UNIVERSITÄT
KOBLENZ · LANDAU
Institut für Wirtschafts- und Verwaltungsinformatik

FB 4
Informatik

Rollenbasierte Zugriffskontrolle (RBAC) im Gesundheitswesen

Rüdiger Grimm
Anastasia Meletiadou

Nr. 15/2007

Arbeitsberichte aus dem Fachbereich Informatik

Universität Koblenz-Landau • Campus Koblenz • Universitätsstraße 1 • 56070 Koblenz
Telefon +49 261 287-0 • http://www.uni-koblenz.de

Arbeitsberichte des Fachbereichs Informatik

ISSN (Print): 1864-0346
ISSN (Online): 1864-0850

Herausgeber / Edited by:

Der Dekan:
Prof. Dr. Paulus

Kontaktdaten der Verfasser

Rüdiger Grimm, Anastasia Meletiadou
Institut für Wirtschafts- und Verwaltungsinformatik
Fachbereich Informatik
Universität Koblenz-Landau
Universitätsstraße 1
D-56070 Koblenz
EMail: grimm@uni-koblenz.de; nancy@uni-koblenz.de;

Rollenbasierte Zugriffskontrolle (RBAC) im Gesundheitswesen

Abstract

Im Gesundheitswesen geht es nicht nur um die Vertraulichkeit von Patientendaten, sondern auch um ihre Integrität, von der die richtige Behandlung und Pflege des Patienten abhängen. Eine Maßnahme zur Absicherung eines Krankenhausinformationssystems (KIS) gegen unautorisierte Angreifer ist eine flexibel organisierte Zugriffskontrolle zum Schutz der patientenbezogenen Daten. Dieser Artikel beschreibt das Konzept einer rollenbasierten Zugriffskontrolle (RBAC – Role Based Access Control) und seine Einsatzmöglichkeiten im Gesundheitswesen.

1 Sicherheit und Zugriffskontrolle

Personenbezogene Daten im Gesundheitswesen gelten als besonders sensibel. Dies zeigt der jüngste publizistische Wirbel um den Fall einer Krankenschwester, deren Laptop mitsamt Informationen über 28.000 Patienten gestohlen wurde. Die Daten waren zwar verschlüsselt, jedoch lagen Benutzerkennung und Passwort dem Gerät bei [Sil2006]. In einem netzbasierten Content Management System wäre das kaum passiert, da dort die Inhaltsdaten gut gesichert im Netz und nicht auf den Laptops der Nutzer liegen. Wie aber sichert man ein Anwendungssystem im Netz?

Wenn man Insider-Angriffe ausschließen kann, dann kann man mit einer aufgabengetreuen Zugriffskontrolle die Sicherheit eines Anwendungssystems (wie eines Krankenhaus-informationssystems) auf die Verantwortung seiner autorisierten Nutzer abstützen. Der Schutz vor unautorisiertem Zugriff hält die Daten nicht nur vertraulich, sondern auch integer im Sinne ihrer berechtigten Bearbeiter. Auch die Verfügbarkeit wäre vor unautorisiertem Ressourcenmissbrauch geschützt.

Zugriffskontrollregeln legen fest, wer welche Rechte in einem IT-System hat und bei welchen Aktionen welche Überprüfung durchzuführen ist. Zugriffskontrollmechanismen werten die Regeln im Betrieb aus und wehren dadurch unautorisierte Zugriffe ab. Bei der Vergabe von Zugriffsrechten spricht man von Subjekten (Benutzern oder Applikationen), die Zugriff auf Objekte (z. B. Dateien oder weitere Applikationen) erhalten [HoPr2003]. Benutzer und Applikationen agieren in System- und Anwendungsprozessen als *Clients,* hier Subjekte genannt.

Die Vergabe von Zugriffsrechten kann man aus zwei Perspektiven sehen [Sch2000]:

- Aus Sicht eines Subjekts: Welche Berechtigungen hat dieses Subjekt, z. B. Löschen eines Patientendatensatzes?
- Aus Sicht eines Objekts: Welche Operationen sind mit diesem Objekt erlaubt, z. B. Lesen, Schreiben, Kreieren, Löschen?

So unterscheidet Unix (und viele der davon abgeleiteten Betriebssysteme) drei Zugriffsarten, *read*, *write* und *execute*. Diese sind voneinander unabhängig, d.h. jemand kann das Recht haben, eine Datei zu lesen, darf diese aber nicht verändern. Windows NT und dessen Nachfolger erlauben eine weitere Differenzierung von Zugriffrechten. So kann beispielsweise gesteuert werden, ob ein Benutzer einzelnen anderen Benutzern Rechte an einer Datei geben darf (*change permissions*, *change ownership*). Zusätzlich werden Rechte für den Zugriff auf die Attribute einer Datei (z. B. Modifikationsdatum) unterschieden vom Zugriff auf die Datei selbst.

Es gibt prinzipiell drei Konzepte für Zugriffskontrolle [HoPr2003] [Sch2000]:

- ***Discretionary Access Control (DAC):*** Die Zugriffsrechte auf Objekte werden für jedes Subjekt einzeln festgelegt. So ist es unter anderem möglich, dass der Eigentümer eines Objekts nach seinem Ermessen anderen Subjekten Rechte erteilt. Dieses Konzept wurde erstmals von B.W. Lampson formuliert [Lam1971].
- ***Mandatory Access Control (MAC):*** Hier werden Regeln für die Berechtigungen der Subjekte systemgesteuert eingeführt und durchgesetzt. Diese Regeln basieren auf einer Klassifizierung der Subjekte und Objekte in Sicherheitsklassen je nach Sensibilität der Daten. Dieses Konzept wird im Bell-LaPadula-Modell eingesetzt [BePa1973].
- ***Role-Based Access Control (RBAC):*** Zugriffsrechte werden unabhängig von Subjekten zu so genannten Rollen zusammengefasst. Eine Rolle ist eine Zusammenstellung von Berechtigungen, die zur Erfüllung spezifischer Aufgaben benötigt werden. Hierbei können Subjekte mehrere Rollen haben. Dieses Konzept stammt ursprünglich von Ferraiolo und Kuhn [FeKu1992].

2 Zugriffskontroll-Modelle

Die beschriebenen grundsätzlichen Strategien können durch strukturierte Modelle konkretisiert werden. Beispiele dafür sind die Zugriffsmatrix, das Bell-LaPadula-Modell und das rollenbasiertes Modell. Diese drei sollen in den folgenden Abschnitten vorgestellt werden.

2.1 Zugriffsmatrix-Modell (DAC)

Das Zugriffsmatrix-Modell nach Lampson [Lam1971] definiert die Objekte und Subjekte eines IT-Systems und legt für jedes Subjekt und jedes Objekt die vorhandenen Zugriffsrechte fest. Diese Zuordnung wird in Form einer Matrix abgebildet (Abbildung 1).

	Datei 1	Applikation 1	Applikation 2
Benutzer 1	lesen, schreiben		
Benutzer 2	lesen	ausführen	
Applikation 1			ausführen

Abbildung 1 Zugriffsmatrix

Die Zeilen entsprechen den Subjekten, die Spalten den Objekten. Die Zellen der Matrix enthalten die Zugriffsrechte.

Die Zugriffsmatrix ist eine komfortable Art der Zugriffskontrolle, da hier sowohl Objekte als auch Subjekte frei festlegbar sind. Somit kann man das IT-System so modellieren, dass die vorgegebenen Sicherheitsanforderungen erfüllt werden. Die direkte Zuordnung von Subjekt und Objekt kann allerdings zu Inkonsistenzen führen, beispielsweise wenn ein Benutzerkonto gelöscht werden soll, weil der entsprechende Mitarbeiter entlassen wurde [Sch2000] [Eck2005].

2.2 Bell-LaPadula Modell (MAC)

Das Bell-LaPadula-Modell definiert Subjekte, Objekte, Zugriffsoperationen und formale Methoden zur Beschreibung von Beziehungen [Sch2000]. Bell-LaPadula erhält zwei wesentliche Regeln [HoPr2003]:

- ***No read up:*** Subjekte dürfen nur Objekte der gleichen oder einer geringeren Sicherheitsstufe lesen.
- ***No write down:*** Subjekte dürfen nur Objekte der gleichen oder einer höheren Sicherheitsstufe schreiben.

Diese Regeln stellen sicher, dass kein Informationsfluss aus einer höheren in eine niedrigere Stufe erfolgen kann. Obwohl dieses Modell in der Praxis eingesetzt wird und großen Einfluss auf die standardisierten Sicherheitskriterien hat, ist es nur sehr begrenzt und umständlich anwendbar. Zum Beispiel kann ein Subjekt einem niedriger eingestuften Subjekt kein Objekt

zum Lesen zukommen lassen, damit sind etwa Weisungen an Mitarbeiter mit Bell-LaPadula nicht direkt ausdrückbar.

2.3 Rollenbasiertes Modell (RBAC)

Seit dem ursprünglichen Entwurf von Ferrariolo und Kuhn [FeKu1992] sind unterschiedliche Modelle und Applikationen eingeführt worden, die das RBAC-Konzept umsetzen [FeSa et al. 2001]. In RBAC werden individuelle Subjekte und aufgabenbezogene Rollen getrennt. Berechtigungen zur Nutzung von Objekten werden an Rollen, nicht an individuelle Subjekte gebunden. Subjekte werden erst anhand ihrer konkreten und oft wechselnden Aufgaben Rollen zugeordnet. Die Spezifikation von Rollen mit ihren Rechten ist die Aufgabe des Anwendungsdesigns. Die Zuordnung von Subjekten zu Rollen ist die Aufgabe des Betriebsmanagements.

Das Konzept eines rollenbasierten Modells wird in der folgenden Abbildung dargestellt. Die Benutzer 4 bis 6 (Subjekte) sind der Rolle 1 zugeordnet und dürfen deshalb bestimmte Transaktionen (trans_a bzw. trans_b) auf die Datei 1 (Objekt) und Applikation 1 (Objekt) durchführen. [FeKu1992]

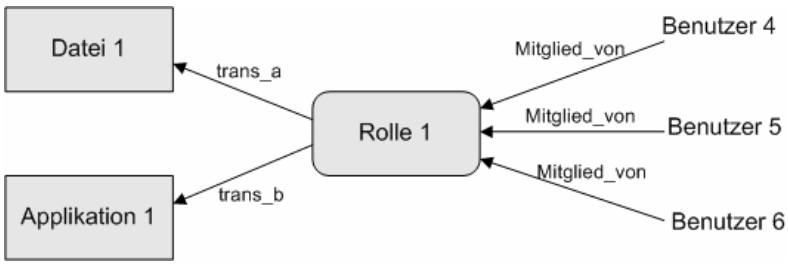

Abbildung 2 RBAC nach [FeKu1992]

Ein rollenbasiertes Sicherheitsmodell wird als Tupel aus sieben Elementen definiert [Eck2005]:

$$RBAC = (S,O,R,P,sr,pr,session)$$

S ist die Menge der Subjekte im System, *O* ist die Menge der zu schützende Objekte, *R* ist die Menge von Rollen. Jede Rolle legt die Berechtigungen der Rollenmitglieder fest. Dass die Berechtigungen aufgabenbezogen korrekt spezifiziert sind, ist die Verantwortung des Anwendungsdesigns und liegt außerhalb der systemunterstützten RBAC-Kontrolle. *P* ist die Menge der Zugriffsberechtigungen. Der Einfachheit halber umfassen hier die Zugriffsberechtigungen $p \in P$ Objekte *und* Zugriffsarten. $p=(o,x) \in P$ bedeutet also, dass die Zugriffsberechtung *p* darin besteht, dass auf das Obkjekt $o \in O$ (z.B. eine Personalakte) mit der Aktion *x* (z.B. lesen) zugegriffen werden darf. *sr, pr* und *session* sind Relationen. Diese werden folgendermaßen definiert:

sr ordnet jedem Subjekt diejenigen Rollen zu, die es ausüben darf.

$$sr : S \rightarrow 2^R \qquad \textit{(Rollenmitgliedschaft)}$$

Mit $sr(s) = \{r_1, \ldots, r_n\}$ ($r_i \in R$) wird angegeben, dass das Subjekt *s* die Rollen r_1 bis r_n annehmen darf.

pr ordnet jeder Rolle ihre Zugriffsberechtigungen zu.

$$pr : R \rightarrow 2^P \qquad \textit{(Berechtigung)}$$

pr ist eine Abbildung, die jeder Rolle $r \in R$ eine Menge an Zugriffsrechten zuordnet. Mit $pr(r) = \{p_1, \ldots, p_n\}$ ($p_i \in P$) wird angegeben, dass jedes Subjekt in der Rolle *r* die Zugriffsrechte p_1 bis p_n hat. Die *erlaubte* Zuordnung von Subjekten zu Rollen wird in der *sr*-Abbildung definiert. Die *tatsächliche* Ausübung von Rollen durch Subjekte wird in der *session*-Relation beschrieben. In der hier vorgestellten Form des RBAC kann sich ein Subjekt in unterschiedlichen Sitzungen befinden und dabei unterschiedliche Rollen annehmen. Dies wird folgendermaßen ausgedrückt:

$$session \subseteq S \times 2^R \qquad \textit{(Sitzung)}$$

Im Unterschied zu *sr* gibt *session* an, in welchen Rollen ein jedes Subjekt *derzeit* aktiv ist. Die Relation *session* ändert sich dynamisch im Laufe des Betriebs in dem Maße, in dem Subjekte (im Rahmen ihrer Berechtigungen gemäß *sr*) neue Rollen annehmen oder bestehende Rollen aufgeben. Für $s \in S$ bedeutet also $(s, r_2, r_7) \in session$, dass das Subjekt *s* derzeit in den Rollen $r_2 \in R$ und $r_7 \in R$ aktiv ist. Die Zusammenhänge zwischen Benutzern, Rollen, Rechten und Sitzungen werden in Abbildung 3 illustriert.

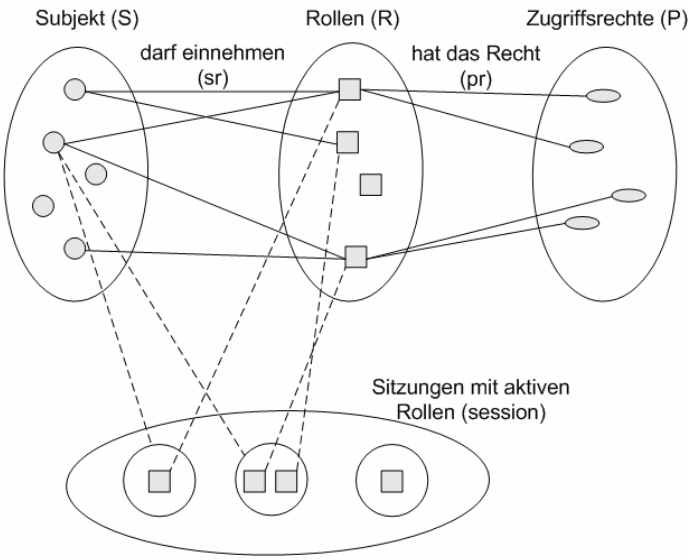

Abbildung 3 RBAC nach [Eck2005]

Mit Hilfe von RBAC sind die folgenden zwei wichtigen Sicherheitsprinzipien gut umsetzbar [FeKu1992]:

- Das Prinzip der minimalen Rechte (*Least Privilege*, *Need-to-Know*) fordert, dass ein Benutzer gemäß seiner Aufgabe nur so viele Rechte zugewiesen bekommt, wie zur

Erfüllung dieser Aufgabe unbedingt nötig sind. Das ist gut mit der Lampson-Matrix umsetzbar, in der statt individueller Subjekte Rollen stehen.

- Das Prinzip der Aufgabentrennung (*Separation of Duty*) [ClWi1987] verhindert, dass einzelne Subjekte sensible Aufgaben missbrauchen können. Die Aufgabentrennung spezifiziert Mengen von sensiblen Transaktionen, die nicht ein einzelner Benutzer alle ausführen kann. Beispielsweise sollte für die Transaktionsmenge „Auszahlung“ und „Auszahlung genehmigen“ sichergestellt werden, dass nur *unterschiedliche* Benutzer diese Transaktionen durchführen dürfen. Die Aufgabentrennung wird bei RBAC auf Rollen bezogen, wobei zusätzlich darauf zu achten ist, dass ein Subjekt nicht in derart getrennten Rollen gleichzeitig tätig sein darf.

Es gibt viele Varianten des RBAC-Modells mit unterschiedlichen Ausprägungen, z. B. [SaCo et al.1996] [FeSa et al. 2001] [ZhAhCh2003]. Eine wichtige Erweiterung ist dabei die Hierarchisierung der Rollen durch eine partielle Ordnung: Wenn R_1 und R_2 Rollen sind mit $R_1 \leq R_2$, dann besitzen die Mitglieder der Rolle R_2 mindestens auch alle Rechte von R_1 [Eck2005] [SaCo et. al.1996] [FeSa et al. 2001].

Möchte ein Benutzer (eine Person oder eine Applikation) eine Transaktion durchführen, muss sie sich nach dem RBAC-Modell zunächst als Subjekt in das System einloggen und dann eine Rolle übernehmen, für die vor jedem Zugriff auf die Transaktionsobjekte die angefragten Rechte geprüft und zugewiesen werden. Der wesentliche Vorteil des RBAC-Modells gegenüber Zugriffsmodellen individueller Nutzer liegt in der Trennung zwischen Rechten (in Rollen) und ihren ausübenden Subjekten. Mit dieser Trennung kann die langfristige Aufgaben*beschreibung* mit ihrer systemischen Implementierung flexibel getrennt werden von der kurzfristigen Aufgaben*organisation* und ihrer dynamischen *Ausführung*:

- Erstens spezifiziert der Anwendungsdesigner Aufgaben und zugehörige Rollen mit ihren Rechten. Das geschieht beim ersten Entwurf und bei einer Neuorganisation einer Aufgabe und bleibt ansonsten stabil im laufenden Betrieb. Dabei beachtet er die Prinzipien der minimalen Rechte und der Aufgabentrennung.
- Zweitens ordnet der Projektorganisator konkreten Subjekten Rollen zu. Das geschieht immer dann, wenn ein neues Subjekt im System angelegt wird oder ein Subjekt in eine andere Rolle wechselt. Diese Zuordnung erfolgt i.d.R. nach den organisatorischen Strukturen eines Unternehmens. Bei der Mehrfachzuordnung von Rollen zu Subjekten dürfen die Prinzipien der minimalen Rechte und der Aufgabentrennung nicht unterlaufen werden.
- Drittens schließlich sorgt das laufende RBAC-Betriebssystem bei der Durchführung einer Aufgabe für die Wahrung der Zugriffsrechte und verhindert dadurch unautorisierten Missbrauch der Daten und Resourcen.

Durch die getrennte Beschreibung ist dieses Modell leichter zu pflegen, wenn sich Änderungen in den Aufgaben der Benutzer ergeben. Wird zum Beispiel ein externer Berater für kurze Zeit in ein Unternehmen beschäftigt, kann ihm eine entsprechende Rolle kurzfristig zugewiesen und danach wieder entzogen werden. Würde man ein System ohne Rollen verwenden, müssten die Rechte an allen betroffenen Objekten geändert werden – eine aufwändige und fehlerträchtige Vorgehensweise.

3 RBAC im Gesundheitswesen

Missbrauch von Patientendaten kann für ein Krankenhaus einen erheblichen Imageverlust und finanzielle und rechtliche Probleme zur Folge haben. Der Patient muss um seine Privatsphäre und möglicherweise sogar um die Integrität seiner Behandlung fürchten.

Aufgrund seiner Struktur mit seinen vielen Akteuren in ihren unterschiedlichen Aufgaben ist das Gesundheitswesen prädestiniert für die Anwendung des RBAC-Modells [FeKu1992] [Cha2001] [EvBo2004]. Der gleiche Mitarbeiter arbeitet in unterschiedlichen Zeitperioden in unterschiedlichen Abteilungen und Aufgaben und benötigt dabei Zugriff auf vielerlei Informationen über den Patienten. Nicht nur Ärzte und Pflegepersonal agieren in wechselnden Rollen, sogar der Wechsel zwischen Personal und Patientenrolle ist möglich. Entsprechend sind die Informationen über den Patienten in geeignet zu separierenden Kategorien mit ihren jeweiligen Zugriffsrechten einzuteilen.

3.1 Objekte im Krankenhausbetrieb

In einem Krankenhaus-Informationssystem (KIS) werden einerseits langfristige Personenstammdaten (Name, Adresse, Geschlecht) und Daten zur Krankheitshistorie einer Person (Allergie, Blutgruppe, Hausarzt) festgehalten. Andererseits werden Daten erfasst und laufend bearbeitet, die erst im Krankenhaus und durch seine Aktivitäten entstehen und sich verändern, wie z. B. behandelnder Arzt, Medikation, einzuhaltende Diät, Abrechnungsdaten.

3.2 Rollen im Krankenhausbetrieb

Gemäß der Aufgabenteilung des Personals sind Rollen mit ihren Rechten und ihrem Zusammenspiel im Krankenhaus festzulegen. Die Fallstudie von [EvBo2004] identifiziert einige Rollen im australischen Gesundheitswesen, die für Deutschland mit gewissen Anpassungen übernommen werden können. Sie werden im Folgenden sehr vereinfacht dargestellt, um das Prinzip einer RBAC-Anwendung im Krankenhaus hervorzuheben, sie müssten aber für einen realen Krankenhausbetrieb erheblich verfeinert werden:

- Ein ***Manager*** (Chefarzt und Krankenhausleiter) hat im Vergleich zu anderen Mitarbeitern die weitestgehenden Zugriffsrechte einschließlich Zugriff auf persönliche, finanzielle und medizinische Daten. Er darf jedoch nicht die persönlichen Notizen der behandelnden Ärzte einsehen. Unter bestimmten Bedingungen (z. B. solange die Dokumentationspflicht eingehalten wird) ist der Manager berechtigt, Daten über den Patienten zu löschen. In einer verfeinerten Version muss die Rolle des Chefarztes von der Rolle des Verwaltungsleiters getrennt werden.
- Mitglieder des ***Pflegepersonals*** müssen eventuell ein Verschwiegenheitsklausel unterschreiben und dürfen auf Dokumente zugreifen, die nicht älter als ein Jahr sind. Sie dürfen die elektronische Patientenakte lesen, aber nicht bearbeiten. Pflegedaten sind gesondert zu behandeln.
- ***Behandelnde Ärzte*** dürfen auf die Patientenakte sowie auf ihre persönlichen Arzt-Notizen lesend und schreibend zugreifen.

- ***Sonstige Mitarbeiter*** aus Verwaltung oder Sekretariaten haben Zugriff auf die Stamm- oder Abrechnungsdaten.

Die folgende Abbildung zeigt mögliche Rollen (1) und Rechte (2) beim Einsatz eines RBAC-Modells in einem Krankenhaus. Benutzer agieren als Subjekte (3) in den angefragten Rollen, die sie gemäß der Rollenabbildung (*sr*, s.o. Abschnitt 2.3) einnehmen dürfen.

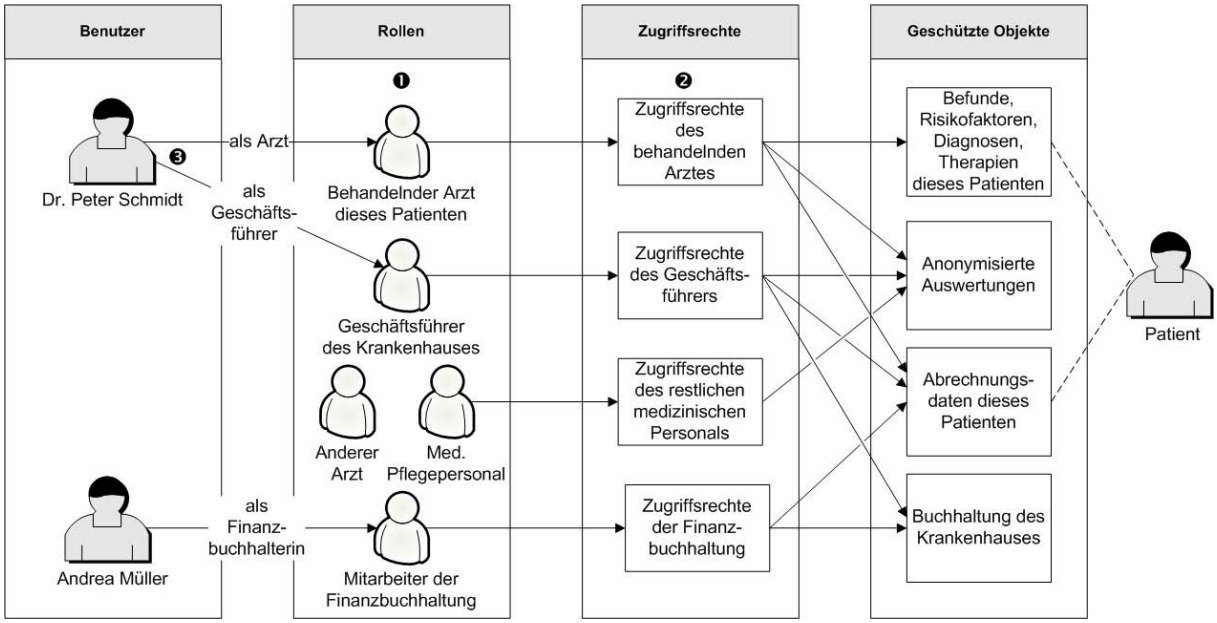

Abbildung 4 Szenario "RBAC in einem Krankenhaus"

3.3 Wechselnde Rollen

Die Rollen der Benutzer sind in der täglichen Praxis nicht starr festgeschrieben. Stattdessen gibt es dynamische Beschränkungen, die kontext- oder zeitbezogen sind [SoDrAh2005]. Zum Beispiel kann ein Arzt auch Geschäftsführer eines Krankenhauses sein und gleichzeitig zeitweise eigene Patienten behandeln (vgl. Dr. Peter Schmidt (3) in Abbildung 4). Entsprechend erhält er unterschiedliche Zugriffsrechte.

Die Arzt-Rolle hängt vom jeweiligen *Kontext* ab, der dynamisch wechselt. Beispielsweise wird ein Patient von dem Chefarzt der Abteilung persönlich behandelt, aber der jeweils Dienst habende Stationsarzt ist an der Behandlung beteiligt. Außerdem wird ein weiterer Facharzt aus einer anderen Abteilung des Krankenhauses zur Behandlung hinzugezogen. Die Rollen sind unterschiedlich mit teilweise überschneidenden Rechten. Das ist im RBAC-Modell durch eine geeignete Rollenbeschreibung leicht zu spezifizieren, ohne Rücksicht auf das tatsächlich vorhandene Personal. Welche konkreten Personen diese Rollen dann einnehmen, bleibt davon zunächst unberührt und kann von der Betriebsorganisation eines Krankenhauses ressourcenbezogen täglich gesteuert werden, ohne die Rollen verändern zu müssen.

Weiterhin werden die *Delegation* und das Widerrufen (*Revocation*) von Rechten durch das RBAC-Modell wesentlich vereinfacht [ZhAhCh2003]. Denn die Neuzuordnung von Rollen zu Subjekten (Delegation) kann unabhängig von der Aufgabenbeschreibung vorgenommen werden. Und das Löschen von Rollen bzw. das Verändern von Rollenrechten (Revocation) kann unabhängig von der Aufgabenverteilung an Personen geschehen.

4 RBAC-Projekte

Die Möglichkeiten, die RBAC als Sicherheitstechnologie für verteilte Informationssysteme bietet, sind vom Gesundheitswesen durchaus erkannt. Es gibt Studien, die sich ausdrücklich auf das Gesundheitswesen beziehen, etwa [Cha2001] [EvBo2004] [SoDrAh2005]. Nach eigenen Angaben der Firma GMD – Gesellschaft für Medizinische Datenverarbeitung mbH (Berlin) verwendet die Anwendung „Elektronische Patientenkarte“ ihres Produkts *e-health®.solutions* RBAC und setzt es bei mehreren Referenzkunden in Deutschland und Italien ein [GMD2006]. Weitere Produkte mit RBAC-Kern in der elektronischen Patientenkarte sind zum Beispiel *Dashboard* von Siemens Medical Solutions (München) [Sie2006], *Lenus* von SER HealthCare Solutions GmbH (Neustadt/Wied) [SER2006] und TeamTrack Version 6 von Serena Software GmbH (Köln) [Serena2006]. Sie alle nennen zahlreiche Referenzkunden, die Dokumentenmanagement in Krankenhäusern betreiben. In der Praxis wurden nach Beobachtung von [SoDrAh2005] (bis 2005) weitergehende Mechanismen wie das hierarchische Konzept noch nicht oder nur unzureichend umgesetzt.

Erfahrungen mit dem Betrieb von RBAC im Gesundheitswesen sind nach unserem Wissen noch nicht veröffentlicht worden. Ein ausführlicher Erfahrensbericht über den Einsatz von RBAC in einem anderen Sektor, nämlich im Bankenwesen, liegt in [ScMoJa2001] vor. Das Ziel ihrer Untersuchung war es zu überprüfen, ob RBAC funktional korrekt und stabil in einer „großen Organisation“ (es kam nicht darauf an, dass es eine Bank ist) laufen kann. Das wird positiv bestätigt. Als Einschränkung entdeckten sie aber einen inhärenten Konflikt zwischen der hierarchischen Vererbung von Rechten einerseits und Kontrollprinzipien, wie zum Beispiel der Aufgabenteilung, andererseits. Auch die Zuordnung von Gruppen, statt nur von einzelnen Subjekten, zu Rollen ist nach ihrer Untersuchung im RBAC-Modell noch ungelöst. Das wäre auch für das Gesundheitswesen sinnvoll, denn manches Subjekt greift gar nicht in einer individuell erworbenen Rolle, sondern als Gruppenmitglied, etwa der Revision oder des Pflegepersonals, auf Patientendaten zu. Clientgruppen sind aber in der Regel bereits in den bestehenden Systemen eingerichtet, denen Rollen schnell zugeordnet werden könnten.

Während RBAC in netzbasierten Anwendungssystemen für die Verwaltung von Inhaltsdaten durchaus verbreitet ist, wird es in Basissystemen wie Betriebs- und Datenbanksystemen nicht eingesetzt. Der Grund liegt darin, dass Rollen einen Bezug zu Aufgaben, d.h. zu den Inhalten haben, aber nicht zu den Daten auf User-Ebene. Hier greift eher ein User-bezogenes Zugriffsmodell wie DAC oder MAC (s.o. Abschnitte 1 und 2). Allerdings muss jede rollenbasierte Zugriffskontrolle eines Anwendungssystems intern auf die Zugriffsmechanismen der zugrunde liegenden Betriebssysteme abgestützt werden.

Wir halten RBAC für eine sinnvolle und praktisch komfortable Lösung für das Gesundheitswesen. RBAC folgt einem nachvollziehbaren Modell, ist in der Standardisierung gut etabliert und es gibt nun auch genügend RBAC-basierte Markenprodukte für den betrieblichen Einsatz.

Literaturverzeichnis

[BePa1973] D.E. Bell, and L.J. LaPadula (1973): Secure Computer Systems: Mathematical Foundations, and A mathematical model. ESD-TR-73-278, MTR-2547, Vols 1&2. The MITRE Corporation, Bedford, MA, Nov 1973.

[Cha2001] Ramaswamy Chandramouli (2001) A Framework for Multiple Authorization Types in a Healthcare Application System Computer Security Division, ITL NIST, Gaithersburg, MD. csrc.nist.gov/rbac/rmouli_healthcare.pdf [6.9.2006]

[ClWi1987] D. Clark, and D. Wilson (1987): A Comparison of Commercial and Military Security Policies. Proceedings of the 1987 IEEE Symposium on Security and Privacy, Oakland, CA. Computer Society Press of the IEEE, Washington DC, 1987, 184-194.

[Eck2005] Claudia Eckert (2005): IT-Sicherheit, Konzepte-Verfahren-Protokolle, Oldenbourg, München.

[EvBo2004] Mark Evered, Serge Bögeholz (2004): A Case Study in Access Control Requirements for a Health Information System. ACM International Conference Proceeding Series; Vol. 54: Proceedings of the second workshop on Australasian Information Security, Data Mining and Web Intelligence, and Software Internationalisation, ACM 2004.

[FeKu1992] David Ferraiolo, Richard Kuhn (1992): Role-Based Access Control, Proceedings of 15th National Computer Security Conference, Gaithersburg, MD, NCSC 1992, 554-563.

[FeSa et al. 2001] David Ferraiolo, Ravi Sandhu, Serban Gavrila, Richard Kuhn, Ramaswamy Chandramouli (2001): Proposed NIST Standard for Role-Based Access Control, ACM Transactions on Information and System Security, Vol. 4, No. 3, August 2001, 224–274.

[GMD2006] GMD (2006): Elektronische Patientenkarte, Anwendung des Produkts health®.solutions mit RBAC. www.gmdworld.com/index.php/106.0.Elektronische_Patientenakte.html sowie www.gmdworld.com/index.php/93.0.Referenzkunden.html [6.9.2006]

[HoPr2003] Gabriele Hoppe, Andreas Prieß (2003): Sicherheit von Informationssystemen, Verlag neue Wirtschafts-Briefe, Herne, Berlin.

[Lam1971] B. W. Lampson (1971): Protection. In Proceedings of the Fifth Annual Princeton Conference on Information Science Systems, 1971, 437-443. Reprinted in Operating Systems Review, Volume 8, Number 1, January 1974, 18-24.

[SaCo et al.1996] Ravi Sandhu, Edward Coyne, Hal Feinstein, Charles Youman (1996): Role-based access control models. IEEE Comput., 29 (2), Feb 1996.

[Sch2000] Bruce Schneier (2000): Secrets and Lies, Digital Security in a Networked World, Wiley Publishing, Inc.

[ScMoJa2001] Andreas Schaad, Jonathan Moffett, Jeremy Jacob (2001): The Role-Based Access Control System of a European Bank: A Case Study and Discussion, SACMAT 2001: 6th ACM Symposium on Access Control Models and Technologies, Chantilly, VA, USA, ACM 2001.

[Serena2003] Christian Weber (2003): Serena Software präsentiert TeamTrack Version 6. In: contentmanager.de, 10.11.2003, www.contentmanager.de/magazin/news_h6107_serena_software_praesentiert_teamtrack_version_6.html [6.9.2006]

[SER2006] SER Pressemitteilung: eHealthCare bei SER: Launch der Hospital Content Management-Suite LENUS. www.ser.de/ww/de/pub/presse/pressemitteilungen/content1883.htm [6.9.2006]

[Sie2001] Siemens AG Medical Solutions (2001): Siemens-Innovationen auf dem RSNA in Chicago, 25.-30. November 2001. In: electromedica 69 (2001) Heft 2, 147-157, besonders S. 149. www.healthcare.siemens.com/medroot/en/news/electro/issues/pdf/heft_2_01_d/Siemens%20Innovationen.pdf [7.9.2006]

[Sil2006] silicon.de: Laptop im Auto vergessen – 28.000 Patientendaten weg. In Security Management, 24.08.2006, www.silicon.de/enid/security_management/21835 [6.9.2006]

[SoDrAh2005] Karsten Sohr, Michael Drouineaud, Gail-Joon Ahn (2005): Formal Specification of Role-based Security Policies for Clinical Information Systems. Proceedings of the 2005 ACM symposium on Applied Computing, ACM 2005.

[ZhAhCh2003] Longua Zhang, Gail-Joon Ahn, Bei-Tseng-Chu (2003) :A Rule-Based Framework for Role-Based Delegation and Revocation. ACM Transactions on Information and System Security, Vol. 6, No. 3, August 2003, 404–441.

Bisher erschienen

Arbeitsberichte aus dem Fachbereich Informatik
(http://www.uni-koblenz.de/fb4/publikationen/arbeitsberichte)

Rüdiger Grimm, Anastasia Meletiadou: Rollenbasierte Zugriffskontrolle (RBAC) im Gesundheitswesen, Arbeitsberichte aud dem Fachbereich Informatik 15/2007

Ulrich Furbach, Jan Murray, Falk Schmidsberger, Frieder Stolzenburg: Hybrid Multiagent Systems with Timed Synchronization-Specification and Model Checking, Arbeitsberichte aus dem Fachbereich Informatik 14/2007

Björn Pelzer, Christoph Wernhard: System Description:“E-KRHyper“, Arbeitsberichte aus dem Fachbereich Informatik, 13/2007

Ulrich Furbach, Peter Baumgartner, Björn Pelzer: Hyper Tableaux with Equality, Arbeitsberichte aus dem Fachbereich Informatik, 12/2007

Ulrich Furbach, Markus Maron, Kevin Read: Location based Informationsystems, Arbeitsberichte aus dem Fachbereich Informatik, 11/2007

Philipp Schaer, Marco Thum: State-of-the-Art: Interaktion in erweiterten Realitäten, Arbeitsberichte aus dem Fachbereich Informatik, 10/2007

Ulrich Furbach, Claudia Obermaier: Applications of Automated Reasoning, Arbeitsberichte aus dem Fachbereich Informatik, 9/2007

Jürgen Ebert, Kerstin Falkowski: A First Proposal for an Overall Structure of an Enhanced Reality Framework, Arbeitsberichte aus dem Fachbereich Informatik, 8/2007

Lutz Priese, Frank Schmitt, Paul Lemke: Automatische See-Through Kalibrierung, Arbeitsberichte aus dem Fachbereich Informatik, 7/2007

Rüdiger Grimm, Robert Krimmer, Nils Meißner, Kai Reinhard, Melanie Volkamer, Marcel Weinand, Jörg Helbach: Security Requirements for Non-political Internet Voting, Arbeitsberichte aus dem Fachbereich Informatik, 6/2007

Daniel Bildhauer, Volker Riediger, Hannes Schwarz, Sascha Strauß, „grUML – Eine UML-basierte Modellierungssprache für T-Graphen“, Arbeitsberichte aus dem Fachbereich Informatik, 5/2007

Richard Arndt, Steffen Staab, Raphaël Troncy, Lynda Hardman: Adding Formal Semantics to MPEG-7: Designing a Well Founded Multimedia Ontology for the Web, Arbeitsberichte aus dem Fachbereich Informatik, 4/2007

Simon Schenk, Steffen Staab: Networked RDF Graphs, Arbeitsberichte aus dem Fachbereich Informatik, 3/2007

Rüdiger Grimm, Helge Hundacker, Anastasia Meletiadou: Anwendungsbeispiele für Kryptographie, Arbeitsberichte aus dem Fachbereich Informatik, 2/2007

Anastasia Meletiadou, J. Felix Hampe: Begriffsbestimmung und erwartete Trends im IT-Risk-Management, Arbeitsberichte aus dem Fachbereich Informatik, 1/2007

„Gelbe Reihe“
(http://www.uni-koblenz.de/fb4/publikationen/gelbereihe)

Lutz Priese: Some Examples of Semi-rational and Non-semi-rational DAG Languages. Extended Version, Fachberichte Informatik 3-2006

Kurt Lautenbach, Stephan Philippi, and Alexander Pinl: Bayesian Networks and Petri Nets, Fachberichte Informatik 2-2006

Rainer Gimnich and Andreas Winter: Workshop Software-Reengineering und Services, Fachberichte Informatik 1-2006

Kurt Lautenbach and Alexander Pinl: Probability Propagation in Petri Nets, Fachberichte Informatik 16-2005

Rainer Gimnich, Uwe Kaiser, and Andreas Winter: 2. Workshop "Reengineering Prozesse" – Software Migration, Fachberichte Informatik 15-2005

Jan Murray, Frieder Stolzenburg, and Toshiaki Arai: Hybrid State Machines with Timed Synchronization for Multi-Robot System Specification, Fachberichte Informatik 14-2005

Reinhold Letz: FTP 2005 – Fifth International Workshop on First-Order Theorem Proving, Fachberichte Informatik 13-2005

Bernhard Beckert: TABLEAUX 2005 – Position Papers and Tutorial Descriptions, Fachberichte Informatik 12-2005

Dietrich Paulus and Detlev Droege: Mixed-reality as a challenge to image understanding and artificial intelligence, Fachberichte Informatik 11-2005

Jürgen Sauer: 19. Workshop Planen, Scheduling und Konfigurieren / Entwerfen, Fachberichte Informatik 10-2005

Pascal Hitzler, Carsten Lutz, and Gerd Stumme: Foundational Aspects of Ontologies, Fachberichte Informatik 9-2005

Joachim Baumeister and Dietmar Seipel: Knowledge Engineering and Software Engineering, Fachberichte Informatik 8-2005

Benno Stein and Sven Meier zu Eißen: Proceedings of the Second International Workshop on Text-Based Information Retrieval, Fachberichte Informatik 7-2005

Andreas Winter and Jürgen Ebert: Metamodel-driven Service Interoperability, Fachberichte Informatik 6-2005

Joschka Boedecker, Norbert Michael Mayer, Masaki Ogino, Rodrigo da Silva Guerra, Masaaki Kikuchi, and Minoru Asada: Getting closer: How Simulation and Humanoid League can benefit from each other, Fachberichte Informatik 5-2005

Torsten Gipp and Jürgen Ebert: Web Engineering does profit from a Functional Approach, Fachberichte Informatik 4-2005

Oliver Obst, Anita Maas, and Joschka Boedecker: HTN Planning for Flexible Coordination Of Multiagent Team Behavior, Fachberichte Informatik 3-2005

Andreas von Hessling, Thomas Kleemann, and Alex Sinner: Semantic User Profiles and their Applications in a Mobile Environment, Fachberichte Informatik 2-2005

Heni Ben Amor and Achim Rettinger: Intelligent Exploration for Genetic Algorithms – Using Self-Organizing Maps in Evolutionary Computation, Fachberichte Informatik 1-2005