DuD
Datenschutz und Datensicherheit

Rollen als Schlüssel für B2B Anwendungen

Technologische Voraussetzungen für Verträge in verteilten, rollenbasierten Systemen

Thomas Gebhardt und Thomas Hildmann

Business-to-Business soll der Goldesel der Zukunft sein. Wirklich Business-gerechte Anwendungen scheitert heute jedoch schon am Problem einer ausreichend flexiblen Autorisierung. Wie zukunftweisende Autorisierung von Benutzern funktioniert, ohne als Firma gleich all seine Personalentscheidungen offen legen zu müssen und mit einem Mehrgewinn an Privatsphäre für den Benutzer zeigt dieser Artikel.

[FOTO]

Dipl.-Inform.
Thomas Gebhardt

Wissenschaftlicher Mitarbeiter am PRZ der TU Berlin, Schwerpunkt: rollenbasierte Zugriffskontrolle

E-Mail: gepard@prz.tu-berlin.de

[FOTO]

Dipl.-Inform.
Thomas Hildmann

Wissenschaftlicher Mitarbeiter am PRZ der TU Berlin, Schwerpunkt: Zugriffskontrollsysteme

E-Mail: hildmann@prz.tu-berlin.de

Einleitung

Ein Mensch bleibt immer derselbe, egal ob er gerade im Büro, beim Einkaufen, zu Hause oder im Schwimmbad ist. Für seine Umgebung ändert er jedoch ständig seine Identität. Er schlüpft in verschiedene Rollen: Die des Familienvaters, des Kollegen, die des harten Verhandlungspartners oder die des Hobbysportlers usw.

Für uns ist das Schlüpfen in verschiedene Rollen eine Möglichkeit, unsere Privatsphäre zu wahren. Je nach unserer Rolle geben wir andere Informationen über uns preis. Wir sind in der Regel jedoch sehr darauf bedacht, dass z.B. der Familienvater im Verborgenen bleibt während wir im Auftrag unserer Firma eine Verhandlung führen.

Wir handeln oft im Auftrag von jemanden, in Vertretung oder als Delegation von einer Person oder einer ganzen Organisation, egal ob wir nun selbst diese Organisation leiten oder einfache Angestellte sind.

Scheinbar nur ein einfacher Einkauf

Der Bücherladen ganz in der Nähe unseres Institutes ist stets ein gefährlicher Ort für mein Bankkonto. Wenn ich mal wieder dort bin, um für die TU Bücher zu kaufen finde ich regelmäßig auch Werke, die mein ganz privates Interesse wecken. Ich muss dann bestimmt Bücher privat aus meiner eigenen Brieftasche kaufen und andere im Namen der TU, die dann die Rechnung übernimmt.

Bei uns in der TU ist das ähnlich gelöst, wie wohl fast überall anders auch. Für die Bücher, die ich im Namen meiner Organisation kaufen soll, habe ich einen offiziellen Bestellschein, der vorher bereits ausgefüllt wurde und der mit Stempel und Unterschrift eines Zeichnungsberechtigten versehen wurde. Für den Laden spielt es auch keine Rolle, ob evtl. ich die Bücher bestelle und eine meiner Kolleginnen oder Kollegen sie später abholt. Es zählt nur der Auftraggeber, der TU-Präsident.

Über Internet kann ich zur Zeit noch nicht auf diese Art und Weise einkaufen gehen. Hier kann ich mir nur einen persönlichen Zugang besorgen oder mit meiner privaten Kreditkarte zahlen. Und selbst wenn es das TU-weite Passwort für den Zugang beim Onlineshop gäbe, wo bleibt die Berechtigung, die ich mir zunächst von unserem Institutsleiter besorgen müsste? Und was, wenn ich irgendwann gar nicht mehr das Recht hätte einzukaufen?

Über Kennwörter und Zugriffslisten lässt sich ein solcher, in der Geschäftswelt absolut üblicher Vorgang nicht so einfach abbilden.

Während im Consumer-to-Business (C2B) Bereich die Verwaltung von Zugriffsrechten über einfache Zugriffslisten noch völlig ausreichend waren, benötigen wir sehr viel flexiblere und mächtigere Zugriffskontrollmechanismen für den Business-to-Business (B2B) Sektor.

Eine System muss an Hand der ihm zur Verfügung stehenden Informationen in der Lage sein zu entscheiden, ob ein Benutzer berechtigt ist, eine Aktion auszuführen oder nicht. Das System muss also eine Komponente enthalten, die die Vertrauenswürdigkeit von Benutzern einstuft, eine sogenannte Trust Management Komponente.

Es gibt zwei grundsätzlich verschiedene Ansätze eine Einstufung der Vertrauenswürdigkeit eines Benutzers vorzunehmen.

Der eine Weg führt über die elektronische Signatur und das darin enthaltene Zertifikat. Im Zertifikat kann bereits die Information enthalten sein, ob ein Benutzer berechtigt ist, eine gegebene Aktion auszuführen oder nicht.

Dies macht das Vertrauensmodell jedoch sehr statisch. Ist die Berechtigung einer Person z.B. von verschiedenen Randbedingungen abhängig und will die Organisation diese Randbedingungen ferner nicht nach außen preisgeben, ist es das einfachste, eine anonyme, nicht zweckgebundene Beglaubigung (Credential) an den Benutzer auszuhändigen. Soll jetzt von dritten geprüft werden, ob der Benutzer das Recht hat im Namen der Organisation eine Aktion auszuführen, kann mittels der ausgestellten Beglaubigung die Organisation nach der Berechtigung befragt werden. Weder der Benutzer noch die Organisation geben so mehr als die unbedingt erforderlichen Informationen preis.

In [Blaze96] werden vier Aufgaben eines solchen Trust Managements identifiziert:

1. Formulierung von Sicherheitsrichtlinien (Security Policies),
2. Beglaubigungen (Security Credentials),
3. Den Zusammenhang zwischen Beglaubigungen und den Richtlinien und
4. die Abgabe von Vertrauen an vertrauenswürdige dritte.

B2B mittels Rollen- und Trustmanagement

Die rollenbasierten Zugriffskontrolle (role-based access control, RBAC) versteht eine Rolle als eine Menge von Rechten (Permissions) und Personen die durch Mitgliedschaft in der Rolle über diese Rechte verfügen. Dieser Ansatz gibt uns die Möglichkeit die Komplexität des Trust Managements auch im B2B-Sektor beherrschbar zu machen.

Aus den typischen B2B Anwendungen ergeben sich eine Reihe von Anforderungen, die bei der Entwicklung von Mechanismen und Modellen für rollenbasierte Zugriffskontrolle zu beachten sind. Dies sind z.B. der Schutz der Anonymität der Teilnehmer, der Schutz von vertraulichen Informationen im Rollen-Modell, die Möglichkeit Rollen und Rechte zu delegieren aber auch die Möglichkeit, Rechte mit praktisch beliebig komplexen Einschränkungen zu versehen und Randbedingungen zu modellieren. Aus technischer Sicht erwarten wir eine ausreichende Skalierbarkeit je nach Komplexität der Zugriffsmodelle und die Möglichkeit, auch innerhalb einer Organisation ein solches Modell weiter zu verteilen.

Policies sind echte Handarbeit

Ein Rollenmodell muss für jede Applikation neu entworfen, implementiert und getestet werden. Jedes Stück Anwendungsfunktionalität, jede der oben genannten Anforderung und jede Randbedingung erhöht die Komplexität eines Modells. Gleichzeitig werden viele Anwendungsfälle, die im B2B-Kontext auftreten, immer wieder in ähnlicher Form in verschiedenen Applikationen und Modellen auftreten. Der Einsatz solch eines aufwändigen Schutzmechanismus ist jedoch effizient, wenn erprobte Lösungen zur Modellierung von Anwendungsfällen in neuen Modellen wiederverwendbar sind. Die Wiederverwendung von Software bzw. Quellcode wurde stets als großer Vorteil der objektorientierten Softwareentwicklung propagiert. Es hat sich allerdings gezeigt, dass es keineswegs trivial ist die richtige Abstraktionsebene der Wiederverwendung zu wählen. Auf der Ebene von Quellcode oder Bibliotheken fällt der erhoffte Produktivitätsgewinn oft der zeitraubenden Anpassung an Programmiersprachen oder Betriebsysteme zum Opfer. In den letzten Jahren hat sich das Herausarbeiten und Dokumentieren von Entwurfsmustern (Design Patterns) zu einer wichtigen Technik der Softwareentwicklung entwickelt. Dabei werden Lösungen auf konzeptioneller Ebene schematisch mit ihren Vor- und Randbedingungen dargestellt, unabhängig von den Einzelheiten der Implementierung. Ein Rollen-Modell kodiert die Informationen darüber wer in einem System welche Handlungen ausführen darf und ist somit ebenfalls ein Programm.

Wenn der Formalismus zum Erstellen eines Modells allgemein genug ist, können Teile von Modellen zumindest auf der konzeptuellen Ebene in Form von Entwurfsmustern wiederverwendet werden. Bei der Verwendung geeigneter, z.B. objektorientierter Modellierungssprachen kann auch auf dieser Ebene eine hohe Wiederverwendbarkeit erreicht werden.

Gerade bei der Modellierung von Sicherheitspolitiken bringt die Verwendung von Mustern nicht nur eine Zeit und Kostenersparnis beim Erstellen von Modellen mit sich, sondern vor allem ein Mehrgewinn an Sicherheit. Durch Einsatz getesteter und geprüfter Muster können Modellierungsfehler verhindert werden.

Ein allgemeines Vertragsmuster

Abbildung 1 illustriert einige unserer grundlegenden Ideen für Geschäftsprozesse in B2B-Systemen mit objektorientierten, verteilten RBAC-Modellen. Eine Person P möchte bei einer Firma O1 elektronisch eine Transaktion ausführen, z.B. Waren bestellen oder stornieren. Die Business-Applikation die P hierfür benutzt befragt das RBAC-Modell, um zu erfahren ob P zu dieser Aktion berechtigt ist. Das Modell enthält eine Repräsentation der Firma O1, diese beinhaltet (z.B. in Form einer Liste) mit welchen Firmen O1 Verträge geschlossen hat, die es diesen Firmen erlauben elektronische Transaktionen mit O1 durchzuführen. Für jede dieser Firmen O2 bis On enthält das Modell ein Stellvertreter-Objekt (Proxy) für die Kommunikation mit den RBAC-Modellen dieser Firmen, die über ein Netzwerk erreichbar sein müssen. Das Objekt O1 prüft zunächst ob P aufgrund ei-

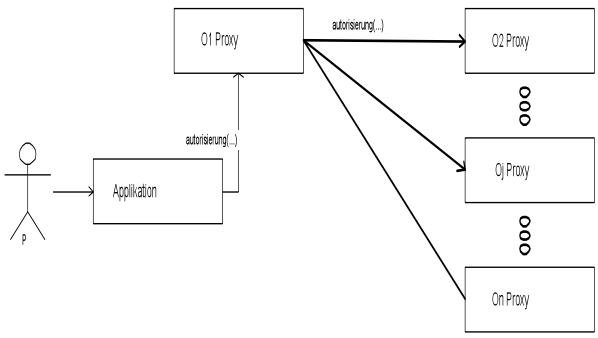

Abb. 1: Allgemeines Vertragsmuster

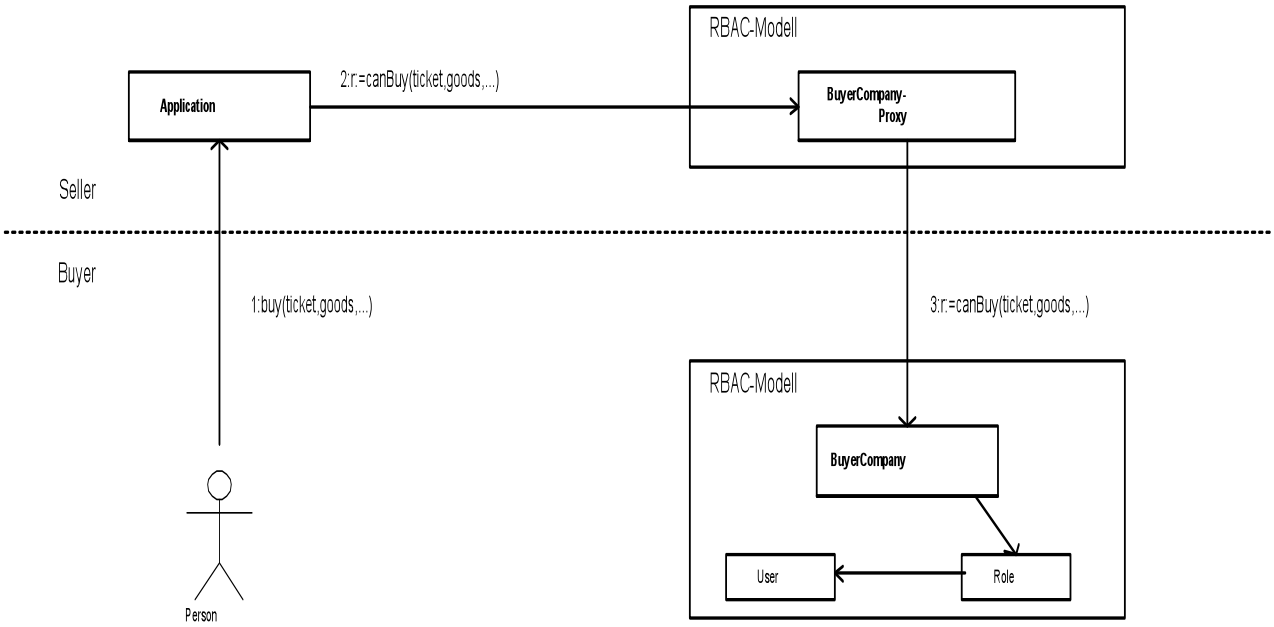

Abb. 2: Vertrags-Modell Käufer/Verkäufer

ner geschäftlichen Beziehung zur Firma O1 das Recht besitzt die Transaktion durchzuführen, z.B. weil er bei der Firma beschäftigt ist. Ist dies nicht der Fall wird die Anfrage mittels der Proxy-Objekte an die Firmen O2 bis On weitergeleitet (Broadcast). Autorisiert nun eine dieser Firmen die Transaktion, weil P bei dieser Firma in einer entsprechenden Position beschäftigt ist oder von ihr beauftragt wurde, so gestattet das Modell von O1 der Business-Applikation mit der Transaktion fortzufahren. Andernfalls wird das Modell die Autorisierungs-Anfrage negativ beantworten und die Applikation wird die Ausführung der Transaktion aufgrund der fehlenden Berechtigung von P verweigern.
Zu beachten ist hierbei das durch den Broadcast der Autorisierungs-Anfrage u.U. vertrauliche Informationen über Transaktionen in die Hände unbeteiligter Firmen gelangen. P kann der Applikation jedoch mitteilen für welche Firma er die Transaktion tätigt und so dem Modell eine gezielte Anfrage ermöglichen.

Käufer und Verkäufer

Das zentrale Vertragsmuster im B2B Bereich ist das Käufer/Verkäufer Muster. Abbildung 2 zeigt den folgenden Vorgang:

Ein Benutzer möchte eine Ware einkaufen. Er gibt den Befehl an die Applikation. Diese prüft die Autorisierung der Person zum Kaufen dieser Ware, indem sie ihr eigenes Repräsentations-Objekt im RBAC-Modell befragt. In diesem Objekt existiert eine Liste derjenigen Objekte, die eine Berechtigung zum Kaufen einer Ware vergeben können. In der Realität sind das in der Regel die Firmen, die einen Vertrag mit dem Verkäufer geschlossen haben und sich als potentielle Käufer haben eintragen lassen. Wie zuvor im allgemeinen Vertragsmuster erläutert, werden nun in zufälliger Reihenfolge alle berechtigten Objekte befragt, ob sie dem anfragenden Benutzer das Recht einräumen, die besagte Ware zu kaufen. Dabei kann die Anfrage die Bezeichnung der Ware, den Preis eine allgemeine Kategorie und beliebige weitere Informationen enthalten, die entscheidend dafür sein können, ob eine Genehmigung erteilt wird oder nicht. Innerhalb des Proxy-Objekts der befragten Organisation kann wiederum eine Reihe von Objekten (z.B. Abteilungen oder Institute) befragt werden, ob diese ein Einkaufsrecht vergeben möchte. Sobald ein Objekt das Recht vergibt, wird diese Antwort protokolliert und an die Anwendung zurückgegeben, die den Verkauf dann durchführen kann.

An dieser Stelle greifen nun weitere Techniken, wie z.B. Zeitstempelverfahren, signierte Dokumente (z.B. signed XML) usw., um eine Rechtsverbindlichkeit zu garantieren. In jedem Fall hat das Proxy-Objekt einer Organisation aber anhand der in ihm enthaltenen Modelle entschieden, ein Recht an einen Benutzer zu geben. Diese Entscheidung wird auf Grund der Rollen und die an die Rolle gebundenen Rechte getroffen, in denen der Benutzer Mitglied ist.

Warum alle Firmen befragen?

Warum nun wenden wir uns als Repräsentations-Objekt der Applikation nicht direkt an die Firma, der der Benutzer angehört und befragen diese nach dem Recht. Das Proxy-Objekt der Firma könnte sich dann sofort an das der Abteilung wenden an dem der Benutzer arbeitet usw.

Die Antwort lautet: Ja, auch das wäre möglich und unter bestimmten Umständen auch sinnvoll.

Die vorgestellte, sehr allgemeine Lösung hat jedoch den Vorteil, dass der Benutzer seine Herkunft der Applikation nicht preisgeben muss. Er könnte z.B. bei mehreren Firmen als freier Mitarbeiter arbeiten, ohne dass dies dem System bekannt sein muss oder der Benutzer mit verschiedenen Identitäten arbeiten müsste. Es wäre auch denkbar das die Firma, für die der Benutzer arbeitet im Auftrag einer anderen Firma Einkäufe zu bestimmten Zwecken tätigen kann. In diesen Fällen könnten mehrere Organisation das Recht zum Kaufen eines Gutes an den Benutzer vergeben. Der Benutzer bleibt vor dem System anonym. Lediglich durch Beobachtung der Antworten könnte z.B. der

Verkäufer herausbekommen bei welcher Firma der gegebene Benutzer wahrscheinlich angestellt ist. Durch Einführung eines Objektes zwischen der Verkäufer-Applikation und den Käuferobjekten könnte aber selbst das noch verschleiert werden.

Weitere Vertrags-Muster

Im Rahmen unserer Forschungsarbeit für Projekte, die sich dem B2B Thema widmeten konnten wir ferner Muster für ein „Vertrieb (Reseller)“, „Makler (Broker)“, „Marktplatz (Marketplace)“ und für das Einführen von „Vertrauenswürdigen Dritten (Trusted-Third-Parties)“ entwerfen. Alle diese Muster arbeiten grundsätzlich auf dem allgemeinen „Käufer/Verkäufer (Buyer/Seller)“ Muster und führen weitere Proxy-Objekte ein, die die Politik der zusätzlich eingeführten Organisationen umsetzen. Nachfolgend wird die Funktion der Vertragsmuster kurz umrissen:

- Vertrieb: Der Käufer wendet sich nicht direkt an den Verkäufer sondern an einen Vertrieb. Der Vertrieb sendet die Anfragen an den Verkäufer bzw. den Hersteller weiter. Dieser bestätigt z.B., dass die Ware zum gegebenen Preis lieferbar ist. Im weiteren Verlauf nimmt der Vertrieb gegenüber dem Verkäufer die Käufer-Rolle ein und gegenüber dem Käufer die Verkäufer-Rolle.
- Makler: Der Makler wird selbst beim Kaufprozess nicht tätig. Er vermittelt dem Käufer nur einen „passenden“ Verkäufer. Nach der Verhandlungsphase (z.B. finde einen Verkäufer der folgende Wahre zu einem Preis von maximal x anbietet) verweist der Makler auf einen Verkäufer. Im weiteren Verlauf verhalten sich Käufer/Verkäufer wie zuvor gezeigt.
- Marktplatz: Ein Marktplatz ist im Modell vor allem ein Sammler von Referenzen auf potentielle Käufer und potentielle Verkäufer. Ein Marktplatz kann die Funktion eines Vertriebs oder die eines Maklers übernehmen.

Business- vs. Access-Roles

Man kann Rollen grundsätzlich in zwei Kategorien teilen: Geschäfts-Rollen (Business-Roles) und Zugriffs-Rollen (Access-Roles). Geschäfts-Rollen sind die uns intuitiv bekannten Rollen, wie „Abteilungsleiterin“, „Sekretär“, „Designer“ oder auch „Familienvater“ oder „Hobbyschwimmer“. Diese natürlichen Rollen stehen im Kontrast zu den Rollen, die für die rollenbasierter Zugriffskontrolle von Interesse sind, nämlich die Zugriffs-Rollen.

Die Zugriffs-Rollen vereinigen Benutzer und Rechte in sich und geben so dem Mitglied in der Rolle die an sie gebundenen Rechte. Man kann diese Zugriffs-Rollen mit Hilfe von sog. Role-Engeneering-Methoden ermitteln, indem man einfach gesagt, zunächst gruppiert, welche Rechte auf eine Ressource jeweils zusammengefasst werden können und wie diese sinnvoll verknüpft werden können. Man erhält so Zugriffs-Rollen, die vor allem aus Sicht einer oder mehrerer Applikationen Sinn machen jedoch für den einfachen Benutzer nicht sofort einsichtig sind.

Wir gehen deshalb den Weg, beide Arten von Rollen in einem Modell zu vereinigen. Zum einen geben wir die Möglichkeit, die Geschäftsstruktur, mit ihren Abteilungen, Arbeitsgruppen, Ausschüssen, etc. mit Hilfe von Geschäfts-Rollen abzubilden. Auf der anderen Seite wird mittels bekannter Role-Engeneering-Methoden ein Satz von Zugriffs-Rollen erstellt. Beide Modelle werden dann miteinander verknüpft.

Der große Vorteil der sich daraus ergibt ist zum einen eine verteilte Wartbarkeit und zum anderen eine höhere Wiederverwendbarkeit des Modells.

Der Entwurf und die Implementierung von Zugriffs-Rollen ist Aufgabe eines Rollenadministrators (bei größeren Organisationen, eines Rollenadministrator-Teams). Dieser muss eng mit den Entwicklern und/oder Betreibern der Applikationen und den Systemadministratoren zusammenarbeiten.

Das Geschäfts-Modell kann anderseits von kundigen Personen aus der Geschäftsleitung oder in Kooperation mit Abteilungs-, Team- und Ausschussleitern erstellt und gewartet werden.

Das bietet z.B. die Möglichkeit, dass ein Abteilungsleiter selbst und ohne Verzögerungen, Rollen innerhalb seines Verwaltungsbereiches belegen kann. Die Rollen-Administratoren hingegen können sich um die systemnahe Verwaltung der Zugriffs-Rollen kümmern. Sie können von Personalfragen unberührt agieren.

Verteilungsmodelle

Je nach Sicherheitsanforderungen einer Organisation sind verschiedene Verteilungsmodelle der Objekte im RBAC-Modell denkbar (siehe [Hild99]). Die einfachste und heute meist verwendete Variante ist die Implementierung des Modells auf einem zentralen Rechner, der die Auswertung durchführt.

Da ein RBAC-Modell jedoch Informationen über die internen Strukturen einer Organisation und personelle Entscheidungen enthält, ist das Rollen-Modell einer Organisation als sensibel einzustufen.

Die Sichtbarkeit von Objekten und deren Inhalt sowie Referenzierung kann über das Modell selbst geregelt werden. Solange das Modell jedoch physikalisch auf der Festplatte einer anderen Organisation gespeichert ist, kann ein Missbrauch technisch gesehen nie ausgeschlossen werden.

Wird dasselbe Business-Rollen-Modell ferner für unterschiedliche Applikationen eingesetzt, die bei verschiedenen Providern laufen, stellt sich die Frage, welches Modell bei welchem Provider verwendet werden soll.

Die naheliegendste Lösung wäre, das Modell auf einem hauseigenen Server zu implementieren und die Provider der verschiedenen Applikationen darauf verweisen zu lassen.

Nicht alle Firmen im B2B Bereich verfügen jedoch über einen permanenten Internetanschluss oder die „kritische Masse“, um selbst eine eigene Rollenadministration durchführen zu können.

Sowohl die Wartung als auch das Hosting von Rollen-Modellen können prinzipiell an andere Organisationen abgegeben werden. Dabei bieten die verschiedenen Varianten unterschiedliche Sicherheitsniveaus, die sich aus der Gefährdung ergeben, andere Organisationen könnten Wissen über die internen Strukturen oder Sicherheitsrichtlinien an andere dritte weitergeben oder selbst gegen die eigene Organisation nutzen.

- Eigene Rollen-Modell-Verwaltung eigener Trust Manager Server → höchste Sicherheit
- Eigene Rollen-Modell-Verwaltung, Trust Manager Server bei vertrauenswürdigen Dritten → hohe Sicherheit, da der vertrauenswürdige Dritte idealer

Weise kein Interesse an den Daten hat, die er vorhält

- Rollen-Modell-Verwaltung und Trust Management Server bei vertrauenswürdigen Dritten → hohe Sicherheit, jedoch Abhängigkeit bei Änderungen im Modell
- Eigene Rollen-Modell-Verwaltung, Trust Manager Server bei Applikations-Anbieter → geringere Sicherheit, Schutz nur durch Rolleninterpreter, Daten können in Rohform analysiert werden
- Rollen-Modell-Verwaltung und Trust Manager Server bei Applikations-Anbieter → geringe Sicherheit, Abhängigkeit bei Änderungen im Modell, einfachstes Geschäftsmodell

Aktueller Status und Aussichten

Im Rahmen der EU Esprit Projekte E2S (End-to-End Security over the Internet) und MultiPLECX konnten wir einen prototypischen Interpreter für RBAC Modelle entwickeln, der über verschiedene Schnittstellen, wie z.B. CORBA von Applikationen als Trustmanagement-Dienst genutzt werden kann.

Dieser Dienst kann jedoch nicht nur von Applikationen genutzt werden, die für zur Verwendung des TrustManagers entworfen wurden. In weiteren Projekten gelang es, bestehende, webbasierte Dienste mit Hilfe vorgeschalteter Application-Level-Firewalls auf Webseiten-Ebene einer rollenbasierten Zugriffskontrolle zu unterwerfen.

Weitere Arbeit muss in die Modellierungssprache, den Interpreter, die Verteilung der Interpreter sowie die Anbindung an Publik-Key-Infrastrukturen (PKI) investiert werden.

Mit dem MESA System gelang es jedoch schon heute dem Schweizer Unternehmen NetUnion eine Applikation auf Basis unseres Rollen-Interpreters prototypisch zu entwickeln. Dieses System soll in den nächsten Monaten zum Einsatz kommen.

Im Rahmen des Campuskarten-Projektes der TU Berlin wird untersucht werden, wie ein rollenbasiertes Modell eine effektive und verlässliche Zugriffskontrolle auf interne und externe Ressourcen regeln kann.

Mehrwert der Nutzer

Wir sehen eine große Chance in der Verwendung von RBAC Systemen sowohl im B2B als auch im Administrationsbereich. Ist die interne Struktur einer Organisation einmal modelliert, kann dieses Modell für die Zugriffssteuerung auf die unterschiedlichsten Ressourcen genutzt werden. Dabei konnten wir bereits zeigen, wie nicht nur neue und speziell dafür entwickelte Applikationen sondern auch bereits eingeführte Intranet-/Internetdienste in ein RBAC System integriert werden können.

Was aber hat der Benutzer von einem solchen System? Wird er nun gänzlich zur anonymen Nummer im System?

Die Antwort hierauf lautet: Je nachdem, wie es dem Benutzer beliebt.

Der von uns entwickelte Interpreter erlaubt eine Administration des Modells durch verschiedene Benutzer, wobei sich hier das Modell selbst schützt, also dafür sorgt, das nur erlaubte Änderungen am Modell vorgenommen werden. So ist es mit Hilfe dieses Prinzips z.B. einem Benutzer zu erlauben, die Informationen über ihn nach außen und nach innen selbst freizugeben oder zu sperren. Mit anderen Worten: Jeder kann selbst bestimmen, wer welche Informationen über ihn erhält. Der Benutzer unterliegt hier nur den Restriktionen und Sicherheitsrichtlinien seiner Firma, die ggfs. die Freigabe bestimmter Informationen nicht gestattet oder prüft. Dies ist jedoch keinesfalls ein Rückschritt. Der Benutzer kann in dem von uns beschriebenen System als mündiger Bürger selbst entscheiden und im Rahmen der ihm gesetzten Grenzen handeln.

Fazit

Die Verwendung rollen-basierter Zugriffssysteme in Kombination mit konsequenter Anwendung von Techniken, die aus dem Bereich mehrseitige Sicherheit bekannt sind, eröffnet vielfältige Möglichkeiten im Bereich Business-to-Bussiness sowie im administrativen Bereich.

> Bei der Erstellung von rollenbasierten Zugriffsmodellen können die aus der Software-Technik bekannten Techniken zur Wiederverwendung insbesondere auf der Ebene der Design-Patterns verwendet werden, was neben einer Zeit- und Kostenersparnis vor allem zur höheren Verlässlichkeit und Sicherheit solcher Modelle führen kann.

Aus Benutzersicht bietet die Verwendung von zentralisierten rollen-basierten Zugriffssystemen vor allem die Option der Konfiguration der eigenen Sicherheitsrichtlinien innerhalb der von der übergeordneten Organisation vorgegebenen Grenzen.

> Für den Benutzer besteht bei Verwendung eines solchen Systems die Möglichkeit einer für ihn transparenten Trust Management Konfiguration seiner persönlichen Daten.

Literatur

[Bart98] J. Bartholdt, K. Nagel: *Smart Card gesicherte Web-Umgebung und rollenbasierte Zugriffskontrolle im administrativen Bereich*, Teil 1 des Beitrages: „Abgesicherte Internet-Umgebungen mit Hilfe rollenbasierter Zugriffsmechanismen für WWW- und Email-Dienste“, 5. Workshop: Sicherheit in vernetzten Systemen des DFN-CERT und DFN-PCA, Hamburg, 4.-5. März 1998

[Blaze96] Matt Blaze et al.: *Decentralized Trust Management*, Proceedings 1996 IEEE Symposium on Security and Privacy, May, 1996

[Busch96]F. Buschmann, et al.: *Pattern-Oriented Software Architecture. A System of Patterns*, John Wiley & Sons, Ltd, 1996

[Gam96] E. Gamma, R. Helm, R. Johnson, J. Vlissides, *Entwurfsmuster*, Addison-Wesley, Bonn 1996

[Hild99] T. Hildmann, J. Bartholdt: *Managing Trust between collaborating Companies using outsourced Role Based Access Control*, Fourth ACM RBAC Workshop, October 28-29, 1999

[Ran97] Kai Rannenberg et al.: *Sicherheit, insbesondere mehrseitige IT-Sicherheit*, aus Mehrseitige Sicherheit in der Kommunikationstechnik, Addison-Wesley-Longmann, 1997

[Sand96] R.S. Sandhu et al., *Role-Based Access Control Models*, IEEE Computer, pp. 38-47, February, 1996

[Waid98] Michael Waidner: *Open issues in secure electronic commerce*, RZ 3070 (\#93116), IBM Research, October, 1998