Modellierung standortabhängiger Zugriffskontrollen für mobil unterstützte Prozesse

Dipl.-Inform. Nikolai Krambrock

Bereich Informationsmanagement
Forschungsinstitut für Rationalisierung (FIR) an der RWTH-Aachen e.V.
Pontdriesch 14/16
52062 Aachen
nikolai.krambrock@fir.rwth-aachen.de

Abstract: Mit mobilen Computern lassen sich Geschäftsprozesse unterstützen und Aufgaben auf Mitarbeiter vor Ort übertragen. Neben den offensichtlichen Nutzen bergen solche Lösungen auch Risiken: Vor allem können Bezugsobjekte verwechselt werden – Fehlbedienungen oder -steuerungen sind die Folge. Der Artikel schlägt vor, diesen Risiken mit ortsabhängigen Zugriffskontrollen zu begegnen und zeigt erste Ansätze zur deren Modellierung.

1 Problemstellung und Hintergrund

Immer mehr und immer kritischere Prozesse werden mit mobilen Computern unterstützt. Mit ihnen werden Dokumentationen angefertigt, Informationen beschafft und Prozesse gesteuert. Der Nutzen solcher Lösungen liegt auf der Hand: Die vor Ort angefertigte Dokumentation muss nicht erneut erfasst werden, die Informationsbeschaffung mit mobilen Endgeräten ersetzt telefonische Recherchen und auch die Steuerung kann direkt und effizient durchgeführt werden.

Dem Produktivitätsgewinn stehen aber auch neue Risiken gegenüber: Der Benutzer eines mobilen Computers kann leicht auf falsche Bezugsobjekte zugreifen; Fehlinformationen oder -steuerungen sind die Folge. Das Forschungsprojekt SimoKIM am FIR betrachtet den Einsatz mobiler Computer beim kommunalen Infrastrukturmanagement. So wird z.B. überprüft, ob die Gaszufuhr bei der Reparatur einer Leitung direkt durch den Instandhaltungsmitarbeiter aus- und wieder eingeschaltet werden kann. Die Folgen einer versehentlich abgestellten Gasleitung beschränken sich auf verärgerte Bewohner, beim Aktivieren einer falschen Gasleitung ist das Risiko weit größer.

Ähnliche Herausforderungen ergeben sich in der Logistik: Wie kann beispielsweise festgelegt und durchgesetzt werden, wo und unter welchen Bedingungen Gefahrgutbehälter geöffnet werden sollen? Auch in der Logistik entstehen mit den zusätzlichen Informations-, Dokumentations-, und Steuerungsmöglichkeiten neue Risiken.

Solchen Risiken kann mit einem effektiven Zugriffsschutz begegnet werden. Zwei Anforderungen muss dieser erfüllen:

- Er muss sich am Prozess der Aufgabenerfüllung orientieren, also nur solche Funktionen zulassen, die zur Erfüllung der jeweiligen Aufgabe notwendig sind und
- er muss Ortsinformationen einbeziehen, um die Aufgabenerfüllung nur am Ort der jeweiligen Aufgabe zuzulassen.

2 Analyse bestehender Ansätze

2.1 Bedeutung von Zugriffskontrollen für die IT-Sicherheit

Zugriffsschutz für Geschäftsprozesse (z.B. in betrieblichen Informationssystemen) wird meist mit Role Based Access Control (RBAC) realisiert; vgl. [Ec06], S. 245. Die Grundidee hinter RBAC ist einfach: Benutzern werden Zugriffsrechte nicht direkt zugewiesen. Stattdessen erhalten sie zur Erfüllung bestimmter Aufgaben und Positionen Bündel von Berechtigungen, genannt Rollen. Auf Basis dieses Konzepts können organisatorische Strukturen eines Unternehmens in Zugriffsrechten abgebildet werden; vgl. [Cl06], S. 26. Abbildung 1 zeigt das weit verbreitete ANSI Core RBAC; vgl. [AN04].

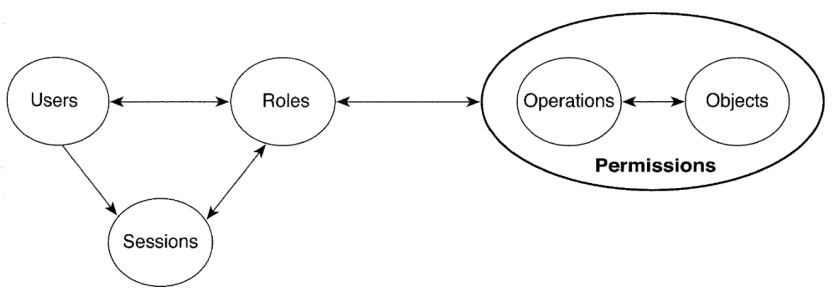

Abbildung 1: Elemente eines vereinfachten RBAC Modells aus [Cl06], S. 18

2.2 Modellierung von Zugriffskontrollen aus Geschäftsprozessen

Die Herausforderung bei der Anwendung des RBAC-Modells liegt in der Definition geeigneter Rollen. [Sc00], S. 2 geht bei großen Produktivsystemen von mehreren Millionen Einzelberechtigungen aus, die ein Benutzer potentiell haben kann. Gleichzeitig kann ein einziger Fehler zu einem unsicheren System führen. Wissenschaftliche Artikel wie [Sc00], [CIN03] schlagen daher ein systematisches Vorgehen unter dem Namen Role-Engineering vor.

2.3 Ortsabhängige Zugriffskontrollen

Location Based Services stellen Informationen in Abhängigkeit einer geografischen Position zur Verfügung. So wird z.B. über touristische Attraktionen in der Nähe per SMS informiert. Bestehende Services machen den Zugriff auf spezifische Informationen ausschließlich vom Ort abhängig, nicht von anderen Berechtigungen oder Rollen. Dieses Vorgehen ist bei der Suche nach touristischen Attraktionen durchaus angemessen. Für den Anwendungsfall sicherheitsrelevanter und vertraulicher Informationen sowie kritischer Steuerungsmöglichkeiten ist dieses Vorgehen inakzeptabel; vgl. [BCD05]. Daher schlagen aktuelle Forschungsberichte vor, das RBAC Modell um Ortsinformationen zu erweitern; vgl. [RY05], [ACD06], [BCD05]. Die Komplexität des Modells nimmt dabei erheblich zu: vgl. Abbildung 1 mit Abbildung 2.

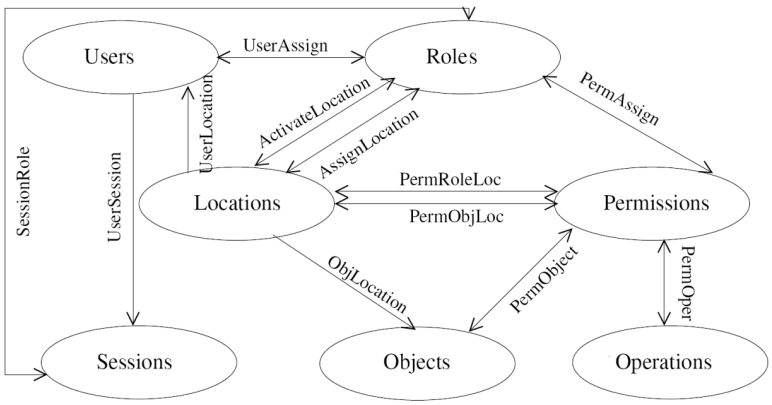

Abbildung 2: Um Ortsinformationen erweitertes RBAC-Modell aus [RY05]

Mit der Komplexität des Modells nimmt auch die Komplexität der Modellierung zu: Es ist detailliertes Wissen um den Geschäftsprozess notwenig, um bestimmen zu können, wann Informationen bzw. Steuerungsmöglichkeiten zur Verfügung gestellt werden sollen. Ein strukturiertes Vorgehen bei der Modellierung ist daher noch bedeutsamer, als bei nicht ortsabhängigen Zugriffskontrollen. Um eine korrekte Umsetzung von Sicherheitsanforderungen zu unterstützten, muss diese Methode zwei Anforderungen erfüllen: Einfache Transformation eines dokumentierten Geschäftsprozesses in Zugriffskontrollen und Berücksichtigung von Ortsinformationen beim Zugriff.

3 Ziel der Arbeit

Im Forschungsprojekt SimoKIM und einer damit verbundenen Dissertation wird eine Methode entwickelt, mit der ortsabhängige Zugriffskontrollen aus dokumentierten, mobil unterstützten Prozessen abgeleitet werden können. Die Methode soll verschieden hohe Sicherheitsanforderungen unterstützen. Ergebnis der Arbeit ist damit ein Vorgehen zur Ableitung von Zugriffsrechten, auch bekannt als Role-Engineering.

4 Lösungshypothese und Vorgehen

Thema des Vorhabens ist das Role-Engineering für ortsabhängige Zugriffskontrollen. Es liegen sowohl Methoden zum Role-Engineering als auch erste Modelle zur Abbildung von Rollen für ortsabhängige Zugriffskontrollen vor; vgl. Kapitel 2 und Abbildung 3. Daher wird sich die Arbeit an diesen Erkenntnissen orientieren.

	Rollen-Modell	Vorgehen (Role-Engineering)
Nicht ortsabhängige Zugriffskontrollen	Umfangreich bearbeitetes Forschungsthema; Standards vorhanden (z.B. [AN04], [Cl06])	Gut bearbeitetes Forschungsthema; Methoden und dokumentierte Anwendungen vorhanden (z.B. [Sc00], [CIN03])
Ortsabhängige Zugriffskontrollen	Neues Forschungsthema; Thesen für Methoden und praktische Anwendungen ohne methodisches Vorgehen liegen vor (z.B. [RY05], [ACD06], [BCD05])	Dissertationsthema: Kaum Arbeiten vorhanden; allenfalls Empfehlungen innerhalb von Rollen-Modellen

Abbildung 3: Einordnung des Forschungsthemas

Abbildung 4 zeigt die verschiedenen Themen der geplanten Arbeit als logische Schritte bei der Entwicklung des Modells: In den ersten drei Schritten werden bestehende Erkenntnisse analysiert, ausgewählt und für die Arbeit angepasst. Im vierten Schritt wird die Methode zum Role-Engineering für ortsabhängige Zugriffskontrollen entwickelt.

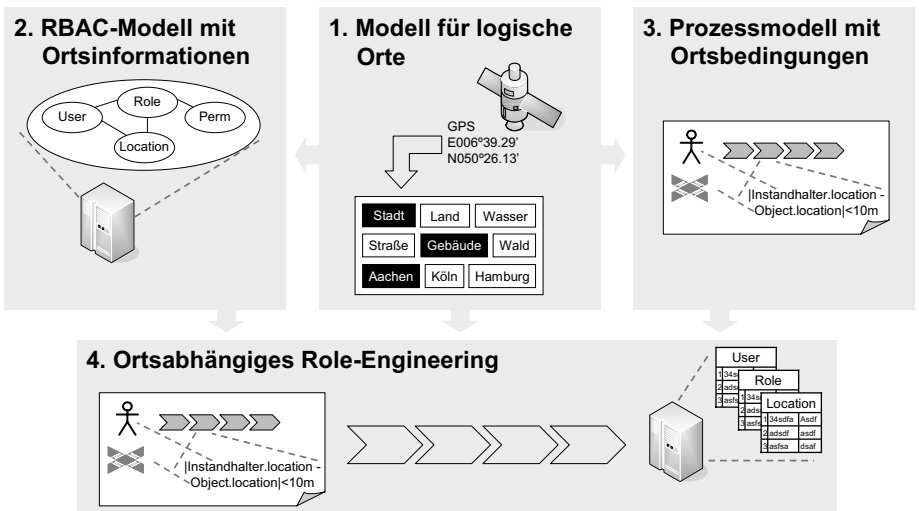

Abbildung 4: Logische Schritte im Design der geplanten Methode

4.1 Ortsabhängige Zugriffskontrollen

Zur Darstellung von Ortsinformationen für Zugriffskontrollen existieren erste Ansätze. Mit Hilfe detaillierter Karteninformationen werden logische Positionen abgeleitet. Solche Positionen können „auf der Straße“, „in der Luft“ oder „auf freiem Feld“ aber auch eine spezifische Stadt sein. Daneben ist die relative Position von einem Benutzer und einem Objekt wichtig zur Vergabe von Zugriffsrechten.

4.2 Auswahl eines RBAC-Modells, das Ortsinformationen berücksichtigt

Durch Auswahl oder Anpassung wird ein Modell zur weiteren Verwendung in der geplanten Arbeit festgelegt. Das Modell darf zur Definition von Rollen keine frei formulierbaren Formeln verwenden, sondern muss mit Verknüpfungen zwischen Entitäten auskommen. Formeln verhindern die einfache Verifikation der Zugriffsrechte; eine darauf aufbauende Methode wäre somit zum Einsatz in großen Systemen wenig geeignet.

4.3 Auswahl eines geeigneten Prozessmodells und Integration von Ortsbedingungen

In der geplanten Arbeit wird ein Modell ausgewählt und um räumliche Bedingungen ergänzt. Diese werden formal und möglichst so formuliert, dass die Übertragung der räumlichen Bedingungen auf die Rollen ohne weitere Umformungen möglich ist.

4.4 Auswahl eines geeigneten Prozessmodells und Integration von Ortsbedingungen

In Analogie zu bestehendem Role-Engineering wird die geplante Methode entwickelt. Diese muss auf höhere Komplexität ausgelegt sein, denn der mobil unterstützte Prozess und dessen Dokumentation sind aufgrund zusätzlich eingesetzter Technologie und den zusätzlichen Ortsinformationen komplexer.

Literaturverzeichnis

[ACD06] ARDAGNA, Claudio A. ; CREMONINI, Marco ; DAMIANI, Ernesto ; VIMERCATI, Sabrina De Capitani di ; SAMARATI, Pierangela: Supporting location-based conditions in access control policies. New York, NY, USA: ACM Press, 2006.

[AN04] ANSI: American National Standard for Information Technology - Role Based Access Control. New York: American National Standards Institute Inc., 2004.

[BCD05] BERTINO, Elisa ; CATANIA, Barbara ; DAMIANI, Maria Luisa ; PERLASCA, Paolo: GEO-RBAC: a spatially aware RBAC. New York, NY, USA: ACM Press, 2005.

[CIN03] CROOK, Robert ; INCE, Darrel ; NUSEIBEH, Bashar: Modelling Access Policies Using Roles in Requirements Engineering. In: Information and Software Technology 45 (2003) Nr. 14, S. 979-991.

[Cl06] CLARK, Ian: An Introduction to Role-Based Access Control. In: TIPTON, Harold F. ; KRAUSE, Micki (Hrsg.): Information Security Management Handbook. Auerbach Publishers Inc., 2006, S. 17-29.

[Ec06] ECKERT, Claudia: IT-Sicherheit. 4. Auflage. Oldenbourg Wissenschaftsverlag, 2006.

[RY05] RAY, Indrakshi ; YU, Lijun: Short Paper: Towards a Location-Aware Role-Based Access Control Model. SECURECOMM'05: First International Conference on Security and Privacy for Emerging Areas in Communications Networks, 2005. IEEE, 2005, S. 234-236.

[Sc00] SCHIMPF, Gerhard: Role-Engineering Critical Success Factors for Enterprise Security Administration. 2000.