Ausblick auf die modellgetriebene, mustergestützte Sicherheit in serviceorientierten Architekturen*

Heiko Klarl [1, 2]

[1]Universität Regensburg
Institut für Medien-, Informations- und Kulturwissenschaft
93040 Regensburg

[2]iC Consult GmbH
Keltenring 14
82041 Oberhaching
h.klarl@klarl.eu

Zusammenfassung

Mit dem Konzept der serviceorientierten Architektur und der damit erwarteten schnelleren und flexibleren Anpassung von Geschäftsprozessen (GP) werden neue Ansätze zur Absicherung solcher Systeme nötig. Sicherheitsanforderungen werden bisher jedoch meist abseits der Geschäftsprozessmodelle betrachtet und separat definiert. Dies führt zu zwei parallelen Modellen der Anforderungsbeschreibung, d. h. die funktionellen Anforderungen des GP existieren losgelöst von dessen nichtfunktionellen Anforderungen, insbesondere der sicherheitsrelevanten. Regelmäßige Änderungen des GP können so zu Inkonsistenzen bei der Absicherung führen. Im Rahmen eines Promotionsverfahrens sollen Möglichkeiten gefunden werden, auf globalen Richtlinien basierende Sicherheitsanforderungen enger mit den Geschäftsprozessmodellen zu verknüpfen und daraus valide Policies für die Sicherheits-Integrations-Ebene zu erzeugen.

Abstract

With the emerging trend of service-oriented architectures and a faster and more flexible adaption of business processes, new security paradigms are being required. Security requirements are mostly separated from business processes. Thus, functional and non-functional requirements exist in two different models. Changes of the business process could therefore lead to an inconsistency of its security models. The future research work concentrates on linking security requirements – based on global policies – to business process models for generating valid policies for the security integration layer.

* Veröffentlicht in: Osswald, Achim; Stempfhuber, Maximilian; Wolff, Christian (Hrsg.) (2007). Open Innovation. Proc. 10. Internationales Symposium für Informationswissenschaft. Konstanz: UVK, 381-383.

1 Einleitung

Das Paradigma der serviceorientierten Architektur verspricht der Unternehmens-IT die schnelle und flexible Anpassung von GP, um einerseits auf Veränderungen des Marktes reagieren und andererseits gesetzliche Vorschriften umsetzen und dadurch Compliance-Anforderungen einhalten zu können. Die Absicherung der serviceorientierten Architektur kann über eine Sicherheits-Integrations-Ebene erfolgen und ist somit nicht mehr plattform- oder applikationsorientiert [Nakamur et al. 2002]. Die funktionellen Aspekte eines GP können mit bewährten Methoden modelliert werden (vgl. [Keller et al. 1992], [UML]), die Beschreibung der nichtfunktionellen Sicherheitsanforderungen ist jedoch noch immer weitgehend von diesen Modellen losgelöst und existiert oftmals nur als Spezifikation in verschiedenen Dokumenten (vgl. [Lodderstedt et al. 2002]). Ziel der künftigen Entwicklung muss es sein, die nichtfunktionellen Anforderungen in das Modell zu integrieren und somit eine engere Kopplung zwischen den funktionellen Anforderungen des GP und seinen nichtfunktionellen Sicherheitsanforderungen zu erreichen.

2 Vorgehensweise und Aufbau der Arbeit

Nichtfunktionelle Sicherheitsanforderungen eines GP setzen sich aus zwei verschiedenen Bereichen zusammen. Auf der einen Seite existieren globale Richtlinien und Anforderungen (organisatorische Sicherheits-Meta-Policies), die durch die Sicherheits-Strategie des Unternehmens vorgegeben sind, auf der anderen Seite existieren zusätzlich die fachlichen Sicherheitsanforderungen (Geschäfts-Policies) an den jeweiligen GP. Diese können eine Konkretisierung der Sicherheits-Meta-Policies oder rein fachliche Anforderungen repräsentieren. Die zukünftige Forschungsarbeit teilt sich in verschiedene Schritte auf. Im ersten Schritt ist zu klären, inwiefern bestehende Modelle zur Beschreibung der *Enterprise Architecture* (vgl. [TOGAF], [Zachman 2003]) die Abbildung von organisatorischen Sicherheits-Meta-Policies unterstützen bzw. um diese erweitert werden können und welchen sinnvollen Umfang diese Sicherheits-Meta-Policies annehmen können. Der zweite Schritt umfasst vor allem die Belange der fachlichen Sicherheitsanforderungen. Es ist zu untersuchen, wie diese basierend auf den Sicherheits-Meta-Policies durch die Fachseite konkretisiert werden können. Ferner sind Wege zu finden, wie die Fachseite bei der Konkretisierung unterstützt werden kann und wie anschließend die formalisierten Geschäfts-Policies in das Modell des GP eingefügt werden können, um daraus valide Infrastruktur-Policies für die Sicherheits-Integrations-Ebene er-

zeugen zu können. Sind diese Arbeiten fortgeschritten, kann der Einsatz von Business Process Security Pattern (BPSP) als mögliche Unterstützung für die Fachseite evaluiert werden. BPSP, in Anlehnung an die in [Tatsubori et al. 2004] vorgestellten *Idioms*, bündeln für eine Anforderungssituation verschiedene Geschäfts-Policies und lassen sich daher als „Lösungsschablone" verwenden. Das Auffinden von BPSP wird vermutlich über zwei verschiedene Wege möglich sein. Wiederkehrende Anforderungen, die mehrere Geschäfts-Policies umfassen können, können aufgrund ihrer logischen Zusammenhänge zu BPSP zusammengestellt werden. Als Beispiel kann die Benutzer-Authentifizierung angeführt werden. Kommt der Benutzer aus dem Intranet, so genügt ein vertrauenswürdiger SAML-Token, kommt er allerdings aus dem Internet, so wird eine Zwei-Faktor-Authentifizierung erforderlich. Andere BPSP werden allerdings nicht so einfach aufzufinden sein und erst erfahrungsgetrieben durch Analyse der modellierten Geschäfts-Policies und ihrer Zusammenhänge beschrieben werden können. Ist eine Menge von BPSP identifiziert, muss eine praktische Evaluierung ihren Nutzen für die Fachseite bewerten.

3 Literatur

[Keller et al. 1992] Keller, G.; Nüttgens, M., Scheer, A.: Semantische Prozessmodellierung auf der Grundlage Ereignisgesteuerter Prozessketten (EPK), *Veröffentlichungen des Instituts für Wirtschaftsinformatik (IWi), Universität des Saarlandes (*1992)

[Lodderstedt et al. 2002] Lodderstedt, T., Basin, D.A., Doser, J.: SecureUML: A UML-Based Modeling Language for Model-Driven Security. In: International Conference on The Unified Modeling Language, S. 426 – 441 (2002)

[Nakamur et al. 2002] Nakamur, Y., Hada, S., Neyama, R.: Towards the Integration of Web Services Security on Enterprise Environments. In: Symposium on Applications and the Internet (SAINT) Workshops, S. 166 (2002)

[Tatsubori et al. 2004] Tatsubori, M., Imamura, T., Nakamura, Y.: Best-Practice Patterns and Tool Support for Configuring Secure Web Services Messaging. In: IEEE International Conference on Web Services, S. 244 (2004)

[TOGAF] The Open Group: The Open Group Architecture Framework, *http://www.opengroup.org/architecture/togaf8-doc/arch/toc.html* (10.04.2007)

[UML] Object Management Group, Inc.: Unified Modeling Language (UML), *http://www.uml.org/#UML2.0* (2007) (10.04.2007)

[Zachman 2003] John A. Zachman: The Zachman Framework: A Primer for Enterprise Engineering and Manufacturing, Electronic book published on www.zachmaninternational.com (2003)