

## Forschung

# Zugriffsrichtlinien automatisch umsetzen



Wolfgang Giersche, Zühlke Engineering AG, Gründungsmitglied HERAS<sup>AF</sup>, Dozent für Informatik an der Hochschule Rapperswil, Schweiz

Unternehmen oder Institutionen, die mit sensiblen Daten umgehen müssen, unterliegen in zunehmendem Masse gesetzlichen Richtlinien für den Schutz und die Integrität dieser Daten – zum Beispiel etwa HIPAA, den Sarbanes-Oxley Act oder Basel II. Zu den am stärksten betroffenen Unternehmen gehören traditionell insbesondere Banken und praktisch alle Gesundheitsdienstleister.

Die tatsächliche Erfüllung aller gesetzlichen wie auch der sonstigen betriebsinternen Richtlinien wird umso schwieriger, je grösser die Zahl der Systeme oder Applikationen ist, die solche Daten speichern und auswerten. In der Regel stellt zwar jede einzelne Softwarekomponente Methoden zum Schutz der in ihr selbst verwalteten Daten zur Verfügung; aber je mehr solche Komponenten eines komplexen IT-Systems untereinander Daten austauschen, umso grösser wird das Bedürfnis nach einer systemübergreifenden Lösung. Dafür jedoch müssten sich zunächst möglichst viele Softwarehersteller auf gewisse Standards für die formale Beschreibung und den Austausch von Zugriffsrichtlinien und Zugriffsanfragen einigen.

Tatsächlich hat das internationale OASIS-Konsortium (Organization for the Advancement of Structured Information Standards) bereits 2003 einen solchen auf XML basierenden Standard mit Namen XACML (eXtensible Access Control

Markup Language) verabschiedet.

## XACML

Der XACML Standard, Version 2 von 2005<sup>1</sup> beinhaltet im Wesentlichen drei Aspekte:

- die Beschreibung einer Anfrage als Menge von Attributen: Name-Wert-Paare, etwa der Form Rolle = Arzt, Zugriff = Lesen, Ressource = Patientengeschichte;

- die Beschreibung von Zugriffskontrollregeln (*Policy*) als logischen Ausdruck auf solchen Attributen, die für jede Anfrage genau eine der folgenden «Entscheidungen» liefern:

- PERMIT (Zugriff gestattet);
- DENY (Zugriff verweigert);
- NOT\_APPLICABLE (Policy nicht anwendbar);
- INDETERMINATE (es ist ein [interner] Fehler aufgetreten);

- eine Architektur zur Umsetzung der Policies, bestehend aus verschiedenen funktionalen Komponenten und einem Protokoll für die Kommunikation zwischen diesen Komponenten.

XACML gehört zur Familie der regelbasierten Zugriffskontrollsprachen. Es erweitert die weithin bekannten rollenbasierten Modelle<sup>2</sup>, in dem es nicht nur Rollen, sondern Attribute im Allgemeinen verwenden kann. Damit ist es möglich, Richtlinien wie die folgende auszudrücken:

*Ein Arzt darf die Patientengeschichte ausschliesslich derjenigen Patienten einsehen, die nicht explizit eben jenen davon ausgeschlossen haben.*

Man möge sich zur Illustration einen Patienten vorstellen, der mit einer heiklen Erkrankung gerade in das Krankenhaus eingeliefert wird, in dem seine Exfrau praktiziert, und der Patient die Details seiner Krankheit nicht mit ihr teilen möchte.

## XACML-Architektur

XACML bedient sich eines Komponentenmodells, dessen grundlegender Gedanke ist, dass Programme, Applikationen oder ganze Systeme mit Kontrollpunkten ausgestattet werden (*Policy Enforcement Point* oder PEP). Diese Kontrollpunkte fangen den Programmverlauf automatisch beim Zugriff auf wohldefinierte Ressourcen ab und formulieren eine Zugriffsanfrage, einen *Request*. Der PEP schickt diesen *Request* an eine zentrale Serverkomponente, den *Policy Decision Point*, kurz PDP. Der PDP nun kennt im Prinzip alle gültigen Zugriffsrichtlinien, «rechnet» mit deren Hilfe die Entscheidung aus und schickt die Entscheidung zurück an den PEP. Dieser kann nun je nach Entscheidung den Programmablauf ungehindert fortfahren lassen: den Zugriff also gestatten oder aber einen Fehler auslösen und den Zugriff damit verweigern.

Der Vorteil dieser Architektur liegt auf der Hand: Alle für eine bestimmte Domäne relevanten Richtlinien werden an einer für diese Domäne zentralen Stelle gespeichert und verwaltet. Dadurch wäre es im Idealfall möglich, dass nach

Inkraftsetzung einer neuen Richtlinie an dieser einen Stelle alle angeschlossenen Systeme von diesem Zeitpunkt an diese Richtlinie tatsächlich auch automatisch befolgen. Eine verführerische Vision, die allerdings in der Umsetzung immer neue Herausforderungen mit sich brachte und noch immer bringt und daher zu einem Gebiet intensiver Forschung avancierte. Im Folgenden beschreiben wir kurz einige der wichtigsten Fragen, die es auf dem Weg zu einer erfolgreichen Sicherheitslösung mit XACML zu lösen gilt.

### **Weitgehende Instrumentierung erforderlich**

Die erste Voraussetzung für eine funktionsfähige Zugriffskontrolle der beschriebenen Art ist sicher die Fähigkeit der existierenden geschäftlichen Anwendungen, die jeweiligen Zugriffe auf kritische Ressourcen auch tatsächlich abzufangen. Die nachträgliche Instrumentierung bestehender Applikationen ist allerdings in vielen Fällen nicht oder nur beschränkt möglich. Bei der Entwicklung neuer Software hingegen wäre die Instrumentierung vergleichbar einfach. Softwareproduzenten aber werden gewiss nicht ohne eindeutig erkennbaren Bedarf im Markt eine solche, die Entwicklung verteuern Instrumentierung vornehmen. Es ist daher wohl anzunehmen, dass nur entweder eindeutige gesetzliche Auflagen oder aber der Einfluss grosser Interessenverbände die Entwicklung von XACML-konformen Anwendungen forcieren könnten.

### **Grammatik mit erweiterbarem Vokabular**

Man kann XACML als eine Art Grammatik zum Austausch von Informationen über sicherheitsrelevante Zugriffe beschreiben. Wo in einem ganzen Satz praktisch jeder menschlichen

chen Sprache Subjekt, Prädikat, Objekt und adverbiale Konstrukte stehen, da stehen bei XACML *Subjekt, Aktion, Ressource* und *Umgebung*. Ein *Request* wird also etwa wie folgt aufgebaut:

Wer (Subjekt) will was (Aktion) womit (Ressource) unter welchen Bedingungen (Umgebung) anstellen?

Die einzelnen Bestandteile werden jeweils mit spezifischen Attributen beschrieben. Der Standard legt eine Grundmenge von Attributen fest, erlaubt aber die Definition weiterer Attribute, damit XACML für praktisch jede geschäftliche Domäne anwendbar ist. Werden aber Elemente verwendet, die nicht in der Sprache festgelegt sind, ist nicht garantiert, dass jede XACML-konforme Anwendung mit einem PDP sprechen kann, der diese Erweiterungen verwendet. Die Richtlinien innerhalb eines PDPs müssen ja mit denselben Attributen ausgedrückt sein, in der ein Kontrollpunkt für eine Anwendung Anfragen formuliert.

### **Richtlinien formulieren**

Richtlinien in der firmeneigenen Umgangssprache zu formulieren ist an sich schon eine komplexe Aufgabe. Um aber diese Richtlinien einem Softwaresystem zugänglich zu machen, müssen die umgangssprachlichen Richtlinien unter Wahrung ihrer Semantik formalisiert werden. Erst dann können sie in ausführbare Richtlinien umgewandelt werden.

Auch wenn diese Formalisierung erfolgreich durchgeführt wurde, müssen diese Richtlinien sicher verwaltet werden. Nehmen wir an, alle Applikationen, beispielsweise die eines grossen Klinikums, wären mit einem PDP verbunden. Jetzt sind es Menschen, die dafür verantwortlich sind, dass Richtlinien erstellt, geprüft und in Kraft gesetzt wer-

den. Während aber die Pflege der Sicherheitseinstellung eines einzelnen Programms noch weitestgehend überschaubar ist, wird wohl kaum ein Mensch die genaue Auswirkung einer neuen Richtlinie auf Hunderte von Applikationen vorhersagen können. Bei jeder neuen Richtlinie wären etwa folgende wichtige Fragen zu klären:

- Steht die neue Richtlinie in Konflikt zu existierenden Richtlinien? Wenn ja, wie soll dieser Konflikt jeweils aufgelöst werden?
- Deckt die Gesamtheit aller Richtlinien wirklich alle möglichen Zugriffsfälle ab?
- Hat die Richtlinie tatsächlich den erwünschten Effekt?

Ohne weitgehende Unterstützung durch ein hochspezialisiertes Programm wie etwa einen Richtlinieneditor mit reichhaltigem Repertoire an Prüffunktionen wäre der Einsatz einer XACML-Architektur wahrscheinlich nur schwer zu verantworten.

### **Merger and Acquisitions**

Wenn zwei Unternehmen durch Fusion oder Übernahme zusammenkommen, stehen die IT-Verantwortlichen beider Firmen vor der Aufgabe, auch die Infrastruktur miteinander zu verschmelzen. Dabei müssen aber auch die Richtlinien abgeglichen werden, wenn Informa-

### **Kurz & bündig**

Gesetzliche Richtlinien hinsichtlich der Integrität und der Vertraulichkeit sensibler Daten erfordern immer teurer werdende Massnahmen. Schon aufgrund der heute typischerweise unüberschaubaren Datenmengen sind zur effizienten und nachvollziehbaren Umsetzung solcher Richtlinien spezialisierte Softwarewerkzeuge unabdingbar. Damit diese aber möglichst breit eingesetzt werden können, ist eine weitgehende Standardisierung erforderlich. Mit dem OASIS-Standard XACML gibt es seit einigen Jahren eine Basis für die Entwicklung generell einsetzbarer Werkzeuge für die Durchsetzung von Zugriffsrichtlinien.



HERAS<sup>AF</sup> Policy Administration Point

tionen aus der einen Datenquelle nun auch in Applikationen der einst fremden Umgebung verwendet werden sollen. Wenn beide Unternehmen vorher bereits eine XACML-basierte Sicherheitslösung eingesetzt haben, dann besteht die Aufgabe darin, aus zwei Sätzen von Richtlinien einen einzigen, widerspruchsfreien und vollständigen Satz zu gewinnen. Die Erforschung dieses Gebietes wird von der Hoffnung getragen, dass es formale und damit automatisierbare Methoden gibt, unterschiedliche Mengen von Policies zu einer einzigen zu «verrechnen». Eine Arbeit, die ohne technische Hilfe vermutlich enorm aufwendig und fehleranfällig wäre.

#### Aktuelle Entwicklungen

Keine der beschriebenen Herausforderungen scheint unlösbar. Und so bemüht sich seit

einigen Jahren eine wachsende Zahl von Softwareherstellern, Universitäten und Fachverbänden um Lösungen.

#### E-Health

Im Juli 2007 hat der schweizerische Bundesrat in seiner E-Health-Strategie die Schaffung der Infrastruktur für ein elektronisches Patientendossier bis zum Jahr 2015 beschlossen<sup>3</sup>. Bis dahin soll es möglich sein, dass alle angeschlossenen Organe des Gesundheitswesens bei bestehender Einwilligung des Patienten unter wohlbestimmten Bedingungen die bei allen anderen Instituten gespeicherten Dossiers dieses Patienten elektronisch anfordern können. Die Initiative IHE4 (*Integrating the Healthcare Enterprise*) bietet eine internationale Plattform für den Dialog zwischen Softwareproduzenten und Softwarebenutzern im Ge-

sundheitswesen. Dort sollen die zugrunde liegenden Prozesse definiert und eine auf XACML basierende Infrastruktur konzipiert werden. In den USA unternimmt die Versorgungseinrichtung für Kriegsveteranen, das *Department of Veterans Affairs*, derzeit massive Anstrengungen, um ein formales Vokabular für den Austausch von Patienteninformationen zu standardisieren<sup>5</sup>.

Neben den eher praktisch orientierten Initiativen der betroffenen Verbände und Institutionen ist auch die theoretische Erforschung der fundamentalen Eigenschaften komplexer Regelsysteme weiter vorangekommen. An der Universität Mailand wurden zum Beispiel die grundlegenden Eigenschaften von Richtlinienensystemen formal als Algebra<sup>6</sup> beschrieben, welche sich leicht auf die Operatoren von XACML anwenden lassen.

## HERAS<sup>AF</sup>

Seit 2006 erarbeitet das Projekt HERAS<sup>AF</sup> der Hochschule für Technik in Rapperswil Softwarelösungen für einige der vorher beschriebenen Probleme. HERAS<sup>AF</sup> steht für *Holistic, Enterprise-Ready Application Security Architecture Framework*, was so viel heisst wie: ganzheitliches Rahmenwerk für unternehmenstaugliche Applikationssicherheit. Im Rahmen von Studienarbeiten von Bachelor- und Master-Studenten ist zunächst eine frei verfügbare XACML-Implementierung entstanden. Basierend auf dieser entstanden weitere wichtige Bausteine, wie etwa ein PEP, eben ein solcher Kontrollpunkt, der Java-Applikationen in die Lage versetzt, Zugriffsentscheidungen an einen zentralen *Policy Decision Point* zu delegieren. In zukünftigen Arbeiten sollen natürlich auch andere Technologien wie etwa .NET oder weitere Programmiersprachen unterstützt werden.

Derzeit fokussieren sich die Anstrengungen des Projektes auf die Entwicklung eines intelligenten Policy-Design-Werkzeugs, mit dem technisch weniger versierte Sicherheitsverantwortliche praktisch in

ihrer Umgangssprache effizient Richtlinien beschreiben können, die dann von diesem Softwarewerkzeug in maschinenlesbare XACML-Policies umgewandelt werden. Aus einer ersten Web-basierten Studie für einen solchen Web-basierten Richtlinien-Designer konnten bereits wichtige Erkenntnisse gewonnen werden. Vor allem ging es darum, dass die eigentlich für das Erlassen von Richtlinien verantwortlichen Personen ohne jegliche Kenntnis der dahinterliegenden Technologie fast intuitiv ihre Richtlinien formulieren können.

Als weiteren wichtigen Meilenstein konnte das Projekt die erfolgreiche Teilnahme an der *Interoperability Demo* auf der letztjährigen OASIS-Konferenz in London verbuchen. Dort konnte man live miterleben, wie Zugriffe auf Patientendaten mittels einer Anwendung aus dem Healthcare-Bereich von den teilnehmenden XACML-Produkten durch unterschiedliche, mitunter komplexe Richtlinien reguliert wurden.

Alle Dokumente und Quelltexte, die im Projekt HERAS<sup>AF</sup> erarbeitet werden, stehen unter einer Open-Source-Lizenz zum Download zur Verfügung.

## Fazit

Zugriffsrichtlinien zentral zu verwalten und damit automatisch domänenweit umzusetzen, ist eine attraktive Vorstellung für diejenigen, die letztendlich die Verantwortung für das Befolgen von Richtlinien tragen. Softwarehersteller wie Oracle und IBM, aber auch viele andere kleinere und mittlere Anbieter bereiten sich auf den Einsatz von XACML vor, indem sie schon heute Teile ihrer Produkte mit XACML-Basistechnologie ausstatten. So ist damit zu rechnen, dass ein breiter Einsatz von XACML in absehbarer Zukunft tatsächlich die Einhaltung gesetzlicher Richtlinien vereinfachen kann. Stellen Sie sich vielleicht das folgende, gar nicht so unwahrscheinliche Szenario vor: Ein neues Gesetz schreibt vor, dass in speziellen Notfällen gewisse Details der Krankengeschichte auch für Pflegepersonal zugänglich sein müssen. Die dazugehörigen XACML-Richtlinien kann man über das Internet beziehen und – nach Prüfung – in das eigene System einspielen. Damit werden sie in der ganzen IT-Infrastruktur unmittelbar wirksam. So oder ähnlich könnte es eines Tages sein. ■

## Literatur, weiterführende Links

- eXtensible Access Control Markup Language Version 2.0, OASIS, 2005.
- RÜDIGER GRIMM/NANCY MELETIADOU, Zugriffskontrolle im Gesundheitswesen, Das Konzept rollenbasierter Zugriffskontrolle (RBAC) zum Schutz von patientenbezogenen Daten, *digma* 2006, 170 ff.
- P. BONATTI ET AL., An Algebra for Composing Access Control Policies. *ACM Transactions on Information and System Security* 5 (2002) 1–35.
- Holistic Enterprise-Ready Application Security Architecture Framework; <[www.herasaf.org](http://www.herasaf.org)>.

## Fussnoten

- <sup>1</sup> Version 3 ist in Arbeit.
- <sup>2</sup> Vgl. MELETIADOU/GRIMM 2006.
- <sup>3</sup> Siehe <<http://www.bakom.admin.ch/themen/infosociety/01689/>> (letztmals besucht: 10.2.2009).
- <sup>4</sup> Integrating the Healthcare Enterprise, <[http://en.wikipedia.org/wiki/Integrating\\_the\\_Healthcare\\_Enterprise](http://en.wikipedia.org/wiki/Integrating_the_Healthcare_Enterprise)> (letztmals besucht: 10.2.2009).
- <sup>5</sup> Cross-Enterprise Security and Privacy Authorization Profile of XACML 2.0 for Healthcare.
- <sup>6</sup> Vgl. BONATTI ET AL. 2002.