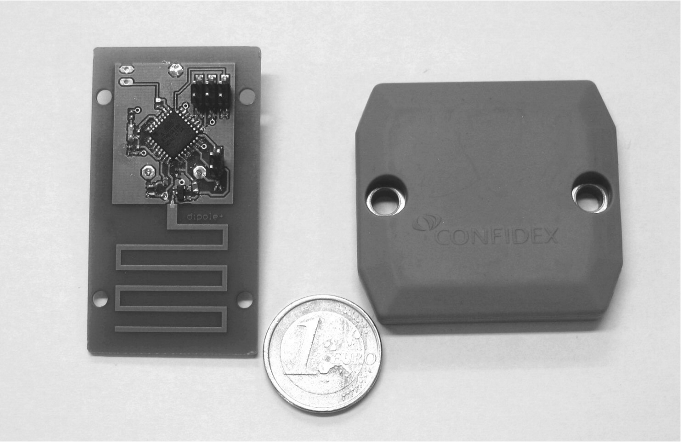


Figure VI-7: *Programmable semi-passive tag prototype that can impersonate EPC tags (left) and a commercial encapsulated tag (right) (Courtesy of Confidex Oy)*

To achieve total conformance with the Gen-2 protocol, a faster and more expensive microcontroller should be used. The problem is to meet the timing requirements of the physical layer with higher communication data rates. However, an adversary who is implementing the protocol does not necessarily need absolute compliance with the standard since all features of the protocol are not likely to be needed in a basic TID check.

A tag impersonation device can also be implemented based on a Field Programmable Gate Array (FPGA) instead of a microcontroller. FPGA implementation is closer to a real hardware implementation and in general requires more effort with Register Transfer Level (RTL) code than a similar task in the C language and a microcontroller. Since the physical design can be omitted, it is still significantly less than a real application-specific integrated circuit (ASIC) design effort (cf. subsection VI.1.3). The required speed should be easy to achieve with an FPGA so, in contrast to a microcontroller, higher data rates should not be a problem. Present Gen-2 chips include roughly 40,000 transistors (Roberti, 2005) which indicates that even a low-cost FPGA is sufficient to implement the same functionality. Prices of such FPGA chips start from ten euros. Also other fixed, non-recurring engineering (NRE) costs are comparable to microcontroller implementation and are only a fraction compared to ASIC design NRE costs.

[7] Center for Systems and Software Engineering (2008). Basic COCOMO-model. http://sunset.usc.edu/csse/research/COCOMOII/cocomo81.htm

Review of Gen-2 Chip Manufacturers

Commercially available Gen-2 chips or tags with not-permalocked and programmable TID memory would make TID number cloning very easy for adversaries, and the cost-to-break would be the market price of such a chip or tag. This subsection reviews how major Gen-2 chip manufacturers secure the TID memory of their products. The presented review is summarized from interviews with chip manufacturers and from product catalogs[8], and the results are summarized in Table VI-1.

- *NXP:* The currently available UHF chips from NXP include UCODE G2XM, UCODE G2XL, SL3 ICS1001, SL3 ICS3101, and SL3 ICS3001. All these chips have unique write-protected transponder ID numbers already today. The tag identifier in the UCODE chips is 64-bit long and includes a 32-bit unique serial number. These TID numbers are written in the TID memory bank of the Gen-2 tags. NXP uses a 140 nanometer manufacturing process. The non-serial part of the TID numbers is not defined by the chip mask but it is programmed to the tag as well. The TID memory is locked by destroying bridges, that is connectors on the surface of the chips, after the TID numbers are written and the tags are tested on the wafer. This happens before cutting the chips from the wafer. After these bridges are destroyed, the TID write command no longer works and even the manufacturer cannot change the TID values. According to the company, NXP would not sell chips with programmable TID numbers to the market since it has been a reliable supplier for security products for years and has a reputation and a brand to maintain.

- *Impinj:* The currently available UHF RFID chips from Impinj comprise Monza, Monza/ID, and Monza/64. Of these chips Monza/ID has a serialized 64 bit transponder ID that is factory-programmed and the other chips have only short, non-serialized TID numbers. The serial part of Monza/ID chip's TID memory is written in the user memory. The non-serial part is defined in the chip-mask and written as hard-wired ROM (cf. subsection II.3.3), and the serial part is permalocked using a lock-bit. Locking is done before cutting the chips from the wafer. In the near future, all UHF chips from Impinj will have serialized TID numbers.

- *Alien:* The current UHF RFID chip ICs of Alien Technology include Higgs-2 (H2) and Higgs-3 (H3). H2 has a 32-bit non-serial TID written in ROM and an optional factory-programmed 32-bit serial number that is written on the chips if needed. Vast majority of the H2 chips in the market do not have serialized TID numbers because the market has only recently started to demand them. H3 chips have the serialized TID number as a standard feature and the company predicts that in two years all UHF chips they sell will have serialized TID numbers. The serialized TID numbers are written during the inlay production process and protected in a *foundry protect* process that disables the

[8] This review dates to Autumn 2008

chip's internal commands for rewriting the TID memory. Alien uses a 160 nanometer manufacturing process.

- *TI:* UHF Gen2 STRAP contains 32-Bit TID Memory (Factory Programmed and Locked). In HF products, TI has chips with 64-bit Factory Programmed Read Only Numbers. According to official documentation, the TID bank is permanently locked. TI uses a 130 nanometer manufacturing process that is currently state-of-the-art in RFID, which makes TI's chips the hardest to tamper with using intrusive techniques like FIB (cf. subsection VI.1.3.)

- *ST Microelectronics:* The current UHF RFID chip IC of ST Microelectronics is XRAG2. It has TID memory bank which can be programmed to store either the serialized 64-bit ISO TID number or the non-serialized 32-bit EPC TID number (cf. Fig. 1 and Fig. 2). To allow writing the TID numbers in both ISO and EPC formats, none of the TID memory is implemented as hard-wired ROM but it can be programmed by the chip manufacturer. The TID numbers are programmed and protected from rewriting while the chips are on the wafer. XRAG2 is manufactured using a 180 nanometer process.

This review suggests that all Gen-2 chips of the reviewed major chip manufacturers have permanently locked TID numbers. Moreover, the author is also not aware of other companies selling unprogrammed Gen-2 chips and thus, to the best of the author's knowledge, it is not possible to buy chips with unprogrammed TID numbers today. However, this review does not guarantee that such chips could not be bought today and even less so in the future.

Table VI-1: *Summary of reviewed Gen-2 chips' characteristics*

Chip	Company	Chip Model ID	Serial TID	TID Lock
Higgs-2	Alien	ROM	Optional	Yes
Higgs-3	Alien	ROM	Standard	Yes
Monza	Impinj	ROM	No	Yes
Monza/ID	Impinj	ROM	Standard	Yes
Monza/64	Impinj	ROM	No	Yes
UCODE G2XM	NXP	EEPROM	Standard	Yes
UCODE G2XL	NXP	EEPROM	Standard	Yes
SL3 ICS1001	NXP	EEPROM	Standard	Yes
SL3 ICS3101	NXP	EEPROM	Standard	Yes
SL3 ICS3001	NXP	EEPROM	Standard	Yes
UHF Gen2 STRAP	TI	ROM	No	Yes
XRAG2	ST M.	EEPROM	Optional	Yes
QR2233	Quanray	EEPROM	Standard	Yes

VI.1.4 Summary and Guidelines

End-users of Gen-2 tags need to understand that a serialized TID number is not a real security feature. The fact that serialized TID numbers provide protection against chip cloning today is mostly based on the fact that programmable Gen-2 chips are not currently available, but there are no guarantees that this will be the case in the long term. The looming threat is that end-users will put too much confidence on TID-based checks, which would create a major potential for an RFID security breach. Owing to the high level of automation that RFID provides, compromising the authenticity checks could lead to a wide scale exploitation—and an urgent market need for stronger security features. However, serialized TID numbers can be used as a partial and temporary solution when certain guidelines are respected.

The review of current TID standards and Gen-2 chip manufacturers revealed that in practice the serialized TID numbers of UHF chips (ISO or EPC) are currently written in different memory banks and the numbers have varying lengths. This complicates applications that need to support different types of UHF chips since the reader does not know which kind of TID number is written on the chip, how long the TID number is, and where it is written in the chip's memory. As a result, an application that must read serialized TID numbers of different types of chips might need up to three read cycles to do it, and steps 4-5 in the protocol, Fig. VI-4, are replaced by i) identification of the AC identifier, ii) identification of the Tag MDID / the Tag manufacturer ID, and iii) identification of the tag serial number / serialized model number. This increases the read time. The upcoming EPC Tag Data Standard will ease the situation by specifying the serial number format, but it will take probably years until most tags on the market will conform to a unified serialized TID number format.

Guidelines for the Use of TID Numbers in Anti-Counterfeiting

- Verify that the chips have serialized TID numbers. Serialized TID numbers are not demanded by the existing EPC standards and all UHF chips do not have them.

- If the application needs to support for different UHF chips of multiple manufacturers, reserve more time for reading the serialized TID numbers. Since the serialized TID numbers of UHF chips (ISO or EPC) are currently written in different memory banks and have varying lengths, they must be read in multiple read cycles if the precise chip type is not known beforehand.

- Do not create an illusion of perfect security, TID checks can be fooled. The serial parts of TID numbers are never written on hard-wired ROM but on EEPROM that by definition is rewritable, though the rewriting functionality is disabled. From a technical point of view, however, TID numbers seems to offer greater protection against copying than MAC addresses.

- Avoid using TID checks when the tags cannot be physically inspected. An important part of security is based on the fact that the TID number is written on an untampered standard chip and not on an impersonating device.

- Do not rely only on serialized TID numbers. This could create a lucrative opportunity for RFID crackers to produce tag impersonation devices or fully programmable chips. If the TID check is used among other security features to provide an additional level of protection, it can deter counterfeiters. In addition, by checking also other features you will learn when TID check will be compromised.

- Do not rely on TID in high value items. The higher the financial motivation for breaking the feature, the faster it will be done. In general, if TID checks are only moderately used in security applications, the lifetime of TID as a security feature will be prolonged.

- Have a serious migration plan to more secure measures (cf. subsection VII.2) and be ready to adopt them once TID checks are compromised. Since authenticity checks are automated, security breaches can cause a great deal of harm before organizations can react.

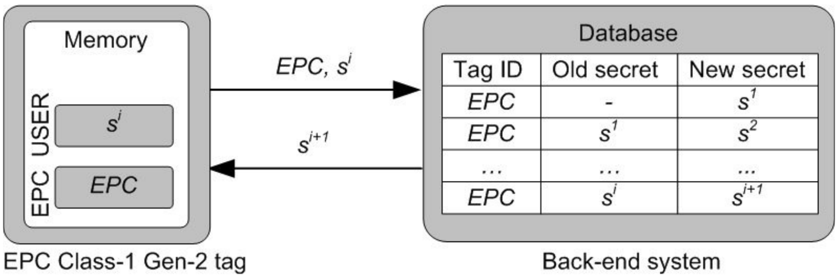
VI.2 Detection of Tag Cloning Based on Synchronized Secrets

This subsection presents and evaluates an approach to detect tag cloning attacks based on *synchronized secrets*. Instead of relying on the strength of the weakest and cheapest devices within the system, the tags, this approach relies on the visibility the tags provide. The underlying technical concept is simple and it has already been proposed for RFID ownership transfer and access control (Ilic et al., 2007; Grummt and Ackermann, 2008; Koscher et al., 2008), and applied for car immobilizers (Alrabady, 2002, p. 21), but it has not yet been considered for detection of cloned RFID tags. Therefore the major contribution of this work is not the idea development itself, but an innovative application and evaluation of an existing idea.

VI.2.1 Description of the Synchronized Secrets Method

The synchronized secrets method makes use of a tag's rewritable memory. In this method, in addition to the static identifiers (EPC and TID), the tag also stores a random number that is changed every time the tag is read. This number is denoted the *synchronized secret* since it is unknown to parties who cannot read the tag. A centralized back-end system issues these numbers and keeps track of which number is written on which tag.

Every time the tag is read, its identifier and synchronized secret are sent to the centralized back-end system. The back-end verifies if the synchronized secret written on the tag matches the one stored on the database for that particular tag. If these numbers match, the tag passes the check—otherwise an alarm is triggered. After the check, the back-end generates a new synchronized secret that the reader device writes on the tag. This is illustrated in Fig. VI-8.



Tag ID	Old secret	New secret
EPC	-	s^1
EPC	s^1	s^2
...	...	...
EPC	s^i	s^{i+1}

Figure VI-8: *Illustration of the synchronized secrets method*

The synchronized secret can be understood as a counter. If a tag's static identifier and counter value are copied to another tag and one of these two tags is scanned by an authorized reader, the tags will no longer be identical because the scanned tag's counter is incremented. The back-end detects the tag with the outdated counter value as soon this tag is scanned. The difference between this illustrative counter scheme and the synchronized secrets method is that the synchronized secret is a random number, which makes it hard to guess for adversaries. As a result, the synchronized secret can also be understood as a one-time password.

If a tag has an outdated synchronized secret, either the tag is genuine but it has not been correctly updated (desynchronization), or someone has purposefully obtained and written an old secret to the genuine tag (sophisticated vandalism), or the genuine tag has been cloned and the cloned tag has been scanned. Since unintentional desynchronization problems can be addressed with acknowledgments in the protocol (cf. Fig. VI-10) and the described form of vandalism appears unrealistic in supply chain applications, an outdated synchronized secret is a strong evidence of a tag cloning attack. Last, if a tag has a valid static identifier but a synchronized secret that has never been issued by the back-end, the tag is likely to be forged.

An outdated synchronized secret alone does not yet prove that a tag is cloned; if the cloned tag is read before the genuine tag after cloning attack occurred, it is the genuine tag that has an outdated synchronized secret. Therefore an outdated synchronized secret is only a proof that tag cloning attack has occurred, but not a proof that a tag is cloned. As a result, the presented method pinpoints the objects with the same identifier but it still needs to be used together with a manual inspection to ascertain which of the objects is not genuine.

To protect the scheme against man-in-the-middle (MITM) attacks between a reader and the back-end and against malicious back-end servers and readers, the back-end and the readers need a secure mutual authentication method to prove their authenticity to each other. The synchronized secrets protocol itself is agnostic to how this is achieved, and a possible implementation can include a trusted reader platform (Soppera et al., 2007) and public key infrastructure.

In addition to knowing that a cloning attack has occurred, the back-end can pinpoint a time window and a location window where the cloning attack happened, given that also the time and location of all read events are included to the back-end database. With this information the method additionally makes it hard to *repudiate* tag cloning to parties who handle the tagged objects. This is a security service that preventive measures like cryptographic tags do not provide and it can support responsive measures, such as pinpointing illicit supply chain partners.

VI.2.2 Analytical Model of the Level of Security

The level of security of a detection-based security measure is characterized by its detection rate. To evaluate the level of security of the synchronized secrets method, an analytical model of the detection rate is constructed based on the time dynamics of read events.

Let us assume a system which consists of a population of tags that have a static identifier and some rewritable non-volatile memory (e.g. EEPROM) to store the synchronized secret. The tags are repeatedly scanned by readers that are connected to a back-end server. The probability that a tag will be scanned sometimes in the future at least once more is constant and denoted by Θ. When a tag is scanned its synchronized secret is updated both on the tag and the back-end as described above in subsection VI.2.1. The time between these updates for a tag is denoted by random variable T_{update}.

The most important threat is an adversary cloning a genuine tag and injecting the cloned tag

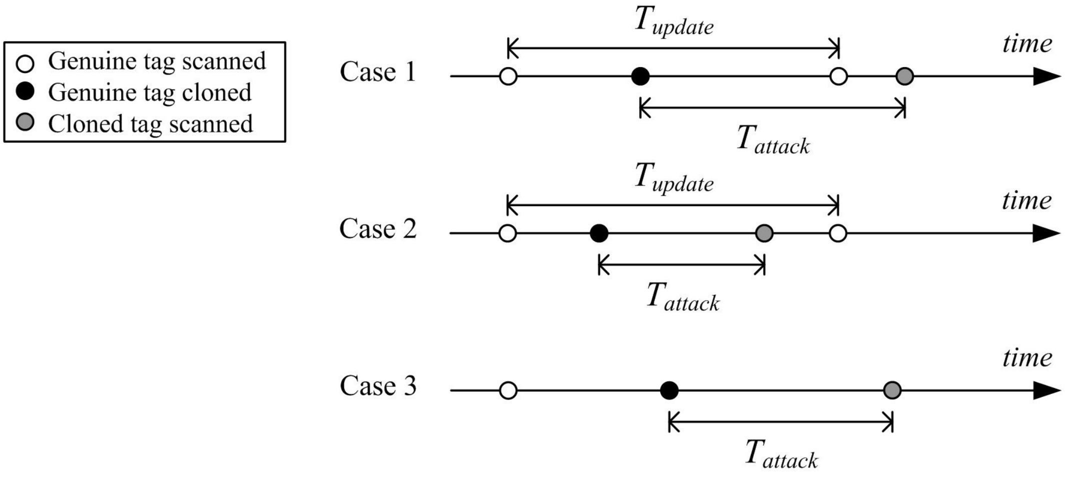


Figure VI-9: *Illustration of the possible outcomes of a cloning attack*

into the system. It is assumed that the adversary can clone any tag whenever he wants and the cloning attacks are independent of the times when the genuine tags are scanned by the authorized readers. The time delay from the cloning attack to the moment when the cloned tag is scanned is denoted by a random variable T_{attack}. Additionally, an adversary can try to guess the value of the synchronized secret.

The above described system's responses can now be statistically analyzed. First, the probability of successfully guessing a genuine tag's synchronized secret is $1/(2^N)$ where N denotes the length of the synchronized secret in bits. Even with short sizes, e.g. $N = 32$, guessing the synchronized secret is hard (ca. 2×10^{-9}) and the system can thus be considered secure against guessing attacks[9]. Second, when a cloning attack occurs, the following three mutually exclusive outcomes are possible (cf. Fig. VI-9):

- *Case 1:* The genuine tag is scanned before the cloned tag and an alarm is thus triggered when the copied tag is scanned.
- *Case 2:* The cloned tag is scanned before the genuine tag and an alarm is thus triggered when the genuine tag is scanned.
- *Case 3:* The genuine tag is not scanned anymore and thus no alarm is triggered for the cloned tag.

In Case 1, the cloning attack is detected as soon as the cloned tag is scanned the first time as it tries to enter the system and the cloned tag can thus be prevented from entering the system. In Case 2, the cloned tag passes a check and enters the system without raising an alarm but the system detects the cloning attack when the genuine tag is scanned. And last, in Case

[9] There is no brute-force attack to uncover the synchronized secret; the secret on the tag can be read without restriction, and the secret on back-end can be accessed only through the protocol (Fig. VI-10).

3 the security fails and the cloning attack goes unnoticed. The system's level of security is characterized by the probability of Case 1 that tells how often a threat is prevented and by the probability of Case 1 or Case 2 that tells how often a threat is detected (an alarm is triggered).

$$\text{Prevention rate} = \Pr(\text{Case } 1) \tag{VI-20}$$

$$\text{Detection rate} = \Pr(\text{Case } 1 \vee \text{Case } 2) \tag{VI-21}$$

The detection rate equals the probability that an alarm is triggered which equals the probability that a genuine tag is ever scanned again, Θ.

The prevention rate equals the probability that the genuine tag is scanned at least once more, Θ, multiplied by the probability that the genuine tag is scanned before the cloned tag. Let us assume that the time when the cloning attack occurs is independent of the times when the genuine tag is scanned and uniformly distributed over the time axis, so the average time before the genuine tag is scanned after a copying attack is $T_{update}/2$. We can now estimate the probability of Case 1 as follows:

$$\Pr(\text{Case } 1) = \Theta \cdot \Pr\left(\frac{T_{update}}{2} - T_{attack} < 0\right) \tag{VI-22}$$

Assuming that $T_{update} \sim N(\mu_{update}, \sigma^2_{update})$ and $T_{attack} \sim N(\mu_{attack}, \sigma^2_{attack})$, we can estimate the probability of Case 1 using a new random variable $Z = \frac{T_{update}}{2} - T_{attack}$ as follows[10]:

$$\Pr(\text{Case } 1) = \Theta \cdot \Pr(Z < 0) \tag{VI-23}$$

Distribution of Z can be calculated using these rules: if $X \sim N(\nu, \tau^2)$, then $aX \sim N(a\nu, (a\tau)^2)$, and if $Y \sim N(\kappa, \lambda^2)$, then $X + Y \sim N(\nu + \kappa, \tau^2 + \lambda^2)$.

$$Z \sim N\left(\frac{\mu_{update}}{2} - \mu_{attack}, \frac{\sigma^2_{update}}{4} + \sigma^2_{attack}\right) \tag{VI-24}$$

Equation VI-22 shows that the level of security of the synchronized secrets method depends on the frequency in which the genuine tags are scanned with respect to the time delay of the attack, and on the probability that the genuine tag is scanned once more. The same finding is confirmed from Equations VI-23 and VI-24 which show more clearly that, in the case of normally distributed time variables, $\lim_{\mu_{attack} - \mu_{update} \to \infty} \Pr(\text{Case } 1) = \Theta$. However, assuming that in the real world the variances of T_{update} and T_{attack} are somewhat high and the thus the distribution of Z has a long positive tail, there exist always some inherent uncertainty when deciding between Case 1 and Case 2.

[10] Since T_{update} and T_{attack} cannot be negative, these assumptions yield viable estimates only when the mean μ is positive and high compared to variance σ

After the last event of the genuine tag, a single cloned tag will always go unnoticed (Case 3). The analytical model assumes a ”statistically average adversary” who does not systematically exploit this vulnerability. However, a real-world adversary who knows the system is not likely to behave in this way. Therefore this vulnerability should be patched by flagging tags that are known to have left the system (e.g. products that are known to have been sold, dispensed, or shipped to a retailer). *This raises the implicit requirement of knowing when products leave the RFID system where they are traced (e.g. certain part of the supply chain).*

VI.2.3 Implementation

To demonstrate the feasibility of synchronized secrets method on low-cost RFID, this subsection presents our experimental implementation using UHF tags conforming to the EPC Class-1 Gen-2 standard (EPCglobal Inc., 2005a). The presented demonstrator is implemented by Daniel Ostojic and Alexander Ilic.

The implemented protocol between the back-end system, the reader, and the tag is presented in Fig. VI-10. In the illustration, s^i denotes the current synchronized secret, s^{i+1} the new synchronized secret, RND_{32} a 32-bit random number, $alarm$ a boolean value whether an alarm is triggered or not, and ack an acknowledgment of a successful update of the synchronized secret. Step 6 is dedicated to establishing a secure connection between the reader and the back-end to mitigate MITM attacks, malicious back-end systems, and to protect the integrity of the back-end.

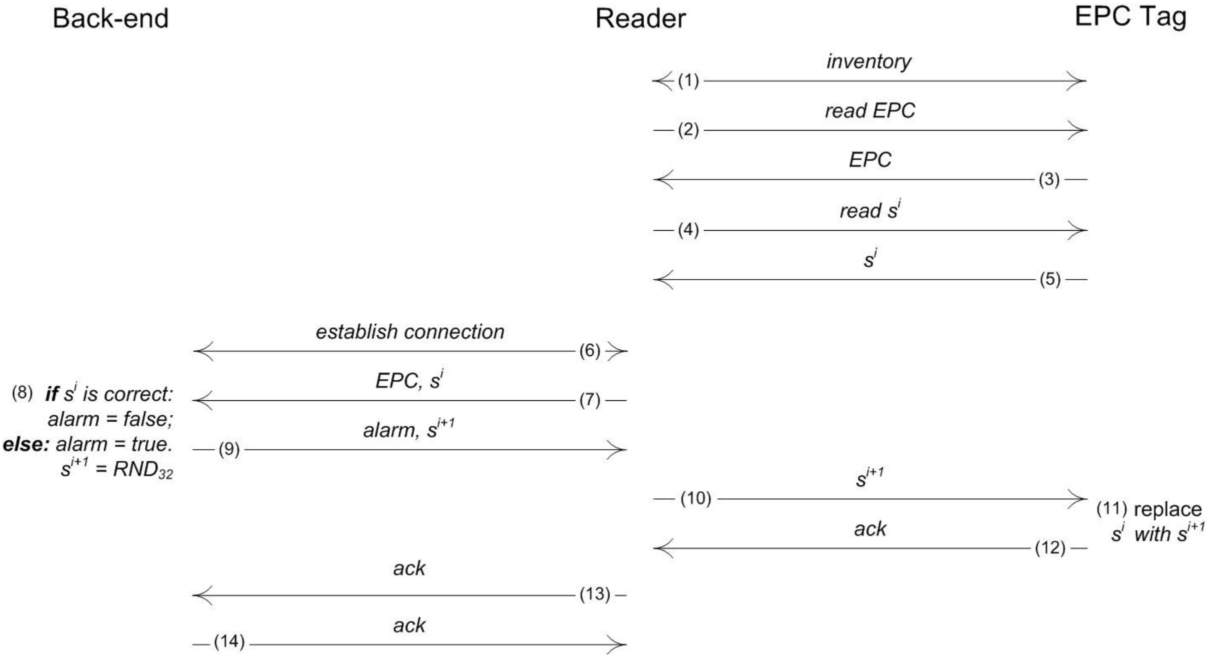


Figure VI-10: *Implemented synchronized secrets protocol*

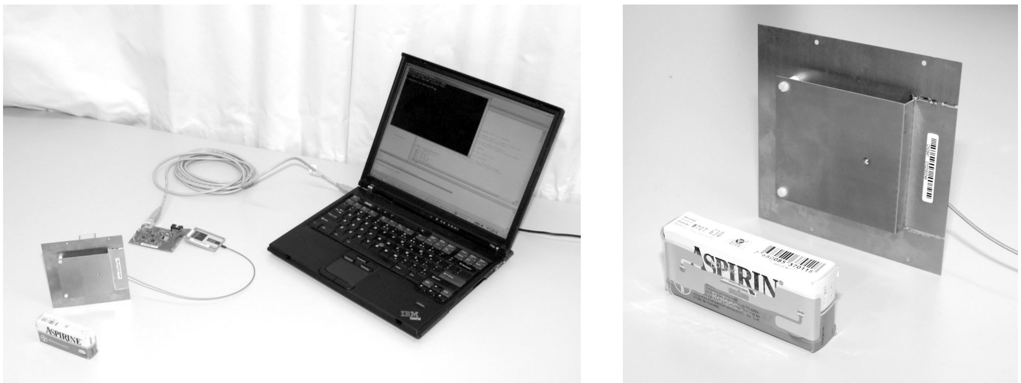


Figure VI-11: *Hardware set-up of the synchronized secrets implementation*

Set-Up

The presented method is implemented using Gen-2 tags from UPM Raflatac that use Monza 1A chips manufactured by Impinj. The reader device is A828EU UHF reader from CAEN and it is controlled by a laptop computer that runs the local client program. The back-end system is implemented as a web server that stores the EPC numbers, synchronized secrets, and time stamps in a MySQL database. The hardware set-up is shown in Fig. VI-11.

Given that an RFID infrastructure is in place and tags have a modest amount of user memory, the only direct cost of the presented method is the time delay of verifying and updating the synchronized secrets, i.e. steps 4-14 of the protocol (cf. Fig. VI-10). This overhead time is measured from 100 reads where the tagged product faces the antenna in 5 cm distance[11].

Performance

The measured average overall processing time of one tag is 864 ms. This includes 128 ms for the inventory command (step 1), 181 ms for reading the EPC number (steps 2-3), and the remaining 555 ms is the time overhead of the synchronized secrets protocol (steps 4-12). The measured average times and their standard deviations are presented in Fig. VI-12.

The results show that the time overhead of the protocol increases one tag's processing time approximately by a factor of 300%, after the inventory command. E*ven though the time overhead is short in absolute terms, it makes a difference in bulk reading where multiple products are scanned at once*. A closer look on the times of different steps reveals that writing a new synchronized secret on the tag is only a slightly slower than reading a secret from the tag, and that the biggest variance is experienced within the back-end access (steps 6-9).

Note that the measured performance depends on the implementation and has potential for improvement through optimization of reader and back-end software. In addition, variance in web

[11] Acknowledgment messages to the back-end, steps 13-14 of the protocol, are omitted from the measurements since they do not increase a tag's processing time

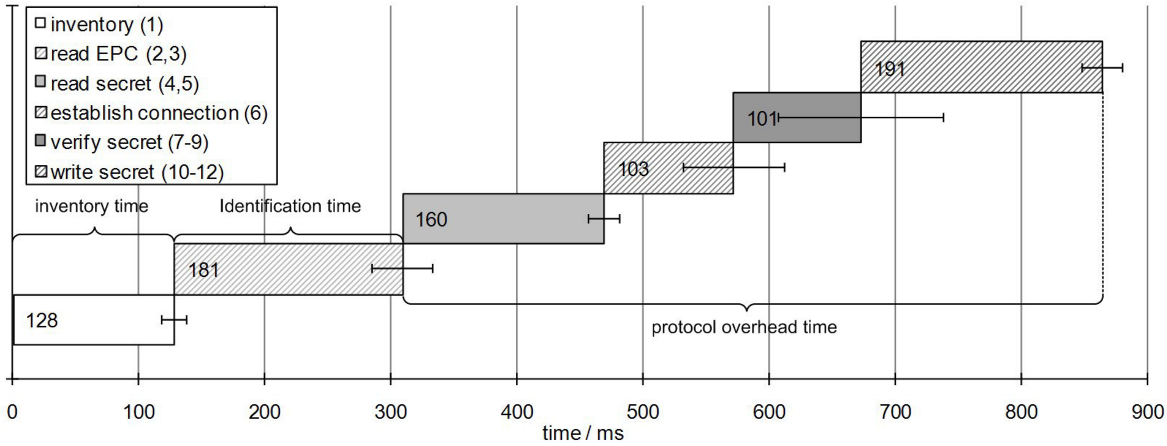


Figure VI-12: *Measured average times and standard deviations (error bars) of different steps (numbers in brackets) in the implemented protocol*

server latency makes the time overhead dependent on network traffic and thus somewhat hard to predict. Despite these limitations, this simple experiment provides evidence that the overhead time can limit the usability of the presented method in time-constrained bulk reading.

VI.2.4 Discussion of Pros and Cons

Uncertainty has a special appearance in the synchronized secrets method. In typical intrusion detection systems an alarm indicates that an intrusion *might* have happened, which is analogous to indicating that a scanned RFID tag *might* be cloned. An alarm in the synchronized secrets method indicates *without uncertainty*—given that desynchronization problems are addressed, e.g. with acknowledgments—that there are two tags with the same ID number, but the method cannot tell which of the two tags is the genuine one (formally: the method cannot distinguish between Case 1 and Case 2, Fig. VI-9). Though this might appear like a shortcoming of the synchronized secrets method, it actually contributes toward reliable detection of cloned tags. This advantage is illustrated with a numeric example below.

The synchronized secrets method does not require sharing of track and trace data, which is a benefit for companies that find this information too sensitive for disclosing. However, if there are large delays between the scans, the synchronized secrets method can trigger an alarm for the cloned tag only after a large delay. In some applications this delay cannot be allowed since it could mean, for example, that a counterfeit medicine has already been consumed. In track and trace based clone detection methods the alarm is triggered—if it is triggered—primarily right after the cloned tag is scanned, and thus similar delays are less likely to occur.

One physical back-end system is unlikely to be scalable enough to run the synchronized secrets protocol for the large numbers of objects that will be tagged. Fortunately, this kind of scalability is also not needed. The back-end can be distributed to virtually an unlimited number of servers by having, for example, one back-end server per product family, per product type, per geographical region, or per a subset of certain kinds of products. This can be implemented either with static lists that map EPC numbers to different back-end systems and that is known by readers, or with the help of EPC ONS or DS that both provide one logical central point for queries about information and services related to a product (EPCglobal Inc., 2009a). Moreover, the scalability requirements of the presented method are the same as in any RFID system where the back-end knows the current location/status of the items. Additional network requirements of the presented method include strong authentication between the reader devices and the back-end to secure the protocol against MITM attacks.

All EPC tags are potentially vulnerable to tampering of the tag data which can be used as a Denial of Service (DoS) attack against the presented method. This DoS vulnerability can be mitigated with the access passwords of EPC tags (EPCglobal Inc., 2005a) by having the reader retrieve the access password and unlock the tag after identification (cf. step 2 in Fig. VI-10), and lock the tag again after updating the synchronized secret. Moreover, write and read protection of the user memory where the synchronized secret is stored can be used to as a complementing security measure to prevent tag cloning and tampering. This method would make clandestine scanning of the synchronized secret unfeasible without cracking the 32-bit access password, though the protocol would still remain unsecure against eavesdropping.

In addition, the use of synchronized secrets opens a door for a new DoS attack that makes a genuine tag cause an alarm even when there are no cloned tags in the system; an adversary that is located near to an authorized reader can eavesdrop the static ID number and the synchronized secret of a genuine tag and impersonate this tag to an authorized reader before the genuine tag is scanned. As a result, the genuine tag will raise an alarm next time it is scanned. This results into an unnecessary manual inspection of the genuine tag (which will reveal the time and location of the impersonation attack). This DoS attack is possible only when adversaries have access to an authorized reader device, which is typically not the case in supply chain applications such as anti-counterfeiting. Furthermore, the time (and potentially the location) of this DoS attack is registered, while there are also simpler attacks that achieve the same outcome without leaving any such trace, namely physical or electromagnetic destruction of the tags.

Example: Level of Security in an Access Control Application

Level of security of the presented method depends on how often the tags are scanned and on how much time the adversary needs to conduct the cloning and impersonation attack (Equation VI-22). Owing to the lack of a public data set and published results for the detection of cloned RFID tags in supply chains, the level of security of the synchronized secrets method is exemplified with a public RFID access control data set (Mirowski et al., 2008). This data set is an activity record of proximity cards within an access control system that controls the access to parts of a building.

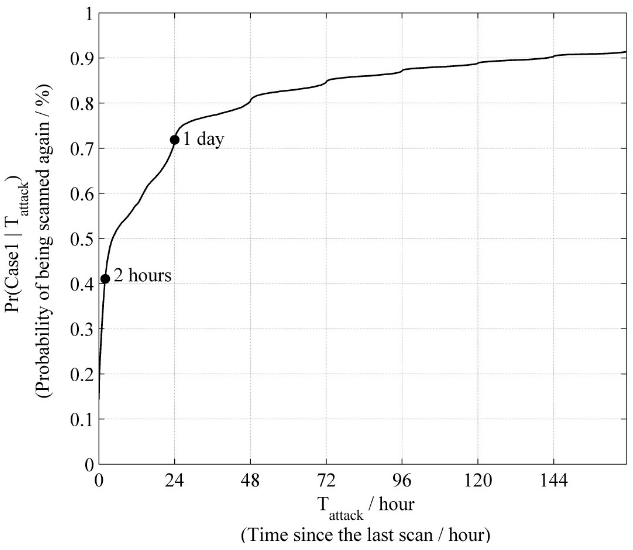


Figure VI-13: *Time delay between consecutive reads in the data set of Mirowski et al. (2008)*

The probability that a tag is scanned again within this data set is presented as a function of the time delay from the previous scan in Fig. VI-13. This equals the probability that a cloned tag raises an alarm when it is scanned for the first time (Case 1), given an attack delay. Assuming that an adversary needs 2 or 24 hours to conduct an impersonation attack after cloning an RFID access card, he faces a 41% or a 72% chance of raising an alarm when the cloned access card is read for the first time, respectively. This corresponds to $P_{reliability} = 41...72\%$. The overall probability of a tag being scanned again, Θ, is 99.15% within the same data set. This corresponds to the detection rate (Equation VI-21), or the probability of Case 1 or Case 2.

Though these results are calculated from average statistics, the findings suggest that only very few cloning attacks would potentially go completely unnoticed in the studied application, and that an adversary needs to conduct the impersonation attack within a few hours after tag cloning to have a relative good chance of not raising an alarm.

The performance and thus the level of security of the synchronized secrets method can be compared to that of Deckard, a system designed to detect cloned tags in the presented access control application based on statistical anomalies (Mirowski and Hartnett, 2007). The published detection rates for Deckard are based on the same data set (Mirowski et al., 2008) than the aforementioned results for the synchronized secrets method, but the results are still not completely comparable since the synchronized secrets method needs an assumption of the attack delay which is not aligned with the simulated attack scenario used in (Mirowski and Hartnett, 2007). Nevertheless, the comparison is accurate enough to give a good indication and a benchmark of the performance of these two methods.

From a simulated attack scenario within the aforementioned data set, Deckard is able to detect 46.3% of cloned tags with a 2.5% false alarm rate, or 63.0% of cloned tags with a 3.7% false alarm rate. This corresponds to $P_{reliability} = 46.3...63.0\%$. The performance of these two

Table VI-2: *Quantitative evaluation of synchronized secrets method access control application*

Method	**Parameters**	**Cloned tags prevented**	**Cloned tags detected**	**Manual verifications**
Deckard (Mirowski and Hartnett, 2007)	*Hit rate* 46.3%, *False-alarm rate* 2.5%	5	5	256
Deckard (Mirowski and Hartnett, 2007)	*Hit rate* 63.0%, *False-alarm rate* 3.7%	6	6	75
Synchronized secrets (2h attack delay)	*Prevention rate* 41%, *Detection rate* 99.15%	4	10	10
Synchronized secrets (24h attack delay)	*Prevention rate* 72%, *Detection rate* 99.15%	7	10	10

methods can be illustrated by assuming that 10,000 tags are scanned containing 10 cloned tags, and that each alarm leads to a manual verification. Now the number of *cloned tags prevented* (the number of cloned tags raising an alarm the first time they are scanned), *cloned tags detected* (the number of cloned tags raising an alarm overall), and the number of *manual verifications* can be calculated for both these methods. The results are summarized in Table VI-2.

The results show that both methods achieve similar number of cloned tags prevented under the taken assumptions about the attack delay, namely 5-6 and 4-7. However, the synchronized secrets method has a clear advantage regarding the overall number of cloned tags detected, and most importantly regarding the number of needed manual verifications that is only 10, compared to the 75 or 256 for Decard. As a conclusion, the facts that 99.15% of cloned tags eventually cause an alarm and that only as many manual verifications are needed than the number of cloned tags scanned are a clear advantage of the synchronized secrets method.

VI.2.5 Summary and Guidelines

The synchronized secrets method detects cloning attacks and pinpoint the different tags with the same ID, using only a small amount of rewritable tag memory. This provides a considerable increase to the level of security for systems that use unprotected low-cost tags. A major benefit of the synchronized secrets measure is that it can be used with today's low-cost RFID tags such as EPC Gen-2, and applied in all RFID applications where tags are repeatedly scanned.

As other detection-based security measures, the synchronized secrets method needs to be complemented by manual verifications to ascertain which of the tags with the same ID number is the cloned one. However, a numeric example illustrates that the the number of needed verifications for the synchronized secrets method is considerably smaller than for Decard, the first published system for the detection of cloned RFID tags. Overall, the presented method has the potential to make harmful injection of cloned tags into RFID-enabled supply chains considerably harder using only a minimal hardware overhead.

Guidelines for the Use of Synchronized Secrets in Anti-Counterfeiting

- Verify that the used tags have a small amount of free rewritable memory to store the synchronized secret, for example 32 bits or more of user memory.

- An alarm denotes that a cloning attack has occurred and it pinpoints the tags with the same EPC, but it cannot tell which of the tags with the same EPC is the cloned one. Therefore also another means of verifying the authenticity of products is needed after an alarm (manual verification), but this other method can be somewhat costly and time-demanding since the synchronized secrets method triggers only so many alarms than the number of cloned tags scanned.

- Tagged products that are known to have left the channel where they are traced should be flagged in the database to prevent ”trace hijacking”. If it cannot be known when the tagged products eventually leave the traced channel, then a cloning attack that occurs after the last event of the genuine tag will go undetected.

- If there is a long delay before the products are scanned in the supply chains, for instance while the products are stored, and the tags are vulnerable to cloning by illicit actors during this delay, then there is a risk that an alarm for a cloned tag is triggered after a long delay. If in such a case a long delay would introduce a big security, safety, or health-related risk for the consumer or end-user, the tags should be scanned more often, or another product authentication mechanism should be used.

VI.3 Detection of Cloned Tags from RFID Traces

Related work suggests that in certain cases cloned RFID tags can be detected by analyzing the RFID trace data. For instance, if the genuine product is known to be in location A, a product with the same identifier in location B is likely to be an impostor.

An important problem behind RFID-enabled location-based authentication is that RFID traces always represent historic events without giving certainty where the traced objects currently really are. In addition, existing RFID systems are still somewhat prone to read errors (cf. subsection II.3.4) and as a result, the visibility that RFID systems provide is not perfect. This makes location-based authentication harder and less reliable.

This subsection investigates a new method to detect cloned tags from incomplete RFID traces based on probabilistic techniques. The goal of the proposed techniques is reliable and automatic detection of cloned tags from a large amount of trace data. The proposed technique is based on the hypothesis that cloned tags create abnormal events that can be detected in the trace.

This subsection first describes common characteristics of RFID traces that affect location-based authentication and then present a probabilistic location-based authentication method. Performance of the method is evaluated in a simulation study based on a real-world pharmaceutical supply chain. The lessons learned are presented as guidelines in the end.

VI.3.1 Characteristics of RFID traces

RFID traces do not provide perfect visibility of the tagged objects. A metaphor for perfect visibility would be a high-precision GPS device attached to every physical object, continuously transmitting the location data. RFID does not provide this kind of perfect visibility but discrete geo-temporal snapshots of physical objects' locations without giving full certainty where the tagged objects really are at a given time. Moreover, some snapshots can be lost due to missing reads (cf. subsection II.3.4). As a result, the visibility that high-level RFID data provides is blurred by *location uncertainty*.

Location uncertainty can be formally expressed as follows. At any given point of time, location uncertainty of trace data stands for the set of different locations where the tagged object can be. If the product's location is known without uncertainty, it can be only in one location and the location uncertainty is zero. If the product can be anywhere, location uncertainty reaches its maximum value, for example one.

Location uncertainty evolves in time according to two principles. First, when a product is shipped from a supply chain location and it generates a corresponding shipping event, the set of locations where it can be increases as time goes by and thus its location uncertainty increases from zero. Second, when a product is received to a new supply chain location and it generates a corresponding receiving event, the product is typically supposed to remain there until the next shipping event occurs for that particular product. If missing reads can occur, however, there is

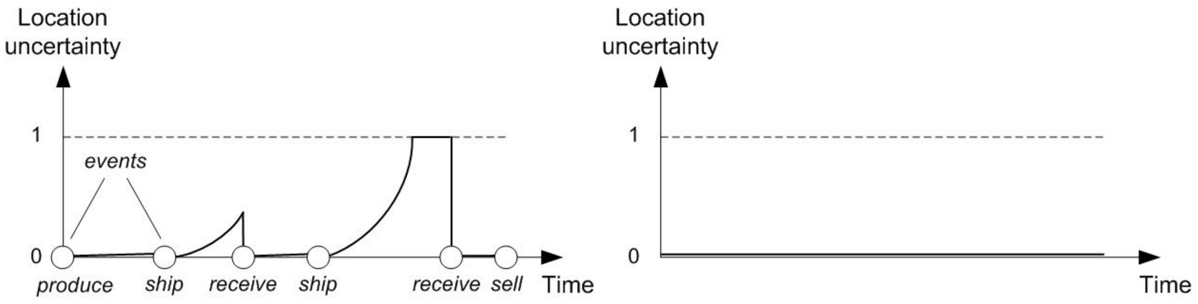


Figure VI-14: *Location uncertainty in RFID (left) and GPS (right) traces*

a small probability that the product leaves the warehouse without generating a shipping event as time goes by, and the location uncertainty increases. These principles are illustrated and compared to the visibility provided by a GPS system in Fig. VI-14.

An RFID trace is a set of discrete events relating to the tagged object. In general, the semantic attributes of events follow a ”*What? When? Where? Why?*” -concept. Table VI-3 (upper part) presents the attributes of event data defined by the EPCIS 1.0.1 specification (EPCglobal Inc., 2007). These events are based on the event type ObjectEvent which indicates an ”event pertaining to one or more physical objects identified by EPCs”, i.e. an actual RFID read. The table shows that there is some redundancy between the *”where”*, *”what”*, and *”why”* attributes that enables simple queries and high granularity data mining.

One practical problem in location-based product authentication is that the term location can be ambiguous in the industry jargon. For example, when a reader is placed in the door between the storage room and the shop floor, the location of the read events might not be clear for business people who perceive that the reader is between two well-defined business locations. This problem has been addressed in EPCIS specification (EPCglobal Inc., 2007) by defining physical and logical reader attributes, a read point attribute, and a business location attribute to describe where the tagged objects are during and after the events are generated (cf. Table VI-3(upper part)). In particular, the *LogicalReader* identifier has been introduced to allow a physical reader to be replaced without making changes in the resulting event, and to allow a single physical reader cover several logical locations by using multiple antennas.

Regarding an anti-counterfeiting application, the most useful information of RFID events is captured by their time and location location attributes. Event time is simply the time when the event was captured. Among the various location attributes defined by the EPCIS 1.0.1 specification (EPCglobal Inc., 2007), business location (*bizLocation*) is the most suitable for location-based authentication since it defines the discrete and unambiguous location where the object is after the event. Furthermore, owing to the redundancy between the attributes, *bizLocation* attribute can also capture the *bizStep* and *action* attributes of an event.

Table VI-3: *EPCIS 1.0.1 (EPCglobal Inc., 2007) track and trace data model (upper part) and our probabilistic data attributes (lower part)*

Attribute	Description	Example
epc	Identifier of the RFID-tagged physical object	urn:epc:id:sgtin:0652642.800031.400
action	How the event relates to the object lifecycle	ADD, OBSERVE, DELETE
BizTransaction	Transaction that the event relates to	0000000260
eventTime	Time when the event was created	2008-02-08T12:00:00.000
eventTimeZoneOffset	Time zone offset	+06:00
PhysicalReader	Physical RFID reader that generated the event	mfg#876
LogicalReader	Event source independent of the physical reader	J
ReadPoint	How or where the event took place	RP-DC#88-A
bizLocation	Where the object is after the event	RP-DC#88-Shipping, urn:epc:id:sgln:0652642.12345.400
bizStep	Business step in which the event took part	receiving, shipping
Disposition	Business condition of the object after the event	available for sale, in storage
auth	Pr(event is generated by a genuine product)	0.98
authMethod	Identifies the method used to estimate *prob*	$SSCM_L, SSCM_T$

VI.3.2 Location-Based Authentication

Tracking and tracing enables location-based authentication (Lehtonen et al., 2007). The underlying assumptions are that all genuine products have a unique ID number and there exists a way to find out whether a unique ID number is valid or not. This scheme is not yet secure because an adversary could clone a tag. The location-based authentication system secures this scheme by detecting the cloned tags based on their locations.

Detection of cloned products from the track and trace data is straightforward if the location uncertainty is zero; for instance, if the track and trace data tells that the product is currently in Switzerland at the same time when a product with the same ID is scanned in Japan, the system can conclude that it is probable that the product in Japan has a cloned tag. However, when the track and trace data says that the product was observed in Switzerland one week ago but it does not tell its current location, authentication becomes harder and false alarms become possible.

A location-based authentication system is built by evaluating *transition probabilities* between the events. A transition probability stands for the probability that a genuine product makes the transition defined by two events. If the transition probability is high, the latter event is likely to be generated by a genuine tag and vice versa. When event i is denoted as E^i, the transition probability P_{tr} from E^i to a consecutive event E^{i+1} can be expressed as $P(E^{i+1}|E^i, E^{i-1}, ..., E^1)$ (cf. Fig. VI-15). The authentication rule can now be formalized as follows. *Event E^i is generated by a genuine product if*:

$$P_{tr} = P(E^{i+1}|E^i, E^{i-1}, ..., E^1) > \epsilon \tag{VI-25}$$

The location-based authentication problem can now be solved by a probabilistic method, namely a *classifier*, that yields high transition probabilities for events generated by genuine tags and low transition probabilities for events generated by cloned tags. Subsection VI.3.3 below presents two proposals for such a classifier.

The transition probability of the first event ($i = 1$) in a product's trace can be estimated by introducing a so called ”zero-event”. Like this, the transition probability of the first event is given by $P(E^1|E^0)$. By limiting the set of locations where this probability is non-zero, the system defines a limited secure environment where new products are allowed to occur. For instance, if the first event of all genuine products appear in the manufacturer's packaging line, the transition probability from the ”zero-event” to the packaging line can be set to one and the transition probability from the ”zero-event” to all other locations to zero.

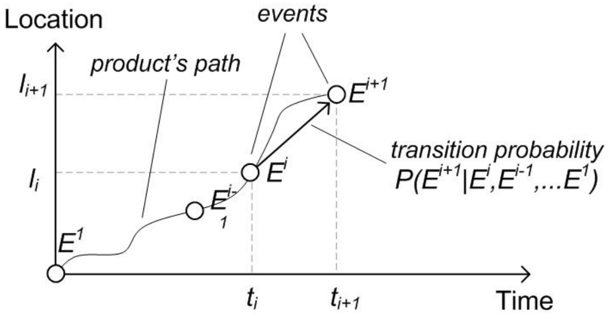


Figure VI-15: *Events and transition probabilities*

Using the Bayes' rule, the transition probability can be further turned into an *a posteriori* probability that an event is generated by a genuine tag. We denote the transition probability generated by an event by the random variable X. The probability that an event is generated by a genuine product, $P(ge)$, given that the transition probability the event generated is smaller than x, can be formulated as follows:

$$P(ge|X < x) = \frac{P(ge, X < x)}{P(X < x)} \tag{VI-26}$$

$$= \frac{P(ge) \cdot P(X < x|ge)}{P(X < x)} \tag{VI-27}$$

All terms in the last expression can be estimated from testing data (e.g. a simulation study) that contains known counterfeit products. Moreover, $P(ge|X < x)$ stands for the probability that the corresponding event has not been generated by a cloned tag, or in other words that the product is authentic. By appending RFID events with an attribute *auth* that stands for the value of this probability, and with *authMethod* that stands for the method how this probability is estimated (cf. Table VI-3 (lower part)), normal track and trace data can be extended to probabilistic track and trace data that also contains information about the authenticity of the underlying products. This is illustrated in Table VI-4.

Table VI-4: *Example of probabilistic RFID track and trace data*

#	epc	action	eventTime	bizLocation	bizStep	auth	authMethod
1	18264.697441.1	ADD	2008-02-10T16:00	RP-MFG#05-Production	internal	0.999	$SSCM_L$
2	18264.697441.1	OBSERVE	2008-02-14T10:00	RP-MFG#05-Shipping	shipping	0.996	$SSCM_L$
3	18264.697441.1	OBSERVE	2008-02-14T22:00	RP-DC#88-Receiving	receiving	0.976	$SSCM_L$
4	18264.697441.1	OBSERVE	2008-02-25T10:00	RP-DC#66-Receiving	receiving	0.008	$SSCM_L$
5	18264.697441.1	OBSERVE	2008-02-26T15:00	RP-DC#88-Shipping	shipping	0.997	$SSCM_L$

VI.3.3 Probabilistic Solution Method

A probabilistic solution method for the previously derived probabilistic authentication approach is detailed below. The data processing steps of the solution are following:

1. Train the supply chain model with training data,
2. Filter the testing data set to find missing reads,
3. Evaluate P_{tr} for all events in the filtered data, and
4. Raise an alarm if P_{tr} is below a threshold.

The generic transition probability, Equation VI-25, is formulated into a more useful form. As discussed above, event time (t) and the discrete business location (l) are enough to give a semantically rich presentation of RFID events. First, first order Markov assumption is taken which corresponds here that the state of the system is fully described by the last event, or:

$$P(E^{i+1}|E^i, E^{i-1}, ..., E^1) = P(E^{i+1}|E^i) \tag{VI-28}$$

This assumption discards path dependency of business locations. By assuming that time and location of new events are mutually independent random variables, and that locations of new events do not depend on time of the preceding events, the transition probability can be expressed as follows:

$$\begin{aligned} P(E^{i+1}|E^i) &= P(l_{i+1}, t_{i+1}|l_i, t_i) \\ &= P(l_{i+1}|l_i, t_i) \cdot P(t_{i+1}|l_i, t_i) \\ &= P(l_{i+1}|l_i) \cdot P(t_{i+1}|l_i, t_i) \\ &= P_{i,i+1} \cdot P(\Delta T_i = t_{i+1} - t_i) \end{aligned} \tag{VI-29}$$

To evaluate the two terms in the last expression, the process how track and trace events are generated in a supply chain is statistically modeled in the following subsection.

Stochastic Supply Chain Model

The Stochastic Supply Chain Model (SSCM) represents a supply chain with $N+1$ distinct states or nodes, $S_0, S_1, S_2, ..., S_N$, and lines that represent transitions between the states. Displaying supply chains as nodes and lines greatly reduced the complexity of RFID data (Cheung et al., 2006). The relation between states in the SSCM and the observed events is following: every time a product enters a state in the model, it generates a track and trace event in the real life. In other words, a state in the model corresponds to a reader device.

The zero-state, S_0, represents the "state of non-existence" where all tagged products are before they are created in the real world, and exceptionally it does not have corresponding events or business location in the real life. All other states in the model correspond to discrete business locations of the real-world supply chain network where tagged products are read. Parameters of the model define how products move from one discrete business location to another.

In the common case, after entering a state, the product stays there during a finite number of steps. This corresponds to a normal observation event. The time before the product generates a new event, called the waiting time, is given by a probability density function (PDF) that is specific to each state. For state i, $1 \leq i \leq N$, this PDF is denoted as $p(\Delta T_i)$. The actual distribution is not constrained by the model and it can be e.g. uniform or Gaussian. After time ΔT from entering a state, the product enters a new state according to the state transition probabilities. The first event in a product's trace is generated when the product leaves the zero-state S_0. After that, the product continues to move in the model through normal states as described above until it reaches an end-state. There are no routes that leave an end-state and thus the waiting time in an end-state can be regarded as infinite.

The state transition probabilities are time independent and denoted as $P_{ij} = P(S_i|S_j) \geq 0$, $i, j \geq 0$. State transition probabilities from a state to itself (P_{ii}) are possible and they correspond the real-life situation where a product's trace has two consecutive reads from the same single business location.

Each company in the supply chain is represented in the SSCM by a maximum of three states corresponding to receiving, internal, and shipping operations. The SSCM is trained from RFID traces and only business locations where products are scanned are present in the SSCM. The resulting model is flexible and intuitive and it has enough degrees of freedom to capture the essential statistics of how single products flow in supply chains. The SSCM is exemplified in Fig. VI-16. This imaginary supply chain illustrates different real-world problems in location-based product authentication: missing reads at reader in business location S_3 (results into a "ghost route" P_{24}, cf. subsection VI.3.3), a wholesaler and a retailer that do not share trace data beyond receiving notifications (S_6 and S_{10}, respectively), and reverse logistics (P_{84}).

Note that if the model would use state transition probabilities from a state to itself to define the time a product stays in a state instead of the waiting time PDFs, the model would be a time-independent first-order discrete time Markov chain (DTMC). However, we have opted for

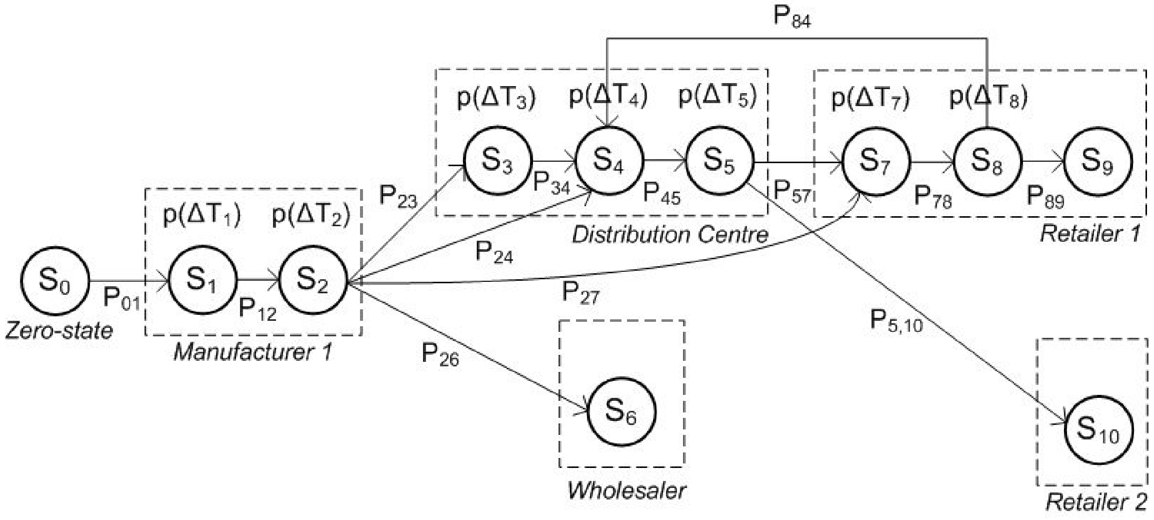


Figure VI-16: *Illustration of the Stochastic Supply Chain Model (SSCM)*

defining the waiting time distribution because it allows for more flexible modeling of the supply chain's time dynamics.

Filtering Traces to Detect Missing Reads

The SSCM can be used to detect missing reads in RFID traces. Missing reads can trigger unwanted false alarms in the clone detection system. Reader devices that have a below 100% read rate create so called ”ghost routes” that are observed as small transition probabilities that do not correspond to real-world transitions (cf. Fig. VI-17). The filtering algorithm tries to detect when a product is moving along such a ”ghost route” as evidence of a missing read event.

Referring to the example in Fig. VI-17, when a transition probability is low (from A to C), the filtering algorithm can search for a more probable alternative route that is obtained by including a new read event between the existing events. If the probability of the new route (from A to B to C) is higher than a threshold, the new event (in B) is added to the trace.

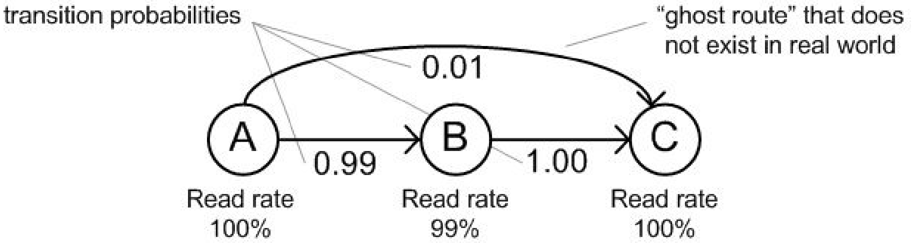


Figure VI-17: *Though all products flow from A to B to C, read errors in B creates a ”ghost route” A to C that the filtering algorithm tries to detect*

The number of missing consecutive read events that the filter can add is called the order of the filter. Filters of all orders can be described by three parameters: i) maximum transition probability (threshold) between the existing events, ii) minimum time difference (threshold) between the existing events, and iii) minimum geometric mean (threshold) of transition probabilities of the new route. The first two parameters define when the filter is allowed to add missing reads between existing events and the third parameter limits the addition of new routes that are too unlikely. The values of these parameters can be defined empirically.

Location-Based Authentication

For E^i, $i > 1$, SSCM enables evaluation of a location transition probability ($P_{i-1,i}$) and a time transition probability ($P(\Delta T_{i-1} = t_i - t_{i-1})$). These two methods are denoted as $SSCM_L$ and $SSCM_T$, respectively, and their performance is compared in a simulation study below. For the first event in a trace, E^1, only the location transition probability is defined. Now the authentication rule from Equation VI-25 can be rewritten in two new ways. *Event E^i is generated by a genuine product if*:

$$SSCM_L\text{: } P_{i-1,i} > \epsilon \tag{VI-30}$$

$$SSCM_T\text{: } P(\Delta T_{i-1} = t_i - t_{i-1}) > \epsilon \tag{VI-31}$$

The value of the threshold ϵ defines the trade-off between the ratio of event of cloned tags that are detected (hit rate) and the ratio of events of genuine products classified as generated by cloned tags (false alarm rate). The value of ϵ can be optimized only by setting a cost for false alarms and a value for hits. In practice, minimization of false alarms might be wanted and hence ϵ can be set to the smallest transition probability of genuine products within the training data. In general, the threshold ϵ has different values in Equations VI-30 and VI-31.

Intuition suggests that an optimal location-based authentication system should combine the location and time transition probabilities presented in Equations VI-30 and VI-31. Finding a way to combine these probabilities is, however, not addressed by this thesis.

VI.3.4 Simulation Study

The proposed methods are evaluated with a simulation study of a real-world pharmaceutical supply chain. The goal of this study is to evaluate how cloned tags – that is, counterfeit products – that are in the supply chain in the same time than the corresponding genuine tags can be distinguished from the genuine tags in the presence of missing reads and limited amount of training data. Detection of cloned tags that appear before the corresponding genuine products are manufactured or after the corresponding genuine products are consumed are not considered because they can be detected with simple static rules.

This study measures how often events created by cloned tags are detected (*hit rate*) versus how often alarms are triggered to genuine products' events (*false alarm rate*). The resulting trade-off is presented as a Receiver Operating Characteristics (*ROC*) curve that characterizes the selectivity of a classifier. In a real-world anti-counterfeiting application, only very small false alarm rates can be tolerated because the number of read events that the genuine products generate is very high.

Only the first events generated by the cloned tags are considered in the results. The reason for this restriction is that the simulated supply chain handles both counterfeit and genuine products in an identical way, so the following events generated by cloned tags have identical statistics than events generated by genuine products. As a result, the results indicate how reliably the cloned tags can be detected as soon as they enter the supply chain and the hit rate directly corresponds to achieved counterfeit product detection rate P_{det}.[12] In addition, events that are generated by genuine products and directly preceded by events from cloned tags are neglected from the results.

In the absence of comprehensive datasets of real-world track and trace data, simulations are the best available method to evaluate the proposed techniques. Moreover, even when such a dataset was available, some real world scenarios would still need to be simulated within that data set, such as counterfeit products with cloned tags entering the supply chain and the effect of imperfect read rates.

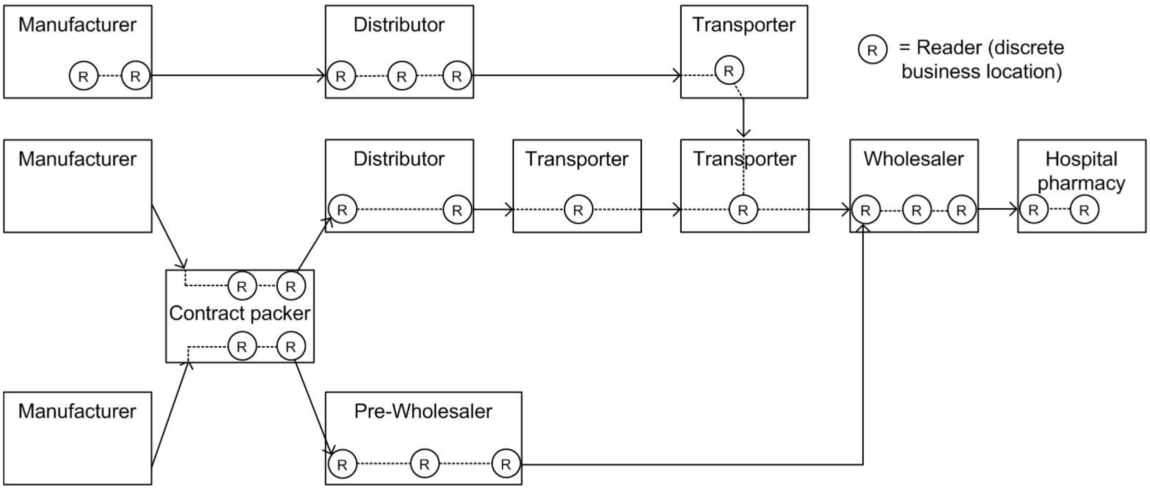


Figure VI-18: *Simulated pharmaceutical supply chain based on the traceability pilot of BRIDGE WP6 (John Jenkins Associates, 2008)*

[12] the corresponding $P_{reliability} = P_{det}/\text{read rate}$

Simulated Real-World Pharmaceutical Supply Chain

The real-world pharmaceutical supply chain under study involves nine different organizations in the UK and Holland, including three manufacturers, a contract packer, distributors, a pre-wholesaler, and a wholesaler that supplies a hospital pharmacy in a major London hospital (John Jenkins Associates, 2008). The products that flow through this supply chain are equipped with printed Data Matrix codes that store serialized ID numbers. Single packs are aggregated into cases and pallets that have both RFID tags and Data Matrix codes. The pallets are scanned in 20 read stations in different supply chain locations to generate track and trace events. The average lead time from production to hospital is about 40 days, varying between approximately one week and two months. The supply chain is illustrated in Fig. VI-18.

In the studied supply chain, traces of products begin either at the manufacturer's production line or at the contract packer's packaging line. Products are shipped to the wholesaler in pallets and the wholesaler uses a "pick, scan, and drop process" to fill boxes that fulfill the pharmacy's orders. The wholesaler delivers products to the hospital pharmacy 2-6 times a day according to orders. The last event in a product's trace occurs when it is scanned in to the hospital pharmacy's inventory, after which the products are identified based on the non-serialized EAN-13 bar codes.

We have built a model of the described supply chain in our own supply chain simulator. The simulator works with three-hour-long discrete time steps. The model is built based on documentation (John Jenkins Associates, 2008) and interviews and it has been validated with direct feedback and example track and trace data. In the simulator, each supply chain node is presented by three different locations corresponding to business steps of receiving, internal processes, and shipping. The time how long an object spends in these locations is given by a uniform distribution. If the product enters a location where there is a reader device, and no read error occurs, a track and trace event is generated. The transitions between the supply chain nodes are determined by transition probabilities. The transition times between the nodes are deterministic and estimated from the distances and transport methods (ship or truck).

The times that logistic units spend in different locations could not be accurate modeled since the real lead time distributions were not precisely known. However, more accurate modeling of the real-world lead times is not likely to affect the results. In addition, because we evaluate the transition probabilities without taking into account correlations among different products' traces, the simulator treats all logistic units as independent from each other, which means that for example aggregation events are not modeled.

Set-Up of the Simulation Study

In every simulation run, all three manufacturers produce 500 tagged products per day during days 1 to 7. This creates 10,500 genuine products and more than 130,000 possible read events. During days 8 to 35, 8 counterfeit products are injected into randomly chosen non-manufacturer supply chain locations per day, constituting a total of 224 counterfeit products. The counterfeit products have ID numbers of randomly chosen genuine products so the events they generate appear in traces of 224 different genuine products. The simulation stops after 60 days. In some rare cases a counterfeit and a genuine product with the same ID are both scanned during the same time step. These cases are not considered in the results.

The results are calculated from the average ROC curves of 10 Monte Carlo iterations. Each iteration yields a number of discrete points in the ROC curve and a continuous curve is drawn by interpolating. The SSCM is trained in each iteration from the training data set and the waiting time distributions in the SSCM are uniform distributions between the smallest and biggest observed waiting times in that business location. The following four tests are performed:

- **Test 1**: The performance of filtering algorithm in finding missing reads from trace data without cloned products with read rates 99.9%, 99.0%, 95%, and 90%, with training data set size of 1000 traces.
- **Test 2**: The performance of $SSCM_L$ and $SSCM_T$ with read rates 99.9%, 99.0%, 95%, and 90%, with training data set size of 300 traces.
- **Test 3**: The performance of $SSCM_L$ with with training data set size 1000, 300, 100, and 50 traces, and read rates 99.9% and 99%.
- **Test 4**: The performance of filtering and $SSCM_L$ with 99% read rate and with training data set size of 300 traces.

Results of the Simulation Study

Results of Test 1 show that the filtering algorithm (subsection VI.3.3) is able to detect up to 86% of missing read events, depending on the read rate and the filter order (cf. Table VI-5). In practice it means, for example, that effective read rate can be increased from 99.0% to 99.84%. Second order filter is able to detect more missing reads than the first order filter when the read rate decreases because of the greater number of consecutive read errors. Moreover, the filter parameters were defined empirically, which still leaves room for optimization.

Table VI-5: *Results of Test 1: Number of missed read events with different filters*

Read rate	No filter	1. Order	2. Order
99.9%	160 (100%)	23 (14%)	23 (14%)
99.0%	1392 (100%)	246 (18%)	228 (16%)
95.0%	6875 (100%)	1541 (22%)	1207 (18%)
90.0%	13920 (100%)	4262 (30%)	2821 (20%)

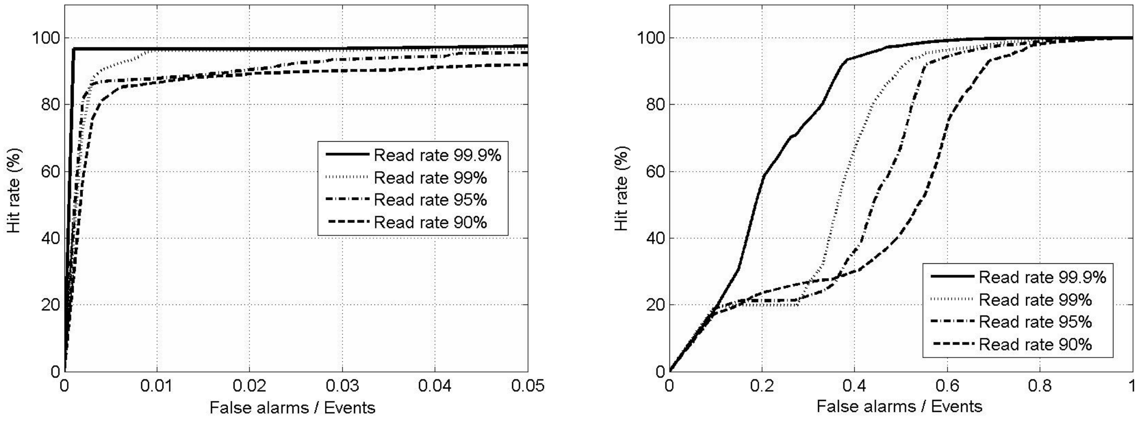


Figure VI-19: *ROC curves for $SSCM_L$ (left) and for $SSCM_T$ (right) (Test 2)*

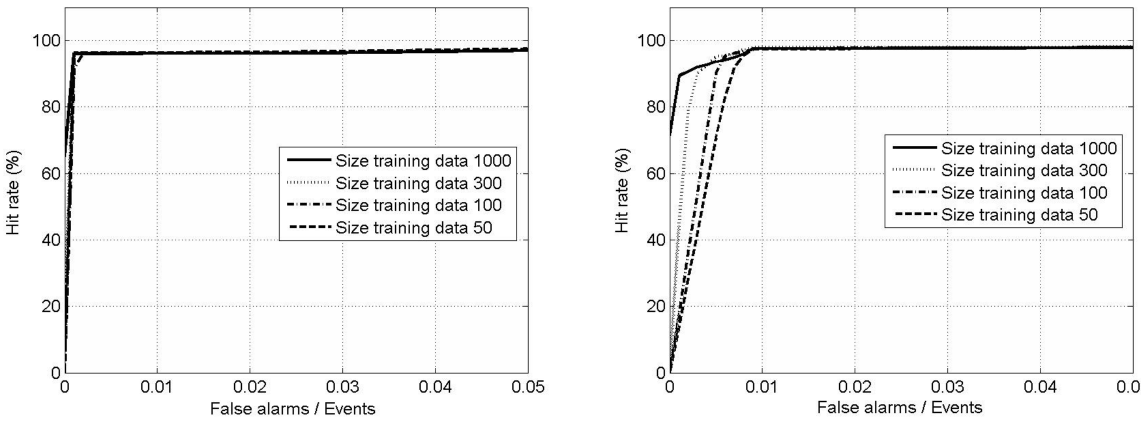


Figure VI-20: *ROC curves for $SSCM_L$ with 99.9% (left) and 99% (right) read rates (Test 3)*

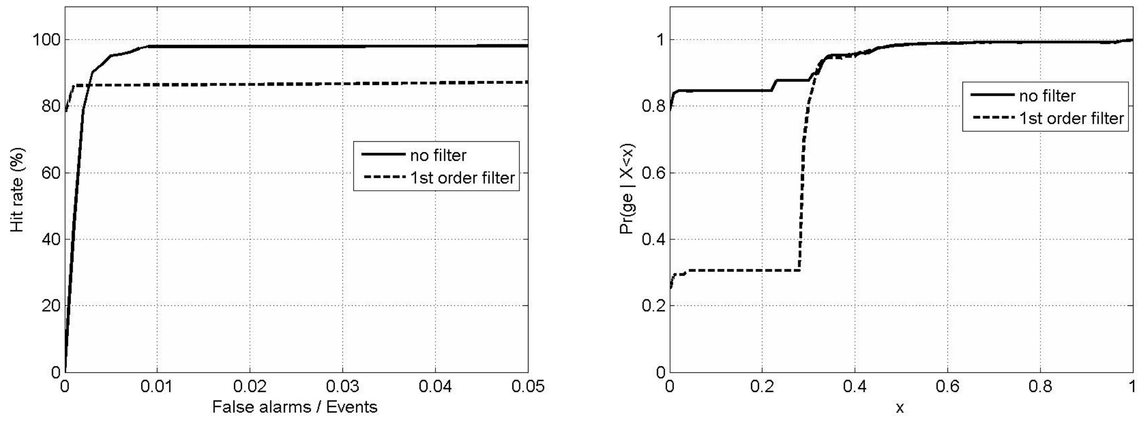


Figure VI-21: *ROC curves (left) and posterior distributions (right) of non-filtered and filtered traces for $SSCM_L$ with 99% read rate (Test 4)*

Results of Test 2 show that that the location-based $SSCM_L$ is much more reliable in detecting cloned tags than the time-based $SSCM_T$, Fig. VI-19 (note the different scales in x-axis). Overall, $SSCM_L$ provides reliable detection results, though the hit rates at the zero false alarm rate are less than 30%. Analysis of false alarms of $SSCM_L$ reveals that in cases when the cloned tag is injected into the location where the genuine product is expected, the cloned tag was not detected (miss) and the genuine product generated a false alarm. The tested $SSCM_T$ method is very prone to false alarms and thus it is not suitable in the studied clone detection application, but the form of the ROC curve confirms that also the transition times carry information that distinguishes events generated by cloned tags from normal events. The results of Test 2 also confirm that missing reads decrease the performance of the studied clone detection methods.

Results from Test 3 show that increasing the amount of training data—that is, more accurate SSCM—improves the reliability of $SSCM_L$ in the presence of missing reads (cf. Fig. VI-20). When the number of missing reads is small, a small amount of training data is enough for accurate modeling of the underlying supply chain. When the number of missing reads increases, more and more ”ghost routes” (cf. Fig. VI-17) appear and more training data is needed to capture them. This indicates that precise modeling of the supply chain contributes to reliable detection of cloned tags.

Results from Test 4 show that the filtering algorithm decreases the number of false alarms cased by missing reads, increasing the hit rate at zero false alarm rate from zero to ca. 80% (Fig. VI-21). Analysis of misses reveals that in some rare cases the filter adds an event before the first event of a cloned tag, causing the miss. However, the overall effect of filtering is clearly positive. The posterior distribution in Fig. VI-21 proofs this by showing that the filtering algorithm increases the probability that an alarm is generated by a counterfeit product from about 30% to 80% in small false alarm rates.

VI.3.5 Summary and Guidelines

The presented study confirms that cloned tags can be detected as abnormal events in RFID traces as soon as the cloned tags enter a protected supply chain. The general learning for anti-counterfeiting is that anomaly-based intrusion detection system techniques, that are commonly used to secure computer networks, could be applied to detect counterfeit products from track and trace data. Missing reads that have not yet been eliminated from existing RFID systems cause abnormal events and thus create false alarms, but they can be effectively mitigated by the presented filtering algorithm that is able to detect most missing reads. Furthermore, the simulation study shows that accurate modeling of the underlying supply chain contributes to reliable detection of cloned tags.

Trying to detect cloned tags based on improbable transition times between supply chain locations did not prove reliable in the conducted simulation study where the cloned and genuine tags flow simultaneously in the supply chain. Nevertheless, this does not mean that event times do not convey information that could be used to improve the reliability of a location-based authentication system.

The concept of location-based authentication is not without limitations. Firstly, if two products with the same identifier are in the same location, a location-based authentication system cannot conclude which of them is the genuine product. In addition, the system can generate false alarms that end-users need to handle with additional verifications. Despite these conceptual shortcomings, the presented method presents a major complication for counterfeiters who want to inject counterfeit products into a protected supply chain, based on processing of the track and trace data that is anyhow captured in many logistics applications.

Guidelines for Track and Trace Data Analysis in Anti-Counterfeiting

- To enable reliable detection of cloned tags, minimize the location uncertainty of the trace data, in the optimal case with a continuous chain of *received-shipped* events for all products in the channel. After the point where all products are no longer scanned, cloned tags can no longer be reliably detected.

- Model the allowed transitions of genuine products between the different supply chain locations. The allowed transitions can be learned from example traces (training data) that do not contain cloned tags, but they can also be manually defined by a supply chain manager. The model needs to be updated when new transitions occur.

- Raise an alarm for the most unlikely transitions that occur for the authenticated products, at least for those transitions that are not allowed for genuine products (i.e. the transition probability is zero).

- Since track and trace data cannot conclude which of two identical tags in the same location is the cloned one, and since false alarms are possible, also another authentication feature is needed. A false alarm can be caused by a missed read for the genuine tag, by a cloned tag that has gone undetected, and by an unusual transition of the genuine product such as reverse logistics.

- If missed read events are likely, have more training data and use the presented filtering algorithm to detect missed reads. The order of the filtering algorithm should correspond to the number of possible consecutive missed reads.

VI.4 Summary of Evaluated Countermeasures

This section evaluates three product authentication concepts for low-cost RFID, two of which are new proposals based on detection of cloned tags. The level of security provided by each method is evaluated with different methods including literature review, expert interviews, an-

Table VI-6: *Summary of pros (+) and cons (-) of the evaluated product authentication concepts*

	Serialized TID Numbers	Synchronized Secrets	Track and Trace Checks
Cost	+ Works on normal low-cost tags	− Requires user memory + Only few manual inspections	+ Works on normal low-cost tags + Works on serialized barcodes − Rare events trigger false alarms
Security	− Vulnerable to tag impersonation − Vulnerable to reprogrammable tags	+ Reliable when scan rate is high − Possible delay before alarm − Vulnerable to trace hijacking − Vulnerable to a new DoS attack + Pinpoints time window of the tag cloning attack	+ Reliable when trace is complete − Vulnerable to trace hijacking
Usability & Performance	− Increased tag read time + Does not require tracing	− Increased tag read time − Additional verification needed + Does not require disclosing of location information	+ No change in tag read time − Additional verification needed − Needs model retraining when underlying supply chain changes

alytical modeling, and simulation study. The need for different methods, and the resulting difficulties in comparing the quantitative results, spurs from the differing quantitative security goals of the three methods. For TID-based tag authentication (subsection VI.1), synchronized secrets method (subsection VI.2), and track and trace checks (subsection VI.3), the quantitative security goals are cost-to-break, detection of tag cloning attacks, and detection of events generated by cloned tags, respectively.

Table VI-6 summarizes the evaluation results. In addition to security, also cost aspects and usability & performance of approaches are considered, and the results are presented as pros and cons. In several cases the line between usability & performance aspects and cost aspects is not clear (e.g. the fact that TID-checks can be conducted without tracing the products). In these cases the judgment call is made from the point of view of the assumed overall RFID project.

Overall, the evaluation shows that secure product authentication can be achieved with low-cost RFID by detection-based measures under certain visibility requirements. Detecting cloned RFID tags is attractive since it does not require more expensive and more energy-thirsty cryptographic tags. Limited visibility introduces uncertainty which is seen as decreasing detection rates and increasing false alarms rates. Moreover, the use of RFID does not remove the need for other security features and additional verifications are still needed to avoid false alarms. Thus these RFID-based approaches should be used as the first step in a multi-step product authentication process that is presented in subsection IV.1.

Owing to heterogeneous characteristics of different approaches, a holistic evaluation is needed to understand all the present trade-offs. For the same reason it is also not possible to conclude which approach is best in general. Rather, the evaluated approaches complements each other. To support brand owners in choosing suitable product authentication approaches, Section VII presents an implementation roadmap toward secure authentication.

VII Consequences and Managerial Guidelines

After a thorough investigation of low-cost RFID-based product authentication concepts, this section synthesizes the managerial research results of this thesis by presenting guidelines for an effective use of low-cost RFID in anti-counterfeiting.

VII.1 Paradigm Shift for Security in Anti-Counterfeiting

An investment in a technical anti-counterfeiting system is an investment in security. The traditional way to think of security in anti-counterfeiting—so called *traditional security paradigm*—is to equate security with the effort to clone or forge the security feature. Thus, affected companies that invest in technical countermeasures pay for cost-to-break and, indeed, modern anti-counterfeiting technologies (e.g. laser surface analysis, color-shifting inks, taggants, microscopic printings, serialized 3D holograms, micro wires, etc.) provide a high cost-to-break.

A market pull for high cost-to-break is also echoed by affected companies' reasons for investing in technical countermeasures. Commonly mentioned reasons for investing in security features are listed below.

- *Removal of the uncertainty about goods' origins:* Though most counterfeit articles can be recognized even only with a trained eye (cf. Fig. VII-1), high-quality fakes can fool even a counterfeit expert. This introduces an uncertainty abouts goods' origins and security features are needed to recognize the increasing number of high-quality fakes.
- *Reliable evidence for legal cases:* Brand owners need security features to have a reliable and credible way to prove the clandestine origins of counterfeit goods in a legal case. In a similar way, brand owners sometimes need a reliably way to prove the clandestine origins of counterfeit goods to consumers in order to avoid disputes.
- *Decrease liability by demonstrating actions:* Affected brand owners can be sued and pushed to protect its clients from counterfeits (e.g. Taylor, 2009; Hopkins et al., 2003, p. 70). By placing security features on their products, a brand owner can measures against counterfeiting to decrease possible liabilities.
- *Visual value-added feature:* A visible security feature such as a hologram can add the perceived value of the genuine product (e.g. Case study National Basketball Association, CACP, 2009).

Though the aforementioned reasons are beneficial for affected companies, they deal with the symptoms of the problem instead of the actual problem itself. This suggests that there is a shortcoming in the traditional security paradigm for anti-counterfeiting—it focuses on making products ”copy-proof” but does not sufficiently address usability and performance aspects which contribute to a higher check rate. And if security features are only rarely checked because the check requires extensive time and effort compared to the perceived benefits, or because the check can be conducted only with special devices that are not widely available, many counterfeit products can flow through the protected supply chain undetected. As a result, the traditional security paradigm might not lead to effective detection of counterfeit products.

Anecdotal evidence of low check rates in today's supply chains support the argument that existing technical countermeasures in general are not effective in detecting counterfeit products. According to statements of affected brand owners, in today's supply chains only a very small ratio of products are checked for authenticity, the checks are not systematic but sporadic, and counterfeit products are rather detected accidentally than as a result of explicit authenticity checks. Even customs inspect only few per cent of consignments (OECD, 1998; Staake, 2007, p. 50). Moreover, the fact that many brand owners do not know how often products are authenticated in their supply chains indicates that authenticity checks are often not systematic.

Counterfeiters' reactions to security features represent further evidence that the risk that counterfeit products are inspected is low for counterfeiters. The argument goes that if the risk that a counterfeit product is inspected is low, counterfeiters do not need to clone or imitate the security features of genuine products. Indeed, empirical data suggests that this is the case by showing that most counterfeit products could be distinguished even without security features. Staake (2007) analyzed the characteristics of 128 counterfeit articles from 38 brands and over ten product categories, constituting the most comprehensive body of empirical data published about counterfeit articles. The data was gathered by interviewing experts[1] and it shows that up to 87.4% of counterfeit products could be recognized by trained inspectors based on visual quality[2] (Staake, 2007, pp. 76-77). This is illustrated in Fig. VII-1.

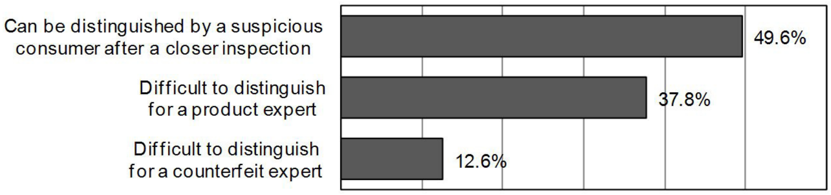


Figure VII-1: *Visual quality of counterfeit products (Staake, 2007)*

All in all, the data shows that most counterfeit products could be detected simply by increasing the number of authenticity checks, even without a high cost-to-break. A high cost-to-break is still needed to detect high-quality fakes—according to Fig. VII-1 about 10% of counterfeit

[1] Interviewed experts were asked to rate the visual quality of counterfeit articles in the following scale: (1) Counterfeit origin obvious for non-expert without closer inspection; (2) Counterfeit origin obvious for non-expert only after closer inspection; (3) Counterfeit can be recognized by suspicious consumer only after closer inspection; (4) Difficult to distinguish for product expert; (5) Difficult to distinguish for counterfeit expert

[2] This implicitly means that the inspector does not using semi-covert, covert, and forensic security features

articles—which have a very high visual quality that can fool even a counterfeit expert. But technical anti-counterfeiting measures do not need to be designed only to help authenticate these high-quality fakes.

Shortcomings in the traditional way to think of security in anti-counterfeiting can be overcome with a paradigm shift. Since the ultimate function of a product authentication system is not to make products ”copy-proof” but to detect counterfeit products, security of a technical anti-counterfeiting solution should rather be equated with the system's capability to detect counterfeit products. This represents a paradigm shift for what security means in anti-counterfeiting.

The new paradigm focuses on securing a supply chain instead of a product, and it can be applied both to licit and illicit supply chains that have different possible points of intervention (cf. subsection VII.3). The qualitative security goal is a high counterfeit product detection rate which, according to the presented econometric analysis (cf. subsection V), is the central parameter of the process of security that defines a counterfeiter's expected payoff. Moreover, the new paradigm represents the practical level of protection provided by the security measure since it takes into account the usability and performance aspects that, according to Bishop (2003), ultimately define a system's security.

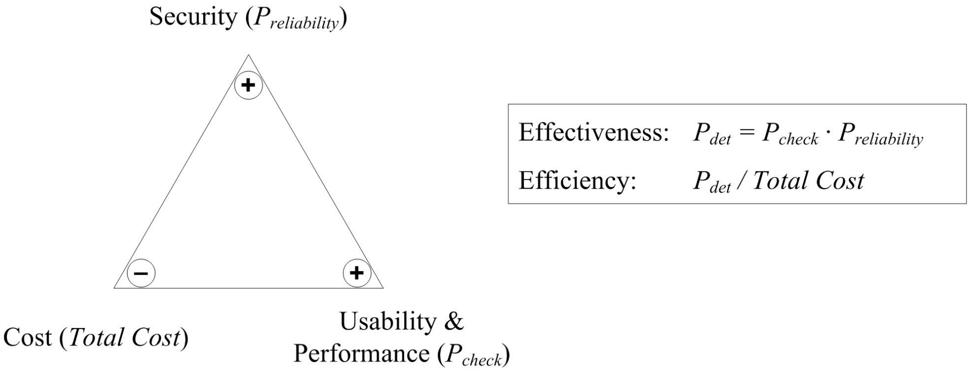

Security ($P_{reliability}$)
+
−
+
Cost (*Total Cost*)
Usability & Performance (P_{check})
Effectiveness: $P_{det} = P_{check} \cdot P_{reliability}$
Efficiency: P_{det} / *Total Cost*

Figure VII-2: *Effectiveness and efficiency of a technical anti-counterfeiting system*

Figure VII-2 presents the quantitative reasoning behind this new paradigm by explaining how the trade-offs that are inherently present in all security applications (cf. subsection I.2.3) define the effectiveness and efficiency of a technical anti-counterfeiting measure. The intrinsic level of security of a security measure defines the probability that a counterfeit product is detected in a check, denoted $P_{reliability}$, and the way the security measure is used defines the probability that a counterfeit product is checked, denoted P_{check}. As a result, the effectiveness of the overall system is characterized by the probability that a counterfeit product is detected, $P_{det} = P_{check} \cdot P_{reliability}$, and its efficiency by P_{det} divided by the total cost of the solution.

The presented paradigm shift demonstrates how goals and metrics matter in security applications. By redefining the goals of technical anti-counterfeiting measures, also their role in a company's overall anti-counterfeiting strategy can be shifted from treating the symptoms and

Table VII-1: *Traditional and new paradigm for security in anti-counterfeiting*

	Traditional security paradigm	New security paradigm
Secured asset	• Product	• Supply chain
Qualitative goals	• Make genuine products ”copy-proof” • Remove uncertainty of goods’ origins • Reliable evidence for legal cases • Decrease liability by demonstrating actions • Visual value-added feature	• Effective and efficient detection of counterfeits • Make counterfeiting financially unattractive
Quantitative goals	• $P_{reliability} = 100\%$ • High *cost-to-break*	• $P_{reliability} >$ ”good enough” • $P_{check} = 100\%$
Major trade-off	• Feature cost vs. *cost-to-break*	• Total cost vs. P_{detect}

minimizing the losses toward making counterfeiting financially unattractive for illicit actors.

Operationalizing this paradigm shift in practice requires increasing check rates and decreasing cost and effort to conduct the checks, which is why RFID appears a particularly effective tool for protecting supply chains against counterfeits. The following subsection discusses the role of RFID with respect to the new security paradigm. Characteristics of the old and new security paradigm are summarized in Table VII-1.

VII.1.1 Low-Cost RFID and the New Security Paradigm

A technical anti-counterfeiting system based on low-cost RFID has the potential to overcome shortcomings of many existing solutions. Foremost, RFID increases the number of products that can be verified in practice. A solution based on standard RFID tags and readers can overcome the problems of dedicated checking equipment and scarcity of hardware vendors (cf. Table I-1). Combined with the ability to check multiple products at once without line of sight, this can lead to a dramatic increase in the number of products that can be checked for authenticity. Even though the authenticity checks that low-cost RFID enables might be less reliable than those enabled by state-of-the-art security features, a solution based on low-cost RFID can still detect more counterfeit products owing to its higher check rate.

Integration of authentication to existing identification processes is a particularly efficient way to authenticate 100% of products with a minimal additional effort. This means conducting authenticity checks as a part of identification when products are handled. Successful integration of authentication to existing identification processes is demonstrated in three real-world trials of the SToP project where pharmaceutical bottles, hard and soft luxury goods, and aircraft parts were authenticated in simulated real-life scenarios (Magerkurth et al., 2008; Lehtonen et al., 2009a). These products were authenticated using standard RFID tags and 2D barcodes as a part of business processes[3] where which include identification (cf. Fig. VII-3). The trialled

[3] The trialled business processes include reception of incoming goods in a pharmacy, packaging of soft luxury

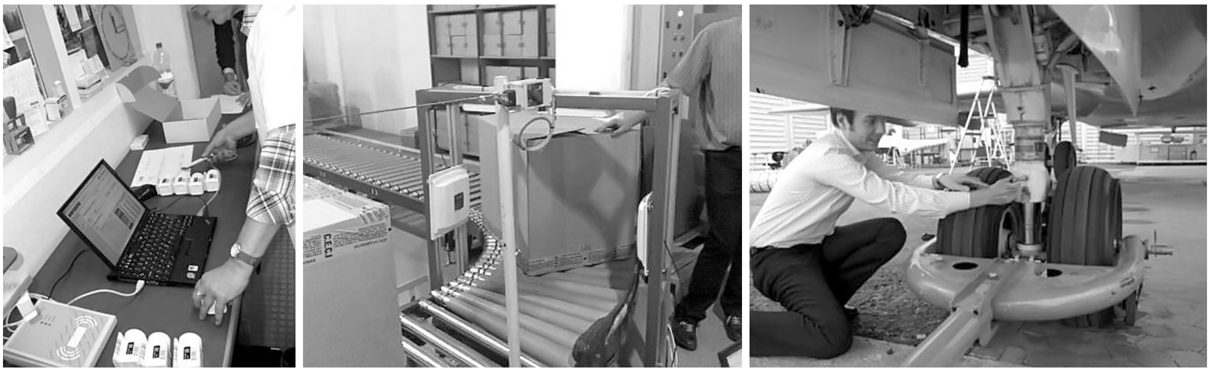


Figure VII-3: *Integration of authentication to existing identification processes using RFID is demonstrated for pharmaceutical goods (left), luxury goods (middle), and aviation spare parts (right) in the SToP project (Magerkurth et al., 2008; Lehtonen et al., 2009a)*

product authentication techniques included TID checks (cf. subsection VI.1), track and trace based checks (cf. subsection VI.3), and manual feature checks by users.

By moving from static hard-to-copy features to detection-based authentication (e.g. track and trace checks), brand owners can steer away from the cat and mouse game of replacing security features as they are compromised and can be forged by counterfeiters. The downside of detection-based measures is the uncertainty caused by location uncertainty in cases where the tracing data is not complete. This uncertainty can cause false alarms and misses (cf. subsection VI.3) and therefore an alarm needs to be preceded by an additional authenticity check. Though this represents duplicated effort, the detection-based measure can be seen as a very effective screening technique. Furthermore, the number of needed additional inspections can be minimized with the presented synchronized secrets method that triggers only as many alarms as there are cloned tags that have entered the system (cf. subsection VI.2).

Regarding the cost to protect one product, low-cost RFID tags can still be up to ten times more expensive than competing security features; while Gen-2 tags cost about $0.10 apiece in volumes of millions (M. Nikkanen 2009, pers. comm., 2 November), security features can be bought for $0.01-0.03 (Hopkins et al., 2003). However, a low-cost RFID tag and a high-tech security feature have very different value propositions and their prices should be evaluated in the context of their business value. In this regard RFID has two important advantages over dedicated security features:

- Because of reasons detailed above, RFID-tagged products can be authenticated more often than products tagged with dedicated authentication technologies. This decreases the price-per-check and contributes toward a high counterfeit product detection rate.
- RFID is a platform technology that enables multiple Auto-ID applications and only a part of the tag cost (and other infrastructure costs) needs to be accounted to anti-counterfeiting

goods in a distribution center, after sales service of hard luxury goods, and aircraft part exchange application. Brand protection can therefore be considered as an additional way to depreciate the overall RFID investment.

VII.2 Roadmap Toward Secure Authentication of EPC-Tagged Products

Products tagged with EPC tags can be authenticated with various security measures. The choice of the security measure affects the level of security, cost, and usability & performance of the technical system and therefore choosing a suitable security measure for a product is challenging. The good enough security paradigm of Sandhu (2003) and the proposed security paradigm for anti-counterfeiting (cf. subsection VII.1) suggest that the security measure should be chosen to provide a high enough $P_{reliability}$ (i.e. close to 100%). This helps keep the cost of the solution down and contributes toward a higher check rate.

Which security measures are needed to achieve a high-enough $P_{reliability}$ depends on counterfeiters' incentives and actions to break or bypass the authenticity checks for that product. Moreover, the needed level of protection evolves in time in a war of escalation between the brand owner and counterfeiters. Since RFID provides a platform of multiple security measures, brand owners can adopt more complex and costly measures as they become necessary.

To help brand owners choose suitable security measures in this war of escalation, a roadmap from identification to secure authentication of EPC-tagged products is presented. The security measures included in this roadmap cover both existing concepts as well as concepts that might become possible for EPC tags in future, namely strong cryptography and physical unclonable functions. The starting point of all serialization-based product authentication approaches is identification of the tagged object and verification that the object's serialized ID number (e.g. SGTIN) is valid. This approach only requires a white list Koh et al. (2003) where the valid identifiers are stored. Alternatively, serialized ID numbers can be verified offline using the digital signature scheme outlined in subsection II.4.2.

For products where the risk due to counterfeiting is low, such as some non-branded fast moving consumer goods, the basic measure provides a good starting point. For products where the risk due to counterfeiting is augmented, such as patented life-saving drugs or airplane spare parts, the need for security is higher and more advanced security measures are needed. The following subsection proposes a roadmap for the implementation of these security measures.

VII.2.1 Security Measures

The basic measure can be turned into secure product authentication by addressing tag cloning and tag removal and reapplying attacks. The former is addressed by security goals of increasing tag cloning resistance and detecting cloned tags and the latter by increasing tag-product integrity. Figure VII-4 illustrates the roadmap as a use/misuse case diagram. In this illustration, white ovals correspond to security goals and gray ovals represent security measures.

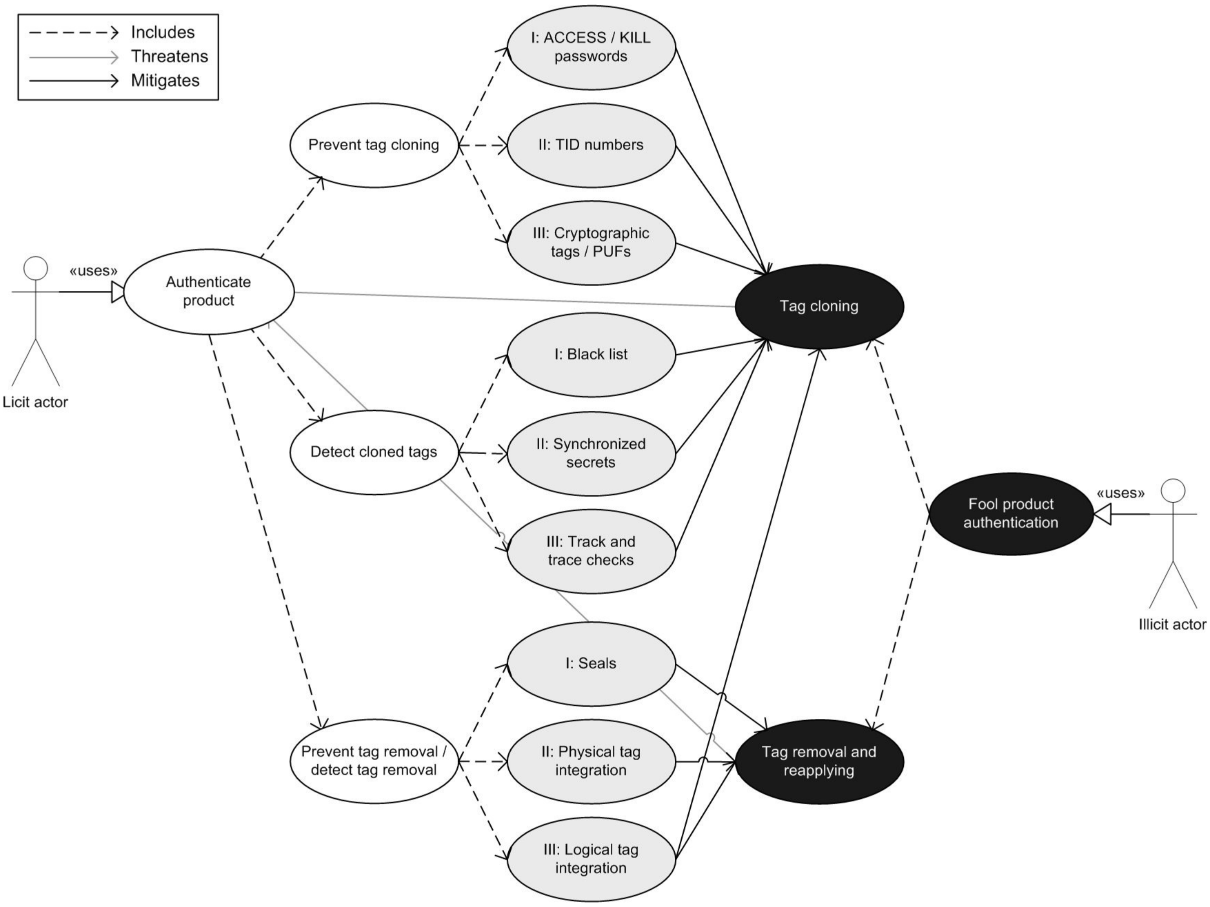

Includes
Threatens
Mitigates
Licit actor
«uses»
Authenticate product
Prevent tag cloning
Detect cloned tags
Prevent tag removal / detect tag removal
I: ACCESS / KILL passwords
II: TID numbers
III: Cryptographic tags / PUFs
I: Black list
II: Synchronized secrets
III: Track and trace checks
I: Seals
II: Physical tag integration
III: Logical tag integration
Tag cloning
Tag removal and reapplying
Fool product authentication
«uses»
Illicit actor

Figure VII-4: *Implementation roadmap toward secure authentication of EPC-tagged products*

Prevent Tag Cloning

The simplest prevention-based measure against tag cloning is to use the *ACCESS and KILL* commands to authenticate the tags (Juels, 2005). Implementation of KILL-password based authentication is feasible in deployed tags, but presents some delicate technical challenges (Koscher et al., 2008). These approaches are vulnerable to brute force attacks against the 32-bit passwords and eavesdropping. The second option is to use serialized *TID numbers* which provide a practical hurdle against tag cloning today but but are not a long-term solution (cf. subsection VI.1). The highest level of tag cloning resistance is achieved with *cryptographic tags* or *physical unclonable functions* (PUFs) that have been demonstrated on UHF tags but are not yet commercially available (cf. subsection III.4).

Detect Cloned Tags

The first detection-based measure against tag cloning is to *black list* identifiers of those products who have been sold, consumed, or otherwise become invalid. This restricts the time window when a given identifier is valid and thus can be exploited by a counterfeiter to fool the product authentication system. More advanced detection-based measured include the *synchronized secrets* approach (cf. subsection VI.2) and *track and trace checks* (cf. subsection VI.3). Compared to black listing, these techniques can also detect cloned identifiers before the corresponding product has been sold or consumed.

Prevent and Detect Tag Removal

Tag-product integrity guarantees that a tag is attached to the right product and it is provided through preventing and detecting tag removal and reapplying. *Sealing of tag* to the product or its packaging is a straightforward way to improve tag-product integrity because it makes removing and reapplying genuine tags harder. In addition, state-of-the-art techniques allow secure integration of RFID tags to various physical products depending on the characteristics of the product, for example inside watches that are fully made of metal (though not with standard Gen-2 tags) (Cook et al., 2008). *Physical tag integration* can make the tag hard to find, hard to remove without breaking the tag and/or the product, and hard to reapply to a counterfeit product. The strongest tag-product integrity is achieved through *logical tag integration* where the product's unique features are stored in the tag and verified to establish that the tag is attached to the right product (Nochta et al., 2006). This also mitigates tag cloning attacks since it corresponds to direct product authentication.

VII.3 Supply Chain Locations for Product Authentication

A product authentication system can be used in different supply chain locations covering check points in both licit and illicit supply chains. The location where authenticity checks are conducted has a major influence on how a technical solution can address product counterfeiting. This subsection analyzes possible supply chain locations for product authentication.

Possible supply chain locations for product authentication are identified based on usage scenarios from SToP and BRIDGE projects and from public example cases. The identified supply chain locations are mapped to a generic model of licit and illicit supply chains (Staake, 2007) spanning from manufacturer to consumer/end-user, excluding suppliers of parts and components. The resulting supply chain locations are illustrated in Fig. VII-5. Description of the supply chain locations cover product handling, how a technical solution addresses the problem, and Auto-ID based solution integration.

VII.3.1 Description of Supply Chain Locations

1. *Inside distribution:* Counterfeit products can enter the licit supply chain in the distribution level between manufacturing and retail (e.g. Lipitor case, 2003[4]). Counterfeits

[4] Pfizer (2007). Case Study: Lipitor US Recall. http://media.pfizer.com/files/products/LipitorUSRecall.pdf

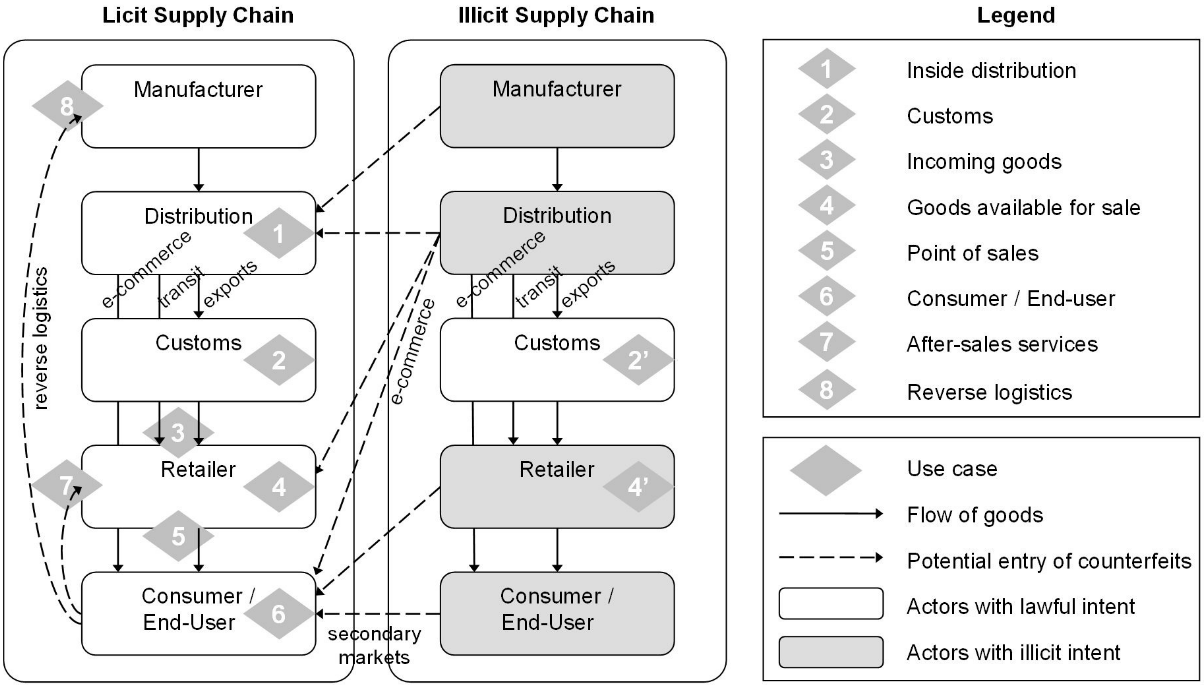


Figure VII-5: *Possible supply chain locations for product authentication*

can appear either as complete consignments of faked goods or co-mingled with genuine goods (e.g. Case study Xerox, CACP, 2009). Authenticity checks in the distribution level, e.g. in distribution centers, help detecting these counterfeits. Since logistic units (pallets, cases, boxes, toads, single goods etc.) are identified using Auto-ID inside the distribution level, the existing Auto-ID processes provide an opportunity for integration of automatic authenticity checks (cf. subsection VII.1.1).

When products are handled in known lot sizes or one by one (e.g. luxury goods), untagged counterfeit articles can be detected without additional effort to count the inspected products. Another important efficiency factor is the relatively small number of distributors (e.g. compared to the number of retailers); when all genuine products flow through a relatively small amount of supply chain locations, the whole product population can be authenticated with a smaller number of check locations. Furthermore, authenticity checks inside distribution can detect the counterfeit products as soon as they enter the licit supply chain, close to the illicit actors. This increases the chances of detecting and successfully prosecuting infringers. On the other hand, counterfeit products can enter the supply chain also further downstream.

When the brand owner or manufacturer does not have its own distribution network but relies on external parties (i.e. external licit supply chain), active collaboration of the external distributors is required. Obtaining the needed commitment from external distributors can be challenging since distributors might not get direct business benefits from conducting authenticity checks. Engaging distributors can be especially challenging for small brand owners. As a partial solution, managerial research suggests that manufacturers can engender cooperativeness of distributors by nurturing satisfaction and dependence in manufacturer-dealer relationships (Olsen and Granzin, 1993). In particular, senior management's commitment to supply chain security is needed in order to gain distributors' assistance in fighting counterfeit trade (Olsen and Granzin, 1993).

2. *Customs:* Customs conduct most counterfeit seizures in the world and thus it is a key stakeholder in any anti-counterfeiting strategy. Though anti-counterfeiting is not the number one priority for customs, customs is often the best locations to interfere the illicit supply chain. Therefore supporting customs in anti-counterfeiting not only protects the licit supply chain from counterfeit products but also affects the illicit supply chain, inflicting a broad effect on counterfeiters' business.

   Brand owners can collaborate with customs by offering training and tools to detect counterfeit products. However, customs are reluctant to adopt multiple authentication devices. Though many brand owners provide customs with devices to authenticate their devices, customs officers rarely know how to use them properly. Rather, a simple standard solution that can handle different kinds of products is preferred. Such a standard solution does not exist today and hundreds of different product authentication solutions are being used, but integration of authentication to RFID standards has potential to change it.

   Today customs verify only few per cent of imported consignments. These checks are sporadic and not coupled with regular goods handling. As a result, a system that is able to authenticate one good at a time is sufficient. Customs need mobile or hand-held verification devices since inspections are conducted not only in customs warehouses, but also on highways, in company warehouses, and other remote locations. Sporadic checks of single samples helps customs identify counterfeit consignments faster and easier, but they are not effective in detecting small quantities of counterfeit articles co-mingled among genuine products. Last, the technical solution does not need to provide a 100% level of confidence since the affected brand owner is in the end responsible of proving the origins of seized products.

3. *Incoming goods:* Retailers are in a critical position to engage in countermeasures against product counterfeiting (Olsen and Granzin, 1992). The retail level comprises typical consumer good retailers and other end-points such as pharmacies, hospitals, as well as small boutiques and garages. Authenticity checks in the retail level can be integrated to the process where incoming goods are scanned in to the inventory before placing them to the back room storage or shop-floor. Authentication of incoming goods in the retail level is potentially a very effective way to secure the licit supply chain.

   When incoming goods are subject to verifications already in the existing process, such as expiry data verification and order completeness verification, the overhead of integrating an authenticity check to the existing process can be done with a small overhead. A small overhead is also a requirement when the process of scanning in incoming goods is time-critical. Furthermore, when the lot sizes of incoming goods are fixed or otherwise known, detection of untagged counterfeit products can be automated.

In theory, the point of sales or point of consumption is the most secure final check point in a supply chain, since injection of counterfeit products is no longer possible after the last check point. In practice, however, the same effect can be achieved more easily by checking incoming goods in the retail level, if the integrity of retail inventory can be guaranteed. In particular, this requires addressing internal threats of employees, such as the possibility of replacing a genuine product by a counterfeit one. A general downside with authenticity checks in the retail level is that the counterfeit products are detected in a late point in the supply chain, which makes tracing the source of counterfeit goods harder. Also, a large number of check points is needed.

Engaging the collaboration of retailers can pose similar challenges than that of external distributors, as discussed above. According to Olsen and Granzin (1992), perceived seriousness of the problem and internal acceptance of responsibility are the most important factors that influence how willingly channel members assist manufacturers in anti-counterfeiting . Furthermore, management practices that induce higher satisfaction and dependence, but lower conflict and control, will enhance a manufacturer's ability to gain the help of retailers (Olsen and Granzin, 1993).

4. *Goods available for sale:* Authenticity checks can secure the retail level from counterfeits also through verifications of goods available for sale (e.g. on shelves). This can be done either with the consent of the retailer, for instance as an audit, or without the consent of the retailer, for instance as mystery shopping by a private investigator. A prerequisite for these checks is that the verified products are openly displayed, which restricts application of this scenario mostly to consumer goods. This restriction, however, can be overcome by conducting test purchases. Therefore this usage scenario also covers test purchases through e-commerce. In addition to brand owner, in principle also consumers can authenticate goods available for sale themselves (cf. consumer / end-user below).

   Checks of goods available for sale can be targeted to suspicious or high-risk targets for an increased effectiveness. These checks are not likely to be conducted as a part of handling processes where goods are identified or otherwise verified, and therefore they cause additional effort. But this effort needs to be seriously considered since, together with checks in customs, this is the only way to interfere with the illicit supply chain (excluding infiltrating private investigators into the illicit supply chain).

   An RFID-based solution with a long read range suits this scenario well since it enables quick and imperceptible verifications in bulk mode. In order to detect untagged counterfeit items, however, the number of verified items must be counted. Last, since this check is conducted at a late state of the supply chain, tracking down the sources of detected counterfeit goods can be hard.

5. *Point of sales:* Authenticating products at the point of sales or at the point of consumption secures the last link of the licit supply chain. At this final step of the distribution channel products are handled one by one so no additional effort is needed to count the verified articles to detect untagged counterfeit articles. Furthermore, point of sales systems already identify products with Auto-ID (e.g. to scan the price, to verify the expiration date of drugs). These two conditions can minimize the additional effort needed to integrate authenticity checks to the process how products are handled.

   On the other hand, introducing systematic authenticity checks in the point of sales level is challenging. Foremost, authenticating products in front of the consumer, patient, or end-user interferes with the customer relationship (Lehtonen et al., 2009a). For example, authentication of pharmaceutical products in front of the patient can decrease the trust toward the doctor or pharmacist, and authentication of luxury goods can ”break the romance” of the carefully designed buying experience. In general, retailers do not want to deal with product counterfeiting issues in front of their customers since it can generate negative associations among customers. In particular, this usage scenario can be the first time when customers learn that counterfeit products could appear in the retail shop. The retailer’s dilemma is that the associations are perceived as negative, though the authenticity checks are conducted for the customers’ own good.

   Also other factors make authenticity checks challenging in the point of sales level. The checks take place in a time-critical process where additional delays are not welcome and they take place far from the sources of counterfeits. Last, the vast number of possible point of sales locations makes diffusion of the technology and process changes burdensome and probably possible only with standards, mandates, and regulations[5].

6. *Consumer / End-user:* Enforcing consumers and end-users with the capability to authenticate products has a big potential in enabling secure supply of genuine goods and countering deceptive counterfeiting in regions where counterfeit products might appear in the retail level. For instance, drugs sold in Ghana have a unique numeric code that can be scratched and send with an SMS to verify their authenticity[6]. Nokia uses similar numbers in their batteries[7], and a similar system is in use in the Hong Kong Airport[8].

   Involving consumers through mobile phones could potentially empower masses of people with the ability to authenticate products in locations where brand owner cannot access otherwise, including secondary markets (e.g. flea markets, C2C sales) and new geographic areas. Also community-based product authentication applications have been proposed for mobile applications (von Reischach et al., 2007). In addition to relying

[5] For instance, the European Federation of Pharmaceutical Industries and Associations (EFPIA) is trialling methods to meet the European Commission’s new traceability requirements. http://www.efpia.org/Content/Default.asp?PageID=566

[6] MPedigree (2009). http://www.mpedigree.org/home/

[7] Nokia (2008). http://www.nokia.co.id/nokia/0,,82227,00.html

[8] RFIDJournal (2009). http://www.rfidjournal.com/article/view/5022/1

on consumers' own devices, this usage scenario can also be enabled by installing reader kiosks where consumers can authenticate products themselves. However, in this approach the consumer has no real means of assuring whether the reader kiosk is trustworthy and yields right results or not.

Despite the vast potential of involving consumers, currently this usage scenario is only very rarely utilized due to an atmosphere of denial and secrecy. In general, many brand owners believe that "*you should not involve your customers in your dirty laundry*". Indeed, there are arguments for not involving consumers in anti-counterfeiting efforts. First, there might be a sales drop due to bad publicity and admittance of the problem. Second, the required effort and cost of empowering consumers might be too high to justify the benefits. Third, by giving consumers the capability to recognize counterfeits more consumers might turn to the secondary markets to buy second-hand products instead of new ones. And fourth, possible false alarms of the authentication technology could lead to liability claims. In addition, consumers also buy some counterfeit products intentionally, which limits this usage scenario to those product categories where consumers have good incentives to buy the genuine product.

While consumers can refuse buying counterfeit articles, they lack law enforcement power to launch responses against the infringers and thus should be supported by the brand owner. In addition, consumers also buy some counterfeit products intentionally, which limits this usage scenario to those product categories where consumers have good incentives to buy the genuine product.

The second part of this usage scenario is authentication of products that are being used by end-users. A prominent example is authentication of spare parts in the aerospace industry where counterfeiting does not really affect the supply chain through which the genuine spare parts are delivered, but the network of repair, maintenance and overhaul depots where the spare parts are used. In this case the authenticity checks can be integrated to existing processes where the spare parts are already identified with Auto-ID. In general, missing tracing infrastructure or lack of data sharing limits the use of detection-based authentication in this usage scenario, so prevention-based measures might be preferred.

7. *After-sales services:* In some cases counterfeit goods can enter the licit supply chain in after sales services when customers return goods that are already bought. This can be a relevant scenario for example in the luxury goods industry where products are used during long periods of times and sometimes they need to be returned for repair, polishing or refurbishment. Though authentication of products in after-sales services does not prevent a consumer from getting a counterfeit product, it enables easy detection of counterfeits in an early phase of the service.

   From the process point of view, authentication of these products is relatively easy since these products are handled one by one or in small quantities, within the premises of a retailer or brand owner (e.g. a luxury goods boutique). Due to the interference with the customer relationship (cf. point of sales scenario above) it might be preferable not to authenticate these products in front of the customer but rather in the back room or service level. This is also a preferable practice in those cases where the customers knowingly bring counterfeit goods to after-sales services with the hope of getting them replaced by genuine goods since a face-to-face conflict with these fraudulent customers is avoided.

From the technical point of view, lack of complete trace data limits the use of location-based authentication approaches in this usage scenario. Regarding the migration of serialization labels, this usage scenario also needs to handle non-tagged genuine products, including those product categories that are not tagged as well as older articles that were not yet tagged. Last, tracing the source of the counterfeit products detected in this usage scenario can be very hard.

8. *Reverse logistics:* Similar to the after-sales services scenario, counterfeit products can enter the licit supply chain also among products that are returned to the manufacturer under warranty. This can be an issue in particular with electronics, batteries, computer chips and mechanical components or accessories, where manufacturers are seeing an increase in counterfeit parts being returned to manufacturers under warranty and claiming replacement. Manufacturers of these products have difficulties authenticating returned articles and, without appropriate technology and processes, can find themselves forced to replace a counterfeit article with a genuine article. In this case an authenticity check can be integrated in the service process on the manufacturer's side.

   Compared to checks in the lowest levels of the supply chains, only a very small number checking locations is needed. The downside of this usage scenario is that it is very far from the source of counterfeits and its benefits are limited to elimi-nating the losses due to replaced or fixed counterfeit products

Table VII-2: *Summary of supply chain locations for product authentication*

Location	Licit Supply Chain	Illicit Supply Chain	Auto-ID Integration	Trace
1. Inside distribution	X		X	X
2. Customs	X	X		X
3. Incoming goods	X		X	X
4. Goods available for sale	X	X		X
5. Point of sales / consumption	X		(X)[9]	X
6. Consumer / end-user	X		(X)[10]	
7. After-sales services	X		X	
8. Reverse logistics	X		X	

[9] Auto-ID integration is typically possible in point of sales but not in point of consumption

[10] Auto-ID integration is typically possible in checks by end-users but not in checks by consumers

Table VII-3: *Conceptual feasibility of RFID-based product authentication approaches*

Location	White List	Black List	Track & Trace	Sync. Sec.	Password/Secret
1. Inside distribution	Ok	Ok	Ok	Ok	Ok
2. Customs	Ok	Ok	Ok	Ok	Ok
3. Incoming goods	Ok	Ok	Ok	Ok	Ok
4. Goods available for sale	Ok	Ok	Ok	Ok	Ok
5. Point of sales / consumption	Ok	Ok	Ok	Ok	Ok
6. Consumer / end-user	Ok				Ok[11]
7. After-sales services	Ok	Limited[12]	Limited[13]	Limited[13]	Ok
8. Reverse logistics	Ok				Ok

VII.3.2 Implications to a Technical Countermeasure

Table VII-2 summarizes the main characteristics of different supply chain locations by presenting if checks in these locations protect the licit supply chain, target the illicit supply chain, provide possibility to integrate authentication to existing Auto-ID process, and potentially have trace data available. In addition to these usage scenarios, technical anti-counterfeiting measures can support private investigators and law enforcement agencies in raids to suspected production and storage locations of counterfeit products.

The choice of supply chain locations restricts the applicability of certain product authentication approaches. Track and trace data can typically be gathered only until the point of sales—though in most cases the manufacturer loses the trace of the product much earlier. This limits the applicability of location-based authentication approaches. Table VII-3 presents the conceptual limitations of the product authentication approaches considered in subsection VII.2.

The use of black list approach is limited after the genuine product's ID number is blacklisted. In further down stream supply chain locations, for instance in after-sales services, black list approach does not help distinguish cloned tags from the genuine tag. Track and trace checks and synchronized secrets approach can detect cloned tags reliably only until the point where the genuine products are tracked and in further down stream supply chain locations a single cloned tag can easily go undetected (a problem denoted as *trace hijacking*). However, the existence of multiple cloned tags can still be detected. Last, the use of approaches that rely on passwords or secrets relying on the tag (e.g. ACCESS/KILL password, symmetric key cryptography depending on implementation) is limited to trustworthy parties if the secret information is disclosed to the authenticator and allow tag cloning.

[11] Can be made available only to trustworthy parties if the verifier learns the password/secret

[12] In addition to copied tags, also the genuine tag will raise an alarm after the ID number is blacklisted

[13] Single cloned tags cannot be reliably detected once the genuine product is no longer traced, but the existence of multiple cloned tags can still be detected, especially if the number of copied tags with same ID number is high

VIII Conclusions

Product counterfeiting continues to plague brand and trademark owners across industry sectors. This thesis has investigated how radio frequency identification (RFID) technology can help brand owners fight product counterfeiting by researching how a supply chain can be effectively protected against counterfeit products using low-cost RFID tags. This question has been answered based on a systematic approach to model security in anti-counterfeiting.

Product authentication is the core of technical anti-counterfeiting measures. The level of security in product authentication is equal to how reliably inspected counterfeit products are detected. According to the starting assumption of this thesis, products that are tagged with low-cost RFID tags such as the EPC Class-1 Gen-2 cannot be authenticated in a secure way since these tags can be cloned. Despite past advances in minimalistic implementations of standard cryptographic primitives, this assumption still holds true because cryptographic units will increase the tag price and thus they will not be available for the most inexpensive tags.

Unlike the majority of contributions in this field, this thesis has investigated product authentication approaches based on reliable detection of cloned tags. The proposed approaches are based on the visibility that RFID provides and they include an approach based on synchronized secrets on tag and back-end and on track and trace data analysis. The major advantage of these approaches over cryptographic tag authentication is that they can be used with existing off-the-shelf low-cost RFID tags. Evaluation of the proposed approaches confirms that they can detect cloned tags in a reliable way in supply chains where tagged products are traced. Moreover, comparison of the proposed approaches revealed many trade-offs between security and cost/usability, and therefore choosing the optimal approach depends on the specific case.

In addition to developing new security concepts for low-cost RFID, the usage of technical anti-counterfeiting measures is studied. Though security literature agrees that the level of security is ultimately defined by the way security measures are used, managerial research on anti-counterfeiting is limited to outlining high-tech labeling strategies without detailing how and where the technology should be used. To bridge this research gap, an implementation roadmap toward secure product authentication with EPC Class-1 Gen-2 is proposed and possible supply chain locations for product authenticity checks are analyzed. In addition, guidelines for reaching a high counterfeit product detection rate with low-cost RFID are presented.

The general findings of this thesis have been used to formulate a new paradigm for security in anti-counterfeiting; instead of equating security with the cost to copy or bypass the security feature, it is argued that security should rather be equated with the system's ability to effectively detect counterfeit products. Indeed, anecdotal evidence suggest that technical anti-counterfeiting measures have failed to detect counterfeit products in an effective way owing to low check rates. Low-cost RFID has the potential to change this by decreasing the effort and cost to authenticate products, contributing toward safer supply chains across industry sectors.

VIII.1 Theoretical Implications

The systematic view to security of this thesis significantly adds to the current understanding of the effectiveness of technical anti-counterfeiting measures. The provided security requirements analysis showed that there are three general approaches to authenticate products corresponding to the three ways how tag cloning attack can be mitigated. In particular, this thesis has formulated a location-based product authentication approach that detects cloned tags based on track and trace data analysis, and extended the existing synchronized secrets concept to detect RFID tag cloning attacks. These detection-based approaches enable authentication of products without needing cryptographic computations from the tags. The general downsides of these approaches are false negatives and false alarms that are both caused by imperfect visibility.

In addition to the mechanisms of product authentication, an explanatory model is provided to the overall effect of technical, organizational, and legal measures that protect a supply chain against counterfeit products. It is shown that a supply chain is protected by subsequent prevent-detect-react processes, though their overall effect can be modeled with only one process to quantify the direct and deterrent effects of security.

The economic analysis derived the theoretical conditions for considering a supply chain secure from counterfeits based on the rational choice theory, and discussed limitations for these conditions caused by bounded rationality. In addition, an explanatory model for the achieved counterfeit product detection rate is provided. This model reveals that real-life factors like lot size, co-mingling, and correlation of false negatives are important determinants behind the effectiveness of a technical countermeasure, and should be taken into account in future studies. Overall, these theoretical results contribute toward the effective use of technical anti-counterfeiting measures.

VIII.2 Practical Implications

This thesis has influenced the RFID and brand protection communities by showing that low-cost RFID such as EPC Class-1 Gen-2 can be considered an anti-counterfeiting technology. Even though TID numbers of low-cost RFID tags do not provide a long term solution for product authentication, this thesis has showed that cloned tags can be detected in a reliable way when products are traced in supply chains.

The resulting practical implication is that by applying the proposed product authentication concepts (or other ways to detect cloned tags), more expensive and energy thirsty cryptographic tags are not necessary for authenticating products inside supply chains. On the other hand, cryptographic tags are still needed to enable secure product authentication when products are no longer traced, such as after the point of sale. Moreover, the proposed product authentication concepts should still be used together with other product authentication techniques to address possible false alarms. But since the number of false alarms can be controlled with the presented data filtering technique that detects missing reads, or by using the synchronized secrets method, the proposed concepts can be understood as effective screening techniques.

This thesis has also contributed toward refinement of technical anti-counterfeiting strategies by discussing the importance of goals and metrics in security. Owing to inherent trade-offs between security and usability & performance, technical anti-counterfeiting strategies are more effective when they aim at protecting the supply chain and achieving a high counterfeit product detection rate, instead of trying to protect the product against copying and achieve a high cost to copy the security feature. Moreover, by showing how technical, organizational, and legal brand protection measures can be aligned behind the goal of protecting a supply chain against counterfeits, this work questions the ”silo-thinking” that sees these measures as distinct brand protection approaches. Last, the practical guidelines about operationalizing the proposed anti-counterfeiting measures contribute toward effective use of low-cost RFID in the fight against product counterfeiting.

VIII.3 Limitations and Possible Directions for Future Research

The proposed product authentication concepts have been studied outside specific industrial application scenarios, such as case studies. Therefore the presented evaluation is not yet a proof of industrial applicability of the concepts, but rather a proof of potential. In addition, due to a lack of empirical data on the effect of technical countermeasures on product counterfeiters, the amount of security that is needed to stop a counterfeiter—as suggested by the rational choice theory—still remains to be confirmed in practice. Other possible directions for future research include finding a reliable way to use the time information of an RFID trace to detect cloned tags and extending the economic models of security to study optimal resource allocation in technical anti-counterfeiting strategies by assigning utilities and costs to brand owner’s and counterfeiter’s actions.

References

ABI Research (2008). Global RFID Market to Reach $5.3 Billion This Year. ABI Research. http://www.abiresearch.com/ (08.07.2009).

Adelmann, R., Langheinrich, M., and Flörkemeier, C. (2006). Toolkit for Bar Code Recognition and Resolving on Camera Phones Jump Starting the Internet of Things. In *Workshop Mobile and Embedded Interactive Systems (MEIS'06) at Informatik 2006*.

Aigner, M., Plos, T., Ruhanen, A., and Coluccini, S. (2008). Secure Semi-Passive RFID Tags - Prototype and Analysis. *Deliverable D4.2.2 of the EU-BRIDGE Project, project number IST-033546*.

Akerlof, G. A. (1970). The market for lemons: Quality uncertainty and the market mechanism. *Quarterly Journal of Economics*, 84:488–500.

Alexander, I. (2003). Misuse cases: use cases with hostile intent. *IEEE Software*, 20(1):58–66.

Alhir, S. S. (2003). *Learning UML*. O'Reilly Online Books.

Alrabady, A. (2002). *Security of Passive Access Vehicle*. PhD thesis, Wayne State University, Detroit, Michigan.

Anderson, R. (1993). Why cryptosystems fail. In *ACM Conference on Computer Security 1993*, pages 215–227.

Anderson, R. (2001a). *Security Engineering: A Guide to Building Dependable Distributed Systems*. Wiley.

Anderson, R. (2001b). Why information security is hard-an economic perspective. In *7th Annual Computer Security Applications Conference, ACSAC*, pages 358–365.

Anderson, R. and Kuhn, M. (1997). Low cost attacks on tamper resistant devices. *International Workshop on Security Protocols (IWSP)*.

Anderson, R. and Moore, T. (2006). The economics of information security. *Science*, 314(5799):610–613.

Anderson, R. and Moore, T. (2007). Information security economics - and beyond. In *Advances in Cryptology - CRYPTO 2007*, volume 4622 of *Lecture Notes in Computer Science*, pages 68–91. Springer Berlin / Heidelberg.

Asanghanwa, E. (2008). Product counterfeiting made easy. and why it's so difficult to prevent. *Atmel White Pape. http://www.rsaconference.com/uploadedFiles/RSA365/Security_Topics /Deployment_Strategies/White_Papers/Atmel/doc5280.pdf (15.10.2008)*, 76(2):169–217.

Avoine, G. and Oechslin, P. (2005). A Scalable and Provably Secure Hash Based RFID Protocol. In *International Workshop on Pervasive Computing and Communication Security – PerSec 2005*, pages 110–114, Kauai Island, Hawaii, USA. IEEE, IEEE Computer Society Press.

Ayres, I. and Levitt, D. (1998). Measuring positive externalities from unobservable victim precaution: An empirical analysis of lojack. *The quarterly journal of economics*, 113(1):43–77.

Bailey, D. and Juels, A. (2006). Shoehorning Security into the EPC Standard. In De Prisco, R. and Yung, M., editors, *International Conference on Security in Communication Networks – SCN 2006*, volume 4116 of *Lecture Notes in Computer Science*, pages 303–320, Maiori, Italy. Springer-Verlag.

Barnett, R., Balachandran, G., Lazar, S., Kramer, B., Konnail, G., Rajasekhar, S., and Drobny, V. (2007). A Passive UHF RFID Transponder for EPC Gen 2 with -14dBm Sensitivity in 0.13m CMOS. *Solid-State Circuits Conference – ISSCC 2007. Digest of Technical Papers. IEEE International*, pages 582–623.

Batina, L., Guajardo, J., Kerins, T., Mentens, N., Tuyls, P., and Verbauwhede, I. (2006). An Elliptic Curve Processor Suitable for RFID-Tags. Cryptology ePrint Archive, Report 2006/227.

Becker, G. (1968). Crime and punishment: An economic approach. *The Journal of Political Economy*, 76(2):169–217.

Becker, G. (1976). *The economic approach to human behavior*. University of Chicago Press.

Bishop, M. (2003). What is computer security? *IEEE Security and Privacy Magazine*, 1(1):67–69.

Bogdanov, A. (2007). Attacks on the KeeLoq Block Cipher and Authentication Systems. In *3rd Conference on RFID Security*, volume 2007.

Boneh, D., Lynn, B., and Shacham, H. (2004). Short Signatures from the Weil Pairing. *Journal of Cryptology*, 17(4):297–319.

Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A., and Szydlo, M. (2005). Security Analysis of a Cryptographically-Enabled RFID Device. In *USENIX Security Symposium*, pages 1–16, Baltimore, Maryland, USA. USENIX.

Bovenschulte, M., Gabriel, P., Gassner, K., and Seidel, U. (2007). RFID: Prospectives for Germany - The state of radio frequency identification - based applications and their outlook in national and international markets. Federal Ministry of Economics and Technology, June 2007, Berlin. http://www.bmwi.de (08.07.2009).

BRIDGE (2007). European passive RFID Market Sizing 2007-2022. Building Radio frequency IDentification Solutions for the Global Environmen. Integrated Project funded by the European Commission. http://www.bridge-project.eu (02.11.2007).

Bringer, J. and Chabanne, H. (2008). Trusted-HB: A Low-Cost Version of HB$^+$ Secure Against Man-in-the-Middle Attacks. *IEEE Transactions on Information Theory*, 54(9):4339–4342.

Bringer, J., Chabanne, H., and Emmanuelle, D. (2006). HB^{++}: a Lightweight Authentication Protocol Secure against Some Attacks. In *IEEE International Conference on Pervasive Services, Workshop on Security, Privacy and Trust in Pervasive and Ubiquitous Computing – SecPerU 2006*, Lyon, France. IEEE, IEEE Computer Society Press.

Bush, R., Bloch, P., and Dawson, S. (1989). Remedies for product counterfeiting. *Business Horizons*, 32(1):59–65.

Buzzard, K. (1999). Computer security - what should you spend your money on. *Computer Security*, 18(4):322–334.

CACP (2006). No Trade in Fakes Supply Chain Tool Kit. The Coalition Against Counterfeiting and Piracy (CACP).

CACP (2009). Intellectual Property Protection and Enforcement Manual: A Practical and Legal Guide for Protecting Your Intellectual Property Rights. The Coalition Against Counterfeiting and Piracy (CACP).

Cameron, G. (1998). Innovation and growth: a survey of the empirical literature. (manuscript).

Camp, L. (2006). The state of economics of information security. Available http://archive.nyu.edu/fda/bitstream/2451/14987/2/Infosec_Book_Camp.pdf (2006).

Camp, L. and Wolfram, C. (2000). Pricing security. In *Proceedings of the CERT Information Survivability Workshop*, pages 31–39, Boston, MA, USA.

Carrender, C. (2009). Focus on RFID's Value, Not Tag Cost. November 2. http://www.rfidjournal.com/article/view/5339/ (10.11.09).

Cavusoglu, H., Mishra, B., and Raghunathan, S. (2004). A model for evaluating it security investments. *Communications of the ACM*, 47(7):87 – 92.

Chakraborty, G., Allred, A., A., S., and T., B. (1997). Use of negative cues to reduce demand for counterfeit products. *Advances in Consumer Research*, 24:345 – 349.

Chatmon, C., van Le, T., and Burmester, M. (2006). Secure Anonymous RFID Authentication Protocols. Technical Report TR-060112, Florida State University, Department of Computer Science, Tallahassee, Florida, USA.

Chaudhry, P. (2006). Changing levels of intellectual property rights protection for global firms: A synopsis of recent U.S. and EU trade enforcement strategies. *Business Horizons*, 49(6):463–472.

Chaudhry, P., Cordell, V., and Zimmerman, A. (2005). Modelling anti-counterfeiting strategies in response to protecting intellectual property rights in a global environment. *The Marketing Review*, 5(1):59–72.

Chaudhry, P. and Walch, M. (1996). An assessment of the impact of counterfeiting in international markets: The piracy paradox persists. *Columbia Journal of World Business*, 31(3):34–48.

Chaudhry, P., Zimmerman, A., Peters, J., and Cordell, V. (2008). Preserving intellectual property rights: Managerial insight into the escalating counterfeit market quandary. *Business Horizons*, 52(1):57–66.

Cheung, C., Cheung, C., Lee, W., and Kwok, S. (2006). An RFID enabled topology visualization system for supply chain management. *Annual Journal of IIE(HK) 2005-2006,*, 26:61–70.

Choi, E. Y., Lee, S. M., and Lee, D. H. (2005). Efficient RFID Authentication Protocol for Ubiquitous Computing Environment. In Enokido, T., Yan, L., Xiao, B., Kim, D., Dai, Y., and Yang, L., editors, *International Workshop on Security in Ubiquitous Computing Systems – SecUbiq 2005*, volume 3823 of *Lecture Notes in Computer Science*, pages 945–954, Nagasaki, Japan. Springer-Verlag.

Collins, J. (2004). DOD Updates RFID Policy. RFID Journal, April 1. http://www.rfidjournal.com/article/articleprint/856/-1/1/ (08.07.2009).

Cook, C., Vogt, H., Muller, J., Dada, A., Pfletschinger, M., Ortel, N., Molan, M., Naraks, A., and Gourmanel, F. (2008). Report on integration of smart/intelligent tags in products. Deliverable D4.3 of the SToP project.

Courtois, N. T., Nohl, K., and O'Neil, S. (2008). Algebraic Attacks on the Crypto-1 Stream Cipher in MiFare Classic and Oyster Cards. Cryptology ePrint Archive, Report 2008/166.

Danev, B., Heydt-Benjamin, T. S., and Capkun, S. (2009). Physical-layer Identification of RFID Devices. In *Proceedings of the 18th USENIX Security Symposium – USENIX'09*, Montreal, Canada.

Department of Justice (2006). Pharmaceutical Distributor Pleads Guilty to Selling Counterfeit Drugs. US Department of Justice, October. http://www.usdoj.gov/criminal/cybercrime/albersPlea.htm (09.08.09).

Derakhshan, R., Orlowska, M., and Li, X. (2007). RFID data management: Challenges and opportunities. In *IEEE International Conference on RFID*, pages 26–28, Grapevine, Texas, USA.

Devadas, S., Suh, E., Paral, S., Sowell, R., Ziola, T., and Khandelwal, V. (2008). Design and Implementation of PUF-Based ”Unclonable” RFID ICs for Anti-Counterfeiting and Security Applications. *IEEE International Conference on RFID*, pages 58–64.

Dimitriou, T. (2005). A Lightweight RFID Protocol to protect against Traceability and Cloning attacks. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*, Athens, Greece. IEEE.

Dimitriou, T. (2006). A Secure and Efficient RFID Protocol that could make Big Brother (partially) Obsolete. In *International Conference on Pervasive Computing and Communications PerCom 2006*, Pisa, Italy. IEEE Computer Society Press.

Dominikus, S., Oswald, E., and Feldhofer, M. (2005). Symmetric Authentication for RFID Systems in Practice. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto.

Duc, D. N., Park, J., Lee, H., and Kim, K. (2006). Enhancing Security of EPCglobal Gen-2 RFID Tag against Traceability and Cloning. In *Symposium on Cryptography and Information Security*, Hiroshima, Japan.

Eisenbarth, T., Kumar, S., Paar, C., Poschmann, A., and Uhsadel, L. (2007). A Survey of Lightweight-Cryptography Implementations. *IEEE Design and Test of Computers*, 24(6):522–533.

Engberg, S., Harning, M., and Damsgaard Jensen, C. (2004). Zero-knowledge Device Authentication: Privacy & Security Enhanced RFID preserving Business Value and Consumer Convenience. In *Conference on Privacy, Security and Trust – PST*, New Brunswick, Canada.

Engels, D. (2005). On Ghost Reads in RFID Systems. Auto-ID Labs Whitepaper SWNET-010. http://www.autoidlabs.org.

EPCglobal Inc. (2005a). Class-1 Generation-2 UHF RFID Conformance Requirements Specification v. 1.0.2. Ratified Standard.

EPCglobal Inc. (2005b). Class-1 Generation-2 UHF RFID Protocol for Communcation at 860 MHZ - 960 MHz. Version 1.1.0. Ratified Standard.

EPCglobal Inc. (2006). EPCglobal Tag Data Standards Version 1.4. EPCglobal Ratified Standard, June 2008. http://www.epcglobalinc.org/standards/tds/tds_1_4-standard-20080611.pdf (14.07.2009).

EPCglobal Inc. (2007). EPCIS 1.0.1 Specification. Ratified Standard. http://www.epcglobalinc.org/standards/epcis/epcis_1_0_1-standard-20070921.pdf (15.8.08).

EPCglobal Inc. (2008). Pedigree Standard v. 1.0. Ratified Standard.

EPCglobal Inc. (2009a). EPCglobal Architecture Framework Final Version 1.3. Ratified Standard. http://www.epcglobalinc.org/standards/architecture/architecture_1_3-framework-20090319.pdf (14.07.09).

EPCglobal Inc. (2009b). Regulatory status for using RFID in the UHF spectrum. http://www.epcglobalinc.org/tech/freq_reg/RFID_at_UHF_Regulations_20090318.pdf (10.11.2009).

ETSI (2008). Radio Frequency Identification Equipment operating in the band 865 MHz to 868 MHz with power levels up to 2 W. European Telecommunications Standards Institute (ETSI) document EN 302 208-1 Ver. 1.2.1.

European Commission (2003). Regulation (EC) no. 1383/2003. Official Journal of the European Union, 2.8.2003, L 196/7.

FDA (2003a). FDA's Continuing Investigation Implicates Additional Lots of Counterfeit Lipitor. Food and Drug Administration, June. http://www.fda.gov/bbs/topics/ANSWERS/2003/ANS01227.html (01.03.09).

FDA (2003b). Update: FDA Investigation Into Counterfeit Lipitor, Two Distributors Recalling All Lipitor Repacked by MED-PRO. Food and Drug Administration, June. http://www.fda.gov/bbs/topics/ANSWERS/2003/ANS01229.html (01.03.09).

Feldhofer, M. (2003). A Proposal for Authentication Protocol in a Security Layer for RFID Smart Tags.

Feldhofer, M. (2008). *Low-Power Hardware Design of Cryptographic Algorithms for RFID Tags*. PhD thesis, University of Graz, Austria.

Feldhofer, M., Dominikus, S., and Wolkerstorfer, J. (2004). Strong Authentication for RFID Systems using the AES Algorithm. In Joye, M. and Quisquater, J.-J., editors, *Workshop on Cryptographic Hardware and Embedded Systems – CHES 2004*, volume 3156 of *Lecture Notes in Computer Science*, pages 357–370, Boston, Massachusetts, USA. IACR, Springer-Verlag.

Feldhofer, M., Wolkerstorfer, J., and Rijmen, V. (2005). AES Implementation on a Grain of Sand. *IEE Proceedings - Information Security*, 152(1):13–20.

Finkenzeller, K. (2006). *RFID-Handbuch - Grundlagen und praktische Anwendungen induktiver Funkanlagen, Transponder und kontaktloser Chipkarten*. Carl Hanser, München.

Finne, T. (1998). A conceptual framework for information security management. *Computer Security*, 17(4):303–307.

FIPS (1979). Guidelines for automatic data processing risk analysis. Federal Information Processing Standards (FIPS) Publication 65.

Fleisch, E. and Mattern, F. (2005). *Das Internet der Dinge. Ubiquitous Computing und RFID in Der Praxis: Visionen, Technologien, Anwendungen, Handlungsanleitungen*. Springer-Verlag, Berlin.

Fleisch, E. and Tellkamp, C. (2006). The Business Value of Ubiquitous Computing Technologies . In Roussos, G., editor, *Ubiquitous and Pervasive Commerce, New Frontiers for Electronic Business*, pages 93–113. Springer London.

Folcke, G. (2008). Tracabilite des implants medicaux en milieu hospitalier (in French). Revue de l'Eléctricité et de l'Eléctronique (REE), Société Intérnationale des Eléctriciens.

Främling, K., Tossavainen, T., and van Blommestein, F. (2007). Comparison of the ID@URI (TraSer) approach with other systems. *TraSer-Project White Paper*.

Frumkin, D. and Shamir, A. (2009). Un-Trusted-HB: Security Vulnerabilities of Trusted-HB. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium.

Gao, X. G., Xiang, Z. A., Wang, H., Shen, J., Huang, J., and Song, S. (2005). An Approach to Security and Privacy of RFID System for Supply Chain. In *Conference on E-Commerce Technology for Dynamic E-Business – CEC-East'04*, pages 164–168, Beijing, China. IEEE, IEEE Computer Society.

Gaukler, G., Seifert, R., and Hausman, W. (2007). Item-Level RFID in the Retail Supply Chain. *roduction and Operations Management*, 16(1):6576.

Geer, D. (2005). Making choices to show ROI. *Secure Business Quarterly*, 1(2):15.

Geer, D., Hoo, K., and Jaquith, A. (2003). Information security: why the future belongs to the quants. *IEEE Security & Privacy*, 1(4):24 – 32.

Gilbert, H., Robshaw, M., and Sibert, H. (2005). An Active Attack Against HB$^+$ – A provably Secure Lightweight Authentication Protocol. Manuscript.

Gordon, L. and Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438 – 457.

Gordon, L. and Loeb, M. (2006). Budgeting Process for Information Security Expenditures. *Communications of the ACM*, 49(1):121–125.

Grand, K. (1998). MAC address cloning. *http://www.netsourceasia.net/resources/mac_address_cloning.pdf (5.12.2008).*

Green, R. and Smith, T. (2002). Executive Insights: Countering Brand Counterfeiters. *Journal of International Marketing*, 10(4):89–lO6.

Grossman, G. M. and Shapiro, C. (1988a). Counterfeit-product trade. *American Economic Review*, 78(1):59–75.

Grossman, G. M. and Shapiro, C. (1988b). Foreign counterfeiting of status goods. *Quarterly Journal of Economics*, 103(1):79–100.

Grummt, E. and Ackermann, R. (2008). Proof of Possession: Using RFID for large-scale Authorization Management. In Mühlhäuser, M., Ferscha, A., and Aitenbichler, E., editors, *Constructing Ambient Intelligence, AmI-07 Workshops Proceedings*, Communications in Computer and Information Science, pages 174–182.

GS1 Germany (2006). Fälschungssicherheit per EPC: Management-Information. March. http://www.gs1-germany.de/internet/common/downloads/epc_rfid/3027_faelschungssicherheit.pdf (09.09.2009).

Guajardo, J., Škorić, B., Tuyls, P., Kumar, S. S., Bel, T., Blom, A. H., and Schrijen, G.-J. (2009). Anti-counterfeiting, key distribution, and key storage in an ambient world via physical unclonable functions. *Information Systems Frontiers*, 11(1):19–41.

Hardgrave, B. and Patton, J. (2008). RFID as electronic article surveillance EAS: feasibility assessment. Information Technology Research Institute Working Paper ITRI-WP117-0808. http://itrc.uark.edu/ (25.08.08).

Harper, J., Morris, J., Satchwell, G., Stevens, P., Taylor, D., and Tremblay, M. (2006). *Coincidence or Crisis? Prescription medicine counterfeiting*. The Stockholm Network in association with Profile Books Ltd, London.

Harvey, M. (1988). A new way to combat product counterfeiting. *Business Horizons*, 31(4):19–28.

Harvey, M. G. and Ronkainen, I. A. (1985). International counterfeiters: marketing success without the cost and the risk. *Columbia Journal of World Business*, 20(3):37–45.

Haythornthwaite, R., Nxumalo, J., and Phaneuf, M. (2004). Use of the focused ion beam to locate failure sites within electrically erasable read only memory microcircuits. *J. Vac. Sci. Technol.*, 22(3).

Hein, D., Wolkerstorfer, J., and Felber, N. (2008). ECC is Ready for RFID - A Proof in Silicon. In *Conference on RFID Security*, Budaperst, Hongria.

Henrici, D. and Müller, P. (2004). Hash-Based Enhancement of Location Privacy for Radio-Frequency Identification Devices Using Varying Identifiers. In Sandhu, R. and Thomas, R., editors, *International Workshop on Pervasive Computing and Communication Security – PerSec 2004*, pages 149–153, Orlando, Florida, USA. IEEE, IEEE Computer Society.

Hevner, A., March, S., and Park, J. (1997). Design science in information systems research. *Management Information Systems (MIS) Quarterly*, 28(1):75–106.

Holton, G. (2004). Defining Risk. *Financial Analysts Journal*, 60:1925.

Hoo, K. (2000). How much is enough? A risk-management approach to computer security. *Consortium for Research on Information Security Policy (CRISP) Working Paper. Stanford University, Stanford, Calif.*

Hopkins, D., Kontnik, L., and Turnage, M. (2003). *Counterfeiting Exposed: Protecting Your Brand and Customers*. Wiley, 1 edition, New Jersey.

Hopper, N. and Blum, M. (2000). A Secure Human-Computer Authentication Scheme. Technical Report CMU-CS-00-139, Florida State University, Department of Computer Science, Carnegie Mellon University.

Hung, C. (2003). The Business of Product Counterfeiting in China and the Post-WTO Membership Environment. *Asia Pacific Business Review*, 10(1):58–77.

Hunt, D., Puglia, A., and Puglia, M. (2007). *RFID - A Guide to Radio Frequency Identification*. Wiley-Interscience.

IDTechEx (2009a). RFID - a surge in orders. IDTechEx report, June 23. http://www.idtechex.com (09.09.2009).

IDTechEx (2009b). RFID Forecasts, Players and Opportunities 2009-2019. IDTechEx report. http://www.idtechex.com (08.07.2009).

Ilic, A., Michahelles, F., and Fleisch, E. (2007). The Dual Ownership Model: Using Organizational Relationships for Access Control in Safety Supply Chains. In *21st International Conference on Advanced Information Networking and Applications Workshops, 2007, AINAW '07.*, volume 2, pages 459–466.

International Civil Aviation Organization (2006a). Machine Readable Travel Documents, Part 1 Volume 1. ICAO Document 9303.

International Civil Aviation Organization (2006b). Machine Readable Travel Documents, Part 1 Volume 2. ICAO Document 9303.

ISO (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) Standard ISO/IEC 27000:2009.

Jacobs, L., Samli, A., and Jedik, T. (2001). The Nightmare of International Product Piracy - Exploring Defensive Strategies. *Industrial Marketing Management*, 30(6):499–509.

Jeffery, S., Garofalakis, M., and Franklin, M. (2006). Adaptive cleaning for RFID data streams. In *32nd International Conference on Very Large Databases (VLDB)*, pages 163–174, Korea.

John Jenkins Associates (2008). Pharma Traceability Pilot – Requirements Analysis. Deliverable D6.2 of EU-BRIDGE Project. http://www.bridge-project.eu/data/File/BRIDGE%20WP06%20Pharma%20 Traceability%20Requirements%20Analysis.pdf (15.09.2008).

Johnston, R. G. (2005). An Anticounterfeiting Strategy Using Numeric Tokens. *International Journal of Pharmaceutical Medicine*, 19(3):163–171.

Jones, P., Clarke-Hill, C., Hillier, D., and Comfort, D. (2005). The benefits, challenges and impacts of radio frequency identification technology (rfid) for retailers in the uk. *Marketing Intelligence & Planning*, 23(4):395–402.

Juels, A. (2004). Minimalist Cryptography for Low-Cost RFID Tags. In Blundo, C. and Cimato, S., editors, *International Conference on Security in Communication Networks – SCN 2004*, volume 3352 of *Lecture Notes in Computer Science*, pages 149–164, Amalfi, Italia. Springer-Verlag.

Juels, A. (2005). Strengthening EPC Tags Against Cloning. Manuscript.

Juels, A. (2006). RFID Security and Privacy: A Research Survey. *IEEE Journal on Selected Areas in Communications*, 24(2):381–394.

Juels, A., Molnar, D., and Wagner, D. (2005). Security and Privacy Issues in E-passports. In *Conference on Security and Privacy for Emerging Areas in Communication Networks – SecureComm*, Athens, Greece. IEEE.

Juels, A. and Pappu, R. (2003). Squealing Euros: Privacy Protection in RFID-Enabled Banknotes. In Wright, R. N., editor, *Financial Cryptography – FC'03*, volume 2742 of *Lecture Notes in Computer Science*, pages 103–121, Le Gosier, Guadeloupe, French West Indies. IFCA, Springer-Verlag.

Juels, A. and Weis, S. (2005). Authenticating Pervasive Devices with Human Protocols. In Shoup, V., editor, *Advances in Cryptology – CRYPTO'05*, volume 3126 of *Lecture Notes in Computer Science*, pages 293–308, Santa Barbara, California, U.S. IACR, Springer-Verlag.

Kahneman, D. (2003). Maps of Bounded Rationality: Psychology for Behavioral Economics. *American economic review*, 93(5):1449–1475.

Kaikati, J. G. and LaGarce, R. (1980). Beware of international brand piracy. *Harvard Business Review*, 58(2):52–58.

Kansas City Business Journal (2005). Floridian admits selling counterfeit Lipitor to KC company. January 21. http://www.bizjournals.com/kansascity/stories/2005/01/17/daily42.html (09.07.09).

Kärkkäinen, M. (2003). Increasing efficiency in the supply chain for short shelf life goods using RFID tagging. *International Journal of Retail & Distribution Management*, 31(10):529–536.

Kasper, T., Oswald, D., and Paar, C. (2009). New Methods for Cost-Effective Side-Channel Attacks on Cryptographic RFIDs. In *Workshop on RFID Security – RFIDSec'09*, Leuven, Belgium.

Katz, J. and Smith, A. (2006). Analyzing the HB and HB+ Protocols in the "Large Error" Case. Cryptology ePrint Archive, Report 2006/326.

Katz, J. and Sun Shin, J. (2006). Parallel and Concurrent Security of the HB and HB$^+$ Protocols. In Vaudenay, S., editor, *Advances in Cryptology – EUROCRYPT'06*, Lecture Notes in Computer Science, Saint Petersburg, Russia. IACR, Springer-Verlag.

Kfir, Z. and Wool, A. (2005). Picking virtual pockets using relay attacks on contactless smartcard systems. In *First International Conference on Security and Privacy for Emerging Areas in Communications Networks, SECURECOMM)*, pages 47–58.

Koblitz, N. (1987). Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177):203–209.

Koh, R., Schuster, E., Chackrabarti, I., and Bellman, A. (2003). Securing the Pharmaceutical Supply Chain. *Auto-ID Labs White Paper, Massachusetts Institute of Technology*.

Kömmerling, O. and Kuhn, M. (1999). Design Principles for Tamper-Resistant Smartcard Processors. In *USENIX Workshop on Smartcard Technology – Smartcard '99*, pages 9–20. USENIX Association.

Koscher, K., Juels, A., Kohno, T., and Brajkovic, V. (2008). EPC RFID Tags in Security Applications: Passport Cards, Enhanced Drivers Licenses, and Beyond. Manuscript.

Kumar, S. and Paar, C. (2006). Are Standards Compliant Elliptic Curve Cryptosystems Feasible on RFID? In *Workshop on RFID Security – RFIDSec'06*, Graz, Austria. Ecrypt.

Kunreuther, H. and Heal, G. (2003). Interdependent Security. *Journal of Risk and Uncertainty*, 26(2-3):231–249.

Kurose, F. and Ross, K. (2003). *Computer Networking - A Top-Down Approach Featuring the Internet*. Addison-Wesley, 2nd edition.

Lampe, M., Flörkemeier, C., and Haller, S. (2005). Einführung in die RFID-Technologie. In Fleisch, E. and Mattern, F., editors, *Das Internet der Dinge - Ubiquitous Computing und RFID in der Praxis*, pages 69–86. Berlin: Springer.

Lee, J., Lim, D., Gassend, B., Suh, G., Dijk, M., and Devadas, S. (2004). A Technique to Build a Secret Key in Integrated Circuits for Identification and Authentication Applications. In *Symposium on VLSI Circuits*, pages 176–179.

Lee, S., Asano, T., and Kim, K. (2006). RFID Mutual Authentication Scheme based on Synchronized Secret Information. In *Symposium on Cryptography and Information Security*, Hiroshima, Japan.

Lee, S.-M., Hwang, Y. J., Lee, D. H., and Lim, J. I. L. (2005). Efficient Authentication for Low-Cost RFID Systems. In Gervasi, O., Gavrilova, M., Kumar, V., Laganaà, A., Lee, H. P., Mun, Y., Taniar, D., and Tan, C. J. K., editors, *International Conference on Computational Science and its Applications - ICCSA 2005, Proceedings, Part I*, volume 3480 of *Lecture Notes in Computer Science*, pages 619–627, Singapore, Republic of Singapore. Springer-Verlag.

Lehtonen, M., Bogataj, K., Klopcic, Z., and Magerkurth, C. (2008). escription of the status quo of existing technical countermeasures, their benefits and shortcomings. *Deliverable D1.3 of the EU-SToP Project, project number IST-034144*.

Lehtonen, M., Boos, D., von Reischach, F., Magerkurth, C., Müller, J., Bogataj, K., Gout, E., Gourmanel, F., Ippisch, T., Oertel, N., and Dada, A. (2009a). Final evaluation of project results accordingly to the identified requirements. *Deliverable D5.4 of the EU-SToP Project, project number IST-034144*.

Lehtonen, M., Michahelles, F., and Fleisch, E. (2007). Probabilistic Approach for Location-Based Authentication. In Bajart, A., Muller, H., and Strang, T., editors, *1st International Workshop on Security for Spontaneous Interaction – IWSSI 07. UbiComp 2007 Workshops Proceedings*, pages 486–491, Innsbruck, Austria.

Lehtonen, M., Michahelles, F., and Fleisch, E. (2009b). How to Detect Cloned Tags in a Reliable Way from Incomplete RFID Traces. In *3rd IEEE International Conference on RFID – IEEE RFID 09*, pages 257 – 264, Orlando, Florida.

Lehtonen, M., Ostojic, D., Ilic, A., and Michahelles, F. (2009c). Securing RFID Systems by Detecting Tag Cloning. In Tokuda, H., Beigl, M., Friday, A., Brush, A., and Tobe, Y., editors, *7th International Conference on Pervasive Computing – Pervasive09*, volume 5538 of *Lecture Notes in Computer Science*, page 291308. Springer-Verlag Berlin Heidelberg.

Lehtonen, M., Ruhanen, A., Michahelles, F., and Fleisch, E. (2009d). Serialized TID Numbers - A Headache or a Blessing for RFID Crackers? In *3rd IEEE International Conference on RFID – IEEE RFID 09*, pages 233–240, Orlando, Florida.

Lei, P., Claret-Tournier, F., Chatwin, C., and Young, R. (2005). A Secure Mobile Track and Trace System for Anti-Counterfeiting. In *EEE '05: Proceedings of the 2005 IEEE International Conference on e-Technology, e-Commerce and e-Service (EEE'05) on e-Technology, e-Commerce and e-Service*, pages 686–689, Washington, DC, USA. IEEE Computer Society.

Leimeister, J., Knebel, U., and Krcmar, H. (2007). RFID as Enabler for the boundless real-time Organisation: Empirical Insights from Germany. *International Journal of Networking and Virtual Organisations*, 3(1):45–64.

Leng, X., Mayes, K., and Markantonakis, K. (2008). HB-MP+ Protocol: An Improvement on the HB-MP Protocol. *IEEE International Conference on RFID*, pages 118–124.

Longstaff, T., Chittister, C., Pethia, R., and Haimes, Y. (2000). Are we forgetting the risk of information technology? *IEEE Computer*, 33(12):43–51.

Lord Kelvin (1883). Electrical units of measurement. *Popular Lectures and Addresses (PLA)*, 1.

Magerkurth, C., Dada, A., Müller, J., Oertel, N., Vogt, H., Gout, E., and Molan, M. (2008). Integrated Real-World Operational Trials (Prototype). *Deliverable D5.3 of the EU-SToP Project (Restricted), project number IST-034144.*

Mattern, F. (2002). Vom Handy zum allgegenwärtigen Computer: Szenarien einer informatisierten Welt. *Analysen der Friedrich-Ebert-Stiftung zur Informationsgesellschaft. http://library.fes.de/fulltext/stabsabteilung/01183.htm (13.07.09).*

Mattern, F. (2005). Ubiquitous computing: Scenarios from an informatised world. In Zerdick, A., Picot, A., Schrape, K., Burgelman, J., Silverstone, R., Feldmann, V., Wernick, C., and Wolff, C., editors, *E-Merging Media - Communication and the Media Economy of the Future*, pages 145–163. Springer.

Miller, V. (1986). Use of elliptic curves in cryptography. In Williams, H., editor, *Advances in Cryptography – CRYPTO'85*, volume 218 of *Lecture Notes in Computer Science*, pages 417–426. Springer-Verlag Berlin Heidelberg.

Mirowski, L. and Hartnett, J. (2007). Deckard: A System to Detect Change of RFID Tag Ownership. *International Journal of Computer Science and Network Security*, 7(7):89–98.

Mirowski, L., Hartnett, J., Williams, R., and Gray, T. (2008). A RFID Proximity Card Data Set. Technical Report of University of Tasmania. http://eprints.utas.edu.au/6903/1/a_rfid_proximity_card_data_set.pdf. (3.3.2009).

Mitsugi, J. (2006). Multipurpose sensor RFID tag. *APMC 2006 workshop on Emerging Technologies and Applications of RFID – WS04-4*, pages 143–148.

Molnar, D., Soppera, A., and Wagner, D. (2005). A Scalable, Delegatable Pseudonym Protocol Enabling Ownership Transfer of RFID Tags. In Preneel, B. and Tavares, S., editors, *Selected Areas in Cryptography – SAC 2005*, volume 3897 of *Lecture Notes in Computer Science*, pages 276–290, Kingston, Canada. Springer-Verlag.

Molnar, D. and Wagner, D. (2004). Privacy and Security in Library RFID: Issues, Practices, and Architectures. In Pfitzmann, B. and Liu, P., editors, *Conference on Computer and Communications Security – ACM CCS*, pages 210–219, Washington, DC, USA. ACM, ACM Press.

Müller, B. (2009). Alles Im Netz. *Spektrum der Wissenschaft (in German)*, Juni:92–95.

Naccache, D. and Stern, J. (2001). Signing on a Postcard. In Frankel, Y., editor, *Financial Cryptography*, volume 1962 of *Lecture Notes in Computer Science*, pages 121–135. Springer-Verlag.

Nochta, Z., Staake, T., and Fleisch, E. (2006). Product Specific Security Features Based on RFID Technology. In *Saint-Workshop, International Symposium on Applications and the Internet Workshops (SAINTW'06)*, pages 72–75.

Odlyzko, A. (2003). Economics, Psychology, and Sociology of Security. In *Financial Cryptography*, volume 2742 of *Lecture Notes in Computer Science*, pages 182–189. Springer Berlin / Heidelberg.

OECD (1998). The Economic Impact of Counterfeiting. *Organization for Economic Cooperation and Development (OECD).*

OECD (2007). Counting the Cost: The Economic Impact of Counterfeiting and Piracy. *Preliminary Findings of the OECD Study presented at Third Global Congress on Combating Counterfeiting and Piracy, 30-31 January 2007, International Conference Center, Geneva.*

Ohkubo, M., Suzuki, K., and Kinoshita, S. (2003). Cryptographic Approach to "Privacy-Friendly" Tags. In *RFID Privacy Workshop*, MIT, Massachusetts, USA.

Olsen, J. and Granzin, K. (1992). Gaining retailers' assistance in fighting counterfeiting: Conceptualization and empirical test for a helping model. *Journal of Retailing*, 68(1):90–109.

Olsen, J. and Granzin, K. (1993). Using channels constructs to explain dealers' willingness to help manufacturers combat counterfeiting. *Journal of Business Research*, 27(2):147–170.

Park, W. G. and Ginarte, J. C. (1997). Intellectual Property Rights and Economic Growth. *Contemporary Economic Policy*, 15(3):51–61.

Pearson, J. (2005). Securing the Pharmaceutical Supply Chain with RFID and Public-key Infrastructure (PKI) Technologies. *Texas Instruments White Paper. http://www.ti.com/rfid/docs/manuals/whtPapers/wp-RFID_and_PKI.pdf (4.2.2009)*, 5310(176).

Pfizer (2007). Case Study: Lipitor US Recall. http://media.pfizer.com/files/products/Lipitor USRecall.pdf (09.07.09)).

Picard, J. (2001). Copy Detectable Images: From Theory to Practice. In *NIP24: International Conference on Digital Printing Technologies and Digital Fabrication 2008*, pages 796–798, Pittsburgh, Pennsylvania.

Picard, J. (2004). Digital authentication with copy-detection patterns. *Optical Security and Counterfeit Deterrence Techniques V, edited by Rudolf L. van Renesse, Proceedings of SPIE 2004*, 5310(176).

Pintsov, L. and Vanstone, S. (2001). Postal Revenue Collection in the Digital Age . In Frankel, Y., editor, *Financial Cryptography*, volume 1962 of *Lecture Notes in Computer Science*, pages 105–120, Heidelberg. Springer-Berlin.

Piramuthu, S. (2006). HB and Related Lightweight Authentication Protocols for Secure RFID Tag/Reader Authentication. In *Collaborative Electronic Commerce Technology and Research – CollECTeR 2006*, Basel, Switzerland.

Poll, E. (2007). Smartcard attacks: invasive attacks. *http://www.cs.ru.nl/ẽrikpoll/hw/slides/smartcards_invasive_attacks.pdf (5.12.2008).*

Purefoy, C. (2008). Poisoned medicine kills dozens of children in Nigeria. CNN, December 18. http://edition.cnn.com/2008/WORLD/africa/12/18/nigeria.poison.drugs/ (28.08.2009).

Ranasinghe, D., Engels, D., and Cole, P. (2004). Security and Privacy: Modest Proposals for Low-Cost RFID Systems. In *Auto-ID Labs Research Workshop*, Zurich, Switzerland.

RFID Journal (2003). Wal-Mart Expands RFID Mandate. RFID Journal, August 18. http://www.rfidjournal.com/article/view/539/1/1 (08.07.2009).

RFID Ready (2009). SecureRF wins support from National Science Foundation. RFID Ready, August 26. http://www.rfid-ready.com/ (03.09.2009).

Rhee, K., Kwak, J., Kim, S., and Won, D. (2005). Challenge-Response based RFID Authentication Protocol for Distributed Database Environment. In Hutter, D. and Ullmann, M., editors, *International Conference on Security in Pervasive Computing – SPC 2005*, volume 3450 of *Lecture Notes in Computer Science*, pages 70–84, Boppard, Germany. Springer-Verlag.

Rivest, R., Shamir, A., and Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, 21(2):120126.

Roberti, M. (2005). The Price of EPC Gen 2. RFID Journal. http://www.rfidjournal.com/article/articleview/1609/1/2/ (5.12.2008).

Salmans, S. (1979). Locking Out the Product Poachers. *International Management*, 34:14–19.

Sandhu, R. (2003). Good-Enough Security: Toward a Pragmatic Business-Driven Discipline. *IEEE Internet Computing*, 7(1):66–68.

Sandvos, J. and Alton, K. (1996). Write-once read-many memory using EEPROM cells. United States Patent 5553019. http://www.freepatentsonline.com/5553019.html (15.10.2008).

Scalet, S. (2007). The 5 Myths of RFID. Chief Security Officer Magazine, May 15. http://www.csoonline.com/article/221197 (09.09.2009).

Schechter, S. E. (2002). Quantitatively differentiating system security. In *The First Workshop on Economics and Information Security*.

Schechter, S. E. (2004). Toward Econometric Models of the Security Risk from Remote Attacks. In *The Third Workshop on Economics and Information Security*.

Schechter, S. E. (2005). Toward Econometric Models of the Security Risk from Remote Attack. *IEEE Security and Privacy*, 3(1):40–44.

Schechter, S. E. and Smith, M. D. (2003). How Much Security Is Enough to Stop a Thief? *Lecture Notes in Computer Science*, 2742:122–137.

Schmitt, P. (2008). *Adoption und Diffusion neuer Technologien am Beispiel der Radiofrequenz-Identifikation (RFID)*. PhD thesis, ETH Zürich, Switzerland. Dissertation no. 18064.

Schneier, B. (1996). *Applied Cryptography*. John Wiley & Sons, 2nd edition, New York.

Schneier, B. (2000). Computer Security: Will We Ever Learn? *Crypto-Gram Newsletter, May 15, 2000*.

Schneier, B. (2003). *Beyond Fear. Thinking Sensibly about Security in an Uncertain World*. Copernicus Books, Springer-Verlag New York Inc.

Schneier, B. (2007). A Security Market for Lemons. Schneier on Security. http://www.schneier.com/blog/archives/2007/04/a_security_mark.html.

SecureRF Corporation (2007). LIME Tag. http://www.securerf.com/pdf/ SecureRF_LIME_Tag_product_sheet.pdf (15.10.2008).

Shapiro, C. and Varian, H. (1998). *Information Rules*. Harvard Business School Press.

Shultz, C. and Saporito, B. (1996). Protecting intellectual property: Strategies and recommendations to deter counterfeiting and brand piracy in global markets. *Columbia Journal of World Business*, 31(1):18–28.

Simon, H. (1955). A behavioral model of rational choice. *The Quarterly Journal of Economics*, 69(1):99–118.

Sindre, G. and Opdahl, A. L. (2005). Eliciting security requirements with misuse cases. *Requirements Engineering*, 10(1):34–44.

Soppera, A., Burbridge, T., and Broekhuizen, V. (2007). A Trusted RFID Reader for Multi-Party Services. EU RFID Convocation.

Staake, T. (2007). *Counterfeit Trade - Economics and Countermeasures*. PhD thesis, University of St. Gallen. Dissertation no. 3362.

Staake, T. and Fleisch, E. (2008). *Countering Counterfeit Trade – Illicit Market Insights, Best-Practice Strategies, and Management Toolbox*. Springer-Verlag, Berlin Heidelberg.

Staake, T., Thiesse, F., and Fleisch, E. (2005). Extending the EPC Network - The Potential of RFID in Anti-Counterfeiting. In *ACM symposium on Applied computing*, pages 1607 – 1612.

Staake, T., Thiesse, F., and Fleisch, E. (2009). The Emergence of Counterfeit Products in the Supply Chain: A Literature Review. *European Journal of Marketing*, 43(3/4):320–349.

Strassner, M. (2005). *RFID Im Supply Chain Management*. PhD thesis, University of St. Gallen, Switzerland. Dissertation no. 3112.

Takaragi, K., Usami, M., Imura, R., Itsuki, R., and Satoh, T. (2001). An ultra small individual recognition security chip. *IEEE Micro*, 21(6):43–49.

Taxation and Customs Union (2008). Results at the European border - 2007. Report on community activities on counterfeiting and piracy.

Taylor, P. (2009). EU 'could make brand owners liable for fakes'. 6. August, Securing-Pharma.com (08.26.09).

Tellkamp, C. (2006). *The impact of Auto-ID technology on process performance - RFID in the FMCG supply chain*. PhD thesis, University of St. Gallen, Switzerland. Dissertation no. 3182.

Texas Instruments (2001). The gap tests texas instruments rfid smart label technology for tracking denim clothing from the factory to store shelves. Texas Instruments Press Release, November 13. http://www.ti.com/rfid/docs/news/news_releases/2001/rel11-13-01.shtml (08.07.09).

Tsudik, G. (2006). YA-TRAP: Yet Another Trivial RFID Authentication Protocol. In *International Conference on Pervasive Computing and Communications – PerCom 2006*, Pisa, Italy. IEEE, IEEE Computer Society Press.

Tuyls, P. and Batina, L. (2006). RFID-Tags for Anti-Counterfeiting. In Pointcheval, D., editor, *Topics in Cryptology - CT-RSA 2006, The Cryptographers' Track at the RSA Conference 2006*, Lecture Notes in Computer Science, pages 115–131, San Jose, California, USA. Springer-Verlag.

United States Attorney (2007). Then Charged in $200 Million Smuggling Operation into the Port of Newark. United States Attorney Southern District of New York. http://www.usdoj.gov/criminal/cybercrime/chuCharge2.pdf.

United States Department of Homeland Security (2008). Privacy impact assessment for the use of radio frequency identification (RFID) technology for border crossings. http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_cbp_rfid.pdf.

Vajda, I. and Buttyán, L. (2003). Lightweight Authentication Protocols for Low-Cost RFID Tags. In *Second Workshop on Security in Ubiquitous Computing – Ubicomp 2003*, Seattle, WA, USA.

van Beek, J. (2008). ePassports reloaded. https://www.blackhat.com/presentations/bh-usa-08/van_Beek/bh_us_08_van_Beek_ePassports_Reloaded_Slides.pdf (09.11.2009).

Varian, H. (2000). Managing online security risks. *Economic Science Column, The New York Times*.

Varian, H. (2003). System reliability and free riding. In Sadeh, N., editor, *Fifth International Conference on Electronic Commerce – ICEC2003*, page 355366. ACM Press.

von Reischach, F., Michahelles, F., and Fleisch, E. (2007). Anti-Counterfeiting 2.0 - A Consumer-Driven Approach towards Product Authentication. In *Late Breaking Results at the 9th International Conference on Ubiquitous Computing (UbiComp 2007)*, Austria.

Weingart, S. (2000). Physical security devices for computer subsystems: A survey of attacks and defenses. In *Workshop on Cryptographic Hardware and Embedded Systems*, pages 302–317.

Weis, S., Sarma, S., Rivest, R., and Engels, D. (2003). Security and Privacy Aspects of Low-Cost Radio Frequency Identification Systems. In Hutter, D., Müller, G., Stephan, W., and Ullmann, M., editors, *International Conference on Security in Pervasive Computing – SPC 2003*, volume 2802 of *Lecture Notes in Computer Science*, pages 454–469, Boppard, Germany. Springer-Verlag.

Westhues, J. (2005). *RFID: Applications, Security, and Privacy*. Addison-Wesley, New York.

Wiechert, T., Thiesse, F., Michahelles, F., Schmitt, P., and Fleisch, E. (2007). Connecting Mobile Phones to the Internet of Things: A Discussion of Compatibility Issues between EPC and NFC. In *Americas Conference on Information Systems, AMCIS*.

Williams, B. (2008). What is the Real Business Case for the 'Internet of Things'? Synthesis Journal, iTSC.

WIPO (2004). Understanding Industrial Property. World Intellectual Property Organization. http://www.wipo.int/freepublications/en/intproperty/895/wipo_pub_895.pdf (09.07.09).

WIPO (2009). The Museum of Counterfeiting, Paris - A Walk on the Wild Side. World Intellectual Property Organization, February. http://www.wipo.int/wipo_magazine/en/2009/01/article_0009.html (09.07.09).

Witteman, M. (2005). Attacks on digital passports. July 28, 2005, WhatTheHack. http://wiki.whatthehack.org/images/2/28/WTH-slides-Attacks-on-Digital-Passports-Marc-Witteman.pdf (09.11.09).

Wolkerstorfer, J. (2005). Is Elliptic-Curve Cryptography Suitable to Secure RFID Tags? Handout of the Ecrypt Workshop on RFID and Lightweight Crypto.

WTO (1994). Agreement on trade-related aspects of intellectual property rights (TRIPS). World Trade Organization. http://www.wto.org/english/tratop_E/trips_e/trips_e.htm.

WTO (2006). Fact sheet: TRIPS and pharmaceutical patents - Obligations and exceptions. World Trade Organization. http://www.wto.org/english/tratop_e/trips_e/factsheet_pharm02_e.htm (09.07.09).

Yang, J., Park, J., Lee, H., Ren, K., and Kim, K. (2005). Mutual Authentication Protocol for Low-Cost RFID. Handout of the Ecrypt Workshop on RFID and Lightweight Crypto.

Yoon, B. (2009). HB-MP++ Protocol: An Ultra Light-weight Authentication Protocol for RFID System. In *IEEE International Conference on RFID – RFID 2009*, Orlando, Florida, USA.

Zhang, X. and King, B. (2005). Integrity Improvements to an RFID Privacy Protection Protocol for Anti-counterfeiting. In Zhou, J., Lopez, J., Deng, R., and Bao, F., editors, *Information Security Conference – ISC 2005*, volume 3650 of *Lecture Notes in Computer Science*, pages 474–481, Singapore, Republic of Singapore. Springer-Verlag.

Zoll (2006). Dem Zoll in Hamburg gelingt vermutlich weltweit gröβter Plagiataufgriff - 117 Container mit gefälschter Ware sichergestellt. November. http://zoll.de.