DISS. ETH NO. 20419

MODELING AND ENFORCING WORKFLOW AUTHORIZATIONS

A dissertation submitted to
ETH ZURICH
for the degree of
Doctor of Sciences

presented by

Samuel Jakob Burri

MSc ETH CS
born on 12 October 1981
citizen of Root (LU) and Malters (LU)

accepted on the recommendation of
Prof. Dr. David Basin, examiner
Dr. Günter Karjoth, co-examiner
Prof. Dr. Srdjan Capkun, co-examiner

2012

Abstract

Authorizations are fundamental in protecting information systems. In this dissertation, we study the modeling and enforcement of authorizations for workflows, which are a well-established abstraction of an organization's business processes. We thereby make authorizations sensitive to their business environment. For example, they may be tailored to workflow-specific relations between tasks and may anticipate potential future task executions. A prevalent class of authorizations, whose realization benefits from this additional information, are Separation of Duty (SoD) constraints. They aim at reducing fraud and errors and are therefore commonplace in regulated environments, such as the financial industry. More specifically, we address two main problems.

First, we study the refinement of abstract SoD constraints to concrete workflow models, and how to integrate an enforcement monitor for the resulting refinement into a heterogeneous workflow environment. We thereby bridge the gap between the formalization of high-level, workflow-independent authorization requirements and their enforcement. Our enforcement formalization and its service-oriented implementation account for the dynamics of today's business environments. In particular, we model administrative activities that reflect organizational changes occurring during workflow execution, addressing a well-known source of fraud.

Second, we propose a novel approach to aligning the enforcement of authorizations with their workflow-based business environment. Existing workflow authorization models make strong restrictions on workflows' control-flows; for example, they do not support loops. Our approach, in particular our novel technique for scoping authorizations within workflows, lifts this restriction. We proceed by identifying the notion of an obstruction, which generalizes deadlock caused by authorizations, and we study the construction of obstruction-free enforcement mechanisms. Finally, we introduce the concept of optimal authorizations for a workflow that maximize protection, yet allow for their obstruction-free enforcement. We provide tool support for our approach by extending a modeling platform and by building on algorithms from optimization theory.

Zusammenfassung

Autorisierungen sind ein fundamentaler Bestandteil des Schutzes von Informationssystemen. Im Fokus dieser Dissertation steht das Modellieren und Durchsetzen von Autorisierungen im Kontext von Workflows, einer etablierten Abstraktion von Geschäftsprozessen. Dadurch werden Autorisierungen mit dem Geschäftsumfeld verknüpft und können beispielsweise auf Beziehungen zwischen mehreren Arbeitsschritten zugeschnitten werden und zukünftige Arbeitsschritte antizipieren. Ein weitverbreitetes Autorisierungskonzept, dessen Realisierung von diesen zusätzlichen Informationen profitiert, ist das Mehr-Augen-Prinzip. Dieses bezweckt, Betrug und Fehler zu verhindern, und ist in regulierten Geschäftsfeldern, wie beispielsweise der Finanzindustrie, allgegenwärtig. Wir beschäftigen uns mit zwei Hauptproblemen.

Erstens studieren wir das Verfeinern von abstrakten Bestimmungen, die auf dem Mehr-Augen-Prinzip beruhen, zu konkreten Workflow-Modellen und die Frage, wie die gewonnenen Verfeinerungen in heterogenen Workflow-Umgebungen durchgesetzt werden können. Damit überbrücken wir die Kluft zwischen einer Workflow-unabhängigen Spezifikation von Autorisierungsanforderungen und deren Durchsetzung. Unsere Formalisierung und deren Service-orientierte Umsetzung sind an die Dynamik der heutigen Geschäftswelt angepasst. So modellieren wir beispielsweise administrative Aktivitäten während der Ausführung von Workflows, die zu Autorisierungsveränderungen führen und bei Nichtbeachtung Betrug begünstigen.

Zweitens präsentieren wir einen neuen Ansatz, um die Durchsetzung von Autorisierungen mit ihrem Workflow-basierten Geschäftsumfeld abzustimmen. Existierende Workflow-Autorisierungsmodelle schränken den Kontrollfluss von Workflows stark ein, da sie beispielsweise keine Schleifen erlauben. Unser Ansatz, insbesondere unsere Technik zum Abgrenzen von Autorisierungen, hebt diese Einschränkungen auf. Weiter führen wir den Begriff der Obstruction ein, die eine durch Autorisierungen begründete, teilweise Blockierung einer Workflow-Ausführung beschreibt. Darauf aufbauend studieren wir die Konstruktion von Obstruction-freien Durchsetzungsmechanismen. Schliesslich führen wir

das Konzept von optimalen Autorisierungen für einen Workflow ein, die eine Obstruction-freie Durchsetzung ermöglichen und dabei maximalen Schutz bieten, beziehungsweise Kosten minimieren. Durch die Erweiterung einer bestehenden Modellierungssoftware und unter Anwendung von bekannten Optimierungsalgorithmen stellen wir eine Werkzeugunterstützung für unseren Ansatz bereit.