Diss. ETH No. 16308
TIK-Schriftenreihe Nr. 75

Impact Analysis, Early Detection and Mitigation of Large-Scale Internet Attacks

A dissertation submitted to the
Swiss Federal Institute of Technology
Zürich

for the degree of
Doctor of Sciences

presented by

Thomas P. Dübendorfer

Dipl. Informatik-Ing. ETH
born May 1st, 1975
citizen of Bassersdorf (ZH), Switzerland

accepted on the recommendation of
Professor Dr. Bernhard Plattner, examiner
Dr. Tom Longstaff, co-examiner
Prof. Dr.-Ing. habil. Wolfgang Kröger, co-examiner

2005

Abstract

Internet security development lags far behind the unprecedented rapid growth of the Internet, which is currently approaching one billion users worldwide. Network operators and companies that rely on the Internet for their daily business are challenged continuously by numerous newly discovered vulnerabilities of their Internet hosts, servers, routers and services. As more and more cyber criminals join the Internet, intensity and frequency of large-scale Internet attacks grow at a discomforting pace.

Currently, economic damage of Internet attacks and spam is mostly ignored, only little is publicly known about the real impact of recent network security incidents, and no comprehensive and efficient early attack detection and mitigation mechanisms exist. This PhD thesis tackles these core problems by contributing an economic damage model for Distributed Denial of Service (DDoS) attacks, in-depth analyses of the past Blaster Internet worm, a software framework for online algorithm research, a method for online host behaviour based worm outbreak detection using flow-level backbone traffic and a fundamental concept for building a safe distributed traffic control system that can be used to mitigate large-scale Internet attacks.

We developed an economic damage model, which is the first public comprehensive model that transparently estimates financial damage caused by DDoS attacks suffered by Internet-dependent organisations and entire nations. With our model we estimated that if the whole of Switzerland is affected by a massive DDoS attack that results in an Internet blackout lasting one week, the economic damage to the Swiss economy with an annual GDP of CHF 482 billion sums up to CHF $\sim$6 billion, i.e. $\sim$1.2% of GDP. Interviewed companies were currently found to be only vaguely

aware of the possibly huge impact of losing Internet connectivity for longer periods. With our model we hope to raise the awareness of many companies and policy makers of economies about their strong and still growing Internet dependence. We also present a method for estimating economic damage caused by spam and virus infected e-mails.

In order to investigate real Internet attack traffic, we cooperated in the DDoSVax project at ETH Zürich with the medium-sized Swiss backbone provider SWITCH (AS559). This gave us access to a comprehensive flow-level (NetFlow) traffic archive, which contains all major worm outbreaks and attacks that took place since spring 2003. Using this wealth of information, we performed in-depth forensic analyses of the network worm Blaster.A and the e-mail worm Sobig.F. We found that while exploit code transfer of the multi stage worm Blaster.A was quite frequent, actual successful infections and worm code transfers over the backbone border routers were surprisingly few. For Sobig.F we revealed among other things the timing characteristics of the immense flood of infected e-mails it created and that its greedy spreading behaviour caused many packet retransmissions.

Insights gained from these analyses lead to the design of generic near real-time online algorithms that use flow-level backbone traffic as input. We developed a new classification of hosts regarding their Internet usage behaviour based on three attack sensitive traffic features. By applying this classification to hosts before and during worm outbreaks, we showed that by tracking the number of members in these classes and class combinations not only network worms like Witty and Blaster but also e-mail worms like Sobig.F and MyDoom.A can be detected early. Using it for an early warning system can help network operators to counteract attacks earlier and more effectively. Our software framework named “UPFrame”, which we used to test and run our online algorithm plug-ins, was released as open source software.

For comprehensive and more effective cyber attack countermeasures, adding more flexibility to the Internet core plays a key role. Ideas like active or adaptive networking were around for many years. However, the hesitation was strong by network operators to incorporate any such technologies as data privacy issues and the danger of losing control over the network were not adequately addressed. We proposed a fundamental concept of “traffic ownership”, which has the potential to diminish if not eliminate such concern. Finally, we designed a novel Internet traffic

control system that incorporates our fundamental concept and allows a safe delegation of specific traffic control features from network operators to network users. Our system enables many previously unthinkable new network-integrated services. In medium term, we expect a shift of the responsibility for enforcing Internet security from network users to network operators. The possibility for new security services integrated into the Internet core will foster this trend. Assured by our research results, we think that incorporating more security within the Internet core is feasible, effective and reasonable.

Zusammenfassung

Die Sicherheit im Internet hat sich wesentlich langsamer entwickelt als das unvorhergesehene gewaltige Wachstum des Internets, das in Kürze weltweit eine Milliarde Benutzer erreichen wird. Netzwerkbetreiber und Firmen, welche für ihr Tagesgeschäft auf das Internet angewiesen sind, werden herausgefordert durch die fortlaufende Entdeckung zahlreicher neuer Schwachstellen bei Computern, Servern, Routern und Diensten im Internet. Da immer mehr Kriminelle im Internet auftauchen, steigen die Intensität und die Häufigkeit grosser Attacken mit einer beängstigenden Geschwindigkeit.

Momentan wird durch Internetattacken und Spam verursachter wirtschaftlicher Schaden mehrheitlich ignoriert, es ist nur wenig öffentlich bekannt zum echten Ausmass kürzlicher Sicherheitsvorfälle im Internet, und es existieren keine umfassenden und effizienten Früherkennungs- und Abwehrmechanismen zu Internetattacken. Diese Dissertation behandelt die eben genannten Kernprobleme mit folgenden Beiträgen: Ein Schadensmodell für Distributed Denial of Service (DDoS) Attacken, detaillierte Analysen zum vergangenen Blaster Internetwurm, ein Software-Framework für die Forschung mit online Algorithmen, eine Methode zur Wurmausbrucherkennung basierend auf dem Verhalten von Internetcomputern und ein fundamentales Konzept für den Bau eines sicheren verteilten Verkehrskontrollsystems u.a. zur Abschwächung von Internetattacken.

Wir haben ein wirtschaftliches Schadensmodell entwickelt, welches das erste solche umfassende und öffentliche Modell ist, das transparent den finanziellen Schaden von DDoS Attacken berechnet, der von Internetabhängigen Firmen oder ganzen Nationen erlitten wird. Eine Schätzung mit unserem Modell ergab, dass im Falle einer massiven DDoS Attacke

auf das Internet der Schweiz, welche einem Totalausfall des Internets gleichkommt und eine Woche dauert, ein wirtschaftlicher Schaden von gegen CHF 6 Milliarden entstehen würde. Dieser Schaden entspricht gut 1.2% des Schweizer Bruttosozialprodukts von CHF 482 Milliarden. Interviewte Firmen waren sich des Risikos, für längere Zeit vorübergehend keinen Internetzugang mehr zu haben, nur vage bewusst. Mit unserem Modell hoffen wir, dass das Bewusstsein vieler Firmen und Entscheidungsträger in der Wirtschaft gesteigert wird in Bezug auf ihre starke und immer stärker werdende Internetabhängigkeit und damit verbundene Gefahren. Als Ergänzung stellen wir zudem eine Methode zur Schätzung des wirtschaftlichen Schadens vor, der durch Spam- und Viren-E-Mails entsteht.

Um reale Internetattacken untersuchen zu können, arbeiteten wir im Projekt DDoSVax an der ETH Zürich mit dem mittelgrossen Schweizer Backboneprovider SWITCH (AS559) zusammen. Dies verhalf uns zu einem umfassenden Datenarchiv mit NetFlow-Daten, das alle grösseren Wurmausbrüche und Attacken umfasst, die seit Frühling 2003 stattfanden. Unter Verwendung dieser riesigen Informationsfülle führten wir detaillierte forensische Analysen des Netzwerkwurms Blaster.A und des E-Mail-Wurms Sobig.F durch. Wir stellten fest, dass beim mehrstufigen Blaster-Wurm im Gegensatz zu den sehr häufigen Übertragungen von Code zur Ausnutzung einer Schwachstelle von Windows erstaunlicherweise nur äusserst wenig Übertragungen des eigentlichen Wurmcodes zwischen dem untersuchten Internet-Backbone und benachbarten Backbones stattfanden. Bei Sobig.F zeigten wir u.a. auf, wie die zeitliche Übertragungscharakteristik der verursachten immensen Flut von Viren-E-Mails war und dass das allzu erfolgshungrige Fortpflanzungsverhalten viele Paketneuübertragungen auslöste.

Erkenntnisse aus diesen Analysen führten zum Entwurf von generischen Echtzeit-Algorithmen, welche als Eingabe auf Datenfluss-Ebene abstrahierten Backbone-Verkehr verwenden. Wir entwickelten eine neue Klassifikation der Computer im Internet bezüglich deren Netznutzungsverhalten basierend auf drei Mustern, die empfindlich sind auf Attacken. Durch die Anwendung dieser Klassifikation zeigten wir, dass durch das Verfolgen der Anzahl Mitglieder pro Klasse bzw. Klassenkombination nicht nur Netzwerkwürmer wie Witty und Blaster, sondern auch E-Mail basierte Würmer wie Sobig.F und MyDoom.A früh erkannt werden können. Die Verwendung als Frühwarnsystem für Internetat-

tacken kann Netzwerkbetreibern helfen, Attacken früher und effektiver zu bekämpfen. Unser Software-Framework "UPFrame", das wir zum Testen und Ausführen unserer online Algorithmen-Plug-ins verwendeten, wurde als Open Source Software veröffentlicht.

Für umfassende und effektivere Gegenmassnahmen zu Internetattacken spielt zusätzliche Flexibilität im Kern des Internets eine Schlüsselrolle. Ideen dazu wie aktive oder adaptive Netzwerktechnologien gibt es schon seit vielen Jahren. Dennoch zögerten die Netzwerkbetreiber stark, irgendwelche solche Technologien einzubauen, weil es bisher keine Lösung gab, um dadurch entstehende Datenschutzprobleme und die Gefahr, die Kontrolle über das Netzwerk zu verlieren, angemessen zu behandeln. Wir schlugen ein fundamentales Konzept namens "Traffic Ownership" (Eigentümerschaft von Verkehrsdaten) vor, welches das Potential hat, solche Bedenken zu mildern oder gar gänzlich zu eliminieren. Schliesslich entwarfen wir ein neuartiges Kontrollsystem für Internetverkehr, welches unser fundamentales Konzept umsetzt und es erlaubt, gefahrlos gewisse Verkehrskontrollfunktionen von den Netzwerkbetreibern an die Netzwerkbenutzer zu delegieren. Unser System ermöglicht es, bisher als undenkbar geltende neue und direkt im Netzwerk integrierte Dienste anzubieten. Mittelfristig erwarten wir, dass sich die Zuständigkeit für die Gewährleistung von Internetsicherheit von den Netzwerkbenutzern zu den Netzwerkbetreibern verlagern wird. Die Möglichkeit für neue direkt im Internet integrierte Sicherheitsdienste wird diesen Trend noch verstärken. Unterstützt durch unsere Resultate denken wir, dass die Integration zusätzlicher Sicherheit ins Internet möglich, wirksam und sinnvoll ist.