Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Ausarbeitung Anwendungen 1 (AI)

Thomas Schmidt

Sicherheit in Location Based Services durch Zugriffskontrolle

Fakultät Technik und Informatik
Studiendepartment Informatik

Hamburg, 17. Juli 2006

Inhaltsverzeichnis

1 Einleitung

Diese Ausarbeitung handelt von der Absicherung von Location Based Services (LBS) durch Anwendung von Zugriffskontrollstrategien. Sie soll zeigen, ob die Sicherheit eines IT-Systems durch Kenntnis des Ortes beinträchtig wird oder ob die Sicherheit sogar erhöht werden kann.

Zu Beginn wird erläutert, was der Begriff Sicherheit in der IT-Branche bedeutet. Anschließend wird ein Teil der Bereiche Informationssicherheit und Datensicherheit genauer betrachtet. In diesen beiden Bereichen geht es um autorisierten Zugriff. Unautorisierte Benutzer sollen keinen Zugang zum System und dessen Daten bekommen.
Das Kapitel 3 gibt eine kurze Übersicht über bestehende Zugriffskontrollstrategien.
Kapitel 4 erklärt den Begriff Location Based Service und die Unterteilung in reaktive und proaktive LBS.
Kapitel 5.1 erläutert eine Zugriffskontrollstrategie, die eine Einteilung der Zugriffsrechte aufgrund des Ortes möglich macht. Diese Strategie wird als Grundlage für das Security Framework verwendet, das in Kapitel 5.2 vorgestellt wird. Dadurch soll eine flexible und sichere Lösung zur Integration von mobilen Geräten in ein IT-System vorgestellt werden.

Kapitel 6 gibt eine Zusammenfassung und einen Ausblick auf das nächste Semester.

2 Sicherheit

„*IT-Sicherheit ist der Zustand eines IT-Systems, in dem die Risiken, die beim Einsatz dieses IT-Systems aufgrund von Bedrohungen vorhanden sind, durch angemessene Maßnahmen auf ein tragbares Maß beschränkt sind.* “(BSI, 1992, Anhang A)

Der Sicherheitsbegriff lässt sich in vier Bereiche aufteilen:[1]

Funktionssicherheit (engl. safety)
Die IST-Funktionalität stimmt mit der SOLL-Funktionalität überein und das System arbeitet somit korrekt und zuverlässig (gem. der jeweiligen Spezifikation).

Informationssicherheit (engl. security)
Das System nimmt nur Zustände an, die zu keiner unautorisierten Informationsveränderung oder -gewinnung führen.

Datensicherheit (engl. protection)
Das System nimmt nur Zustände an, die zu keinem unautorisierten Zugriff auf Systemressourcen oder Daten führen. Unter diesem Punkt wird auch Datensicherung (Schutz vor Datenverlust durch Sicherheitskopien) verstanden.

Datenschutz (engl. privacy)
Eine Person hat die Fähigkeit die Weitergabe von Informationen, die sie persönlich betreffen, zu kontrollieren.[2]

3 Zugriffskontrollstrategien

Alle IT-Systeme haben im Grunde das Problem, dass die Benutzer nicht auf alle Informationen Zugriff haben sollen. Es wird eine Möglichkeit benötigt, um festzulegen, welche Aktionen ein Benutzer im System ausüben darf.
Sobald ein Benutzer auf ein Objekt zugreift, soll zuerst eine Zugriffskontrolle erfolgen, die anhand vorher vergebener Zugriffsrechte überprüft, ob der Zugriff erlaubt ist.
Dieses Kapitel gibt eine kurze Übersicht über bestehende Zugriffskontrollstrategien.

[1] Vgl. Eckert (2001), Seite 3
[2] für weitere Informationen siehe BDSG (1977)

3.1 Discretionary Access Control

Discretionary Access Control (DAC) steht für benutzerbestimmbare Zugriffskontrollstrategie. Bei dieser Strategie ist jedem Objekt ein Benutzer als Besitzer zugeordnet. Dieser ist verantwortlich für die Vergabe und Pflege der Zugriffsrechte.

Meist wird DAC durch Zugriffskontrollisten realisiert, die folgende Struktur besitzen:
`benutzer_name, zugriffsrechte`

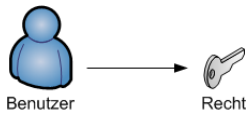

Abbildung 1: Zugriff auf Benutzerebene

Der Vorteil dieser Strategie ist die Tatsache, dass sie relativ einfach zu implementieren ist. Allerdings ist die schlechte Skalierung ein entscheidender Nachteil, da dies in Umgebungen mit vielen Benutzern und verschiedenen Rechten zu Problemen führen kann (bei langen Listen aufwändiges, ineffizientes Durchsuchen).

3.2 Mandatory Access Control

Mandatory Access Control (MAC) bedeutet systembestimmte Zugriffskontrollstrategie.
Bei dieser Strategie ist die Zugriffskontrolle über Vertraulichkeitsstufen realisiert. Jedes Objekt im System ist einer Vertraulichkeitsstufe zugeordnet und jeder Benutzer hat eine Freigabe für eine Vertraulichkeitsstufe (siehe Abbildung 2).

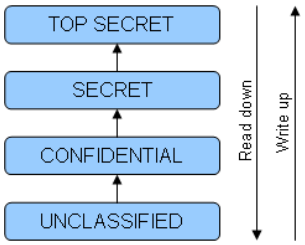

Abbildung 2: Vertraulichkeitsstufen

Die Zugriffskontrolle wird durch folgende Regeln definiert:

Read-Down-Regel
Vertraulichkeitsstufe[Objekt] <= Vertraulichkeitsstufe[Benutzer]

Benutzer können lesend nur auf Objekte ihrer oder niedrigerer Vertraulichkeitsstufe zugreifen.

Write-Up-Regel
Vertraulichkeitsstufe[Objekt] >= Vertraulichkeitsstufe[Benutzer]
Benutzer können schreibend nur auf Objekte ihrer oder höherer Vertraulichkeitsstufe zugreifen.

Der Nachteil an dieser Strategie ist, dass die Vertraulichkeitsstufen statisch sind und somit in Umgebungen mit häufig wechselnden Anforderungen zu inflexibel sind.

3.3 Role Based Access Control

Role Based Access Control (RBAC) bedeutet rollenbasierte Zugriffskontrollstrategie.
Es werden Rollen definiert, die einem Systembenutzer zugeordnet werden. Einer Rolle umfasst ein oder mehrere Rechte (authorisations), die den Zugriff auf das System einschränken oder erweitern.

Durch dieses Vorgehen wird ein Zugriffsrecht nicht mehr direkt an eine Person gebunden. Ein Zwischenschritt (Rolle) reduziert den Aufwand bei Änderungen und vermeidet Fehler (z.B. falsche Rechtezuordung, vergessenes Löschen eines Rechtes). Siehe Abbildung 3.

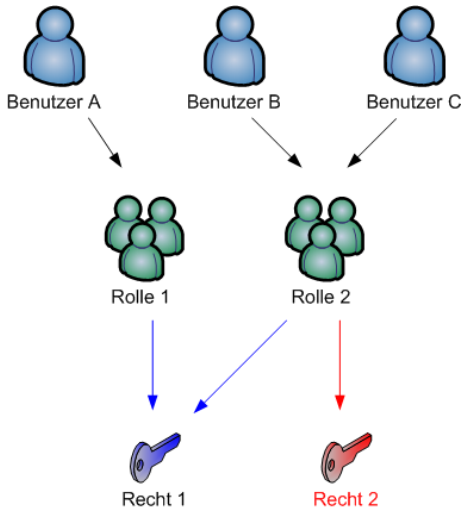

Abbildung 3: Rollenbasierte Zugriffskontrolle

Die Kontrolle des Zugriffs auf das System bzw. auf Systemressourcen kann effektiver gestaltet werden. Anhand der Rolle kann erkannt werden, welche Berechtigungen ein Benutzer hat. Der Administrator muss nicht jeden Nutzer einzeln neu erfassen und dann entsprechende Zugriffsregeln setzen.

Durch dieses Konzept wird eine gute Skalierbarkeit geschaffen, da unterschiedlich große Rollenmodelle unterschiedliche Organisationsstrukturen repräsentieren.

In der Literatur wird zwischen 'Static Separation of Duty' und 'Dynamic Separation of Duty' unterschieden:

Static Separation of Duty (SSD)
Die statische Trennung von Aufgaben ermöglicht die Definition von Rollenmitgliedschaften, die sich gegenseitig ausschließen. Hierfür werden Relationen zwischen den, sich gegenseitig ausschließenden, Rollen angelegt.
Sobald ein Benutzer eine neuen Rolle zugewiesen bekommt, wird überprüft, ob der Benutzer schon eine Rolle besitzt, die in einer SSD-Relation steht. Wenn dies der Fall sein sollte, wird die Zuweisung nicht vorgenommen.[3]

Dynamic Separation of Duty (DSD)
Die dynamische Trennung von Aufgaben wird genau wie bei SSD durch Relationen zwischen Rollen definiert. Bei DSD können zwei Rollen in einer Benutzersitzung nicht gleichzeitig aktiv sein.
Die Einschränkungen werden also zur Laufzeit überprüft.[4]

4 Location Based Services

In diesem Kapitel wird der Begriff Location Based Service erklärt und die Unterteilung in reaktive und proaktive LBS erläutert.

4.1 Allgemein

'Location Based Services' sind eine Teilmenge der 'Context Aware Services'. Im Allgemeinen werden 'Context Aware Services' als Dienste gesehen, die ihr Verhalten automatisch entsprechend ihres Kontextes anpassen.[5]

Unter 'Location Based Services' (LBS) sind standortbezogene Dienste zu verstehen. Diese stellen selektive Informationen mittels zeit- und positionsabhängiger Daten für den Nutzer zur Verfügung.

[3] Vgl. Ferraiolo u. a. (Apr. 2003)
[4] Vgl. Ferraiolo u. a. (Apr. 2003)
[5] Vgl. Küpper (2005), Seite 2

„*Location services can be defined as services that integrate a mobile device's location or position with other information so as to provide added value to a user.*“
(Schiller und Voisard, 2004, S.10)

Die GSM Association (ein Konsortium aus 600 GSM-Netz-Betreibern) definieren Location Based Services als Dienste, die die Location des 'Zielobjektes' nutzen um einen Dienst aufzuwerten.[6]

Wenn man diese Definitionen betrachtet, stellt sich die Frage, was unter einer Aufwertung eines Dienstes gemeint ist. Die Antwort auf diese Frage erschließt sich schnell, wenn man an z.B. an ein Navigationssystem denkt. Durch die Bestimmung des Ortes, an dem sich die Person befindet, kann die Route zum Ziel berechnet und aktualisiert werden. Eine einfache Straßenkarte wird somit zu einem Leitsystem aufgewertet.

4.2 Reaktive LBS

Reaktive LBS werden explizit vom Benutzer des Dienstes angestoßen. Er stellt eine Anfrage an den Service und bekommt eine Antwort. Ein Nutzer möchte z.B. wissen, welche Restaurants ins seiner Nähe sind und der Dienst listet diese auf. Dieser Zyklus ist eine synchrone Interaktion zwischen Nutzer und Dienst. (siehe Abbildung 4)

Abbildung 4: Reaktive LBS

4.3 Proaktive LBS

Poraktive LBS werden automatisch initialisiert sobald ein vordefiniertes, ortsbezogenes Ereignis eintritt. Der Aufenthaltsort des Nutzers wird permanent abgefragt. Sobald ein bestimmter Bereich betreten wird bekommt er eine Mitteilung des Dienstes. Ein elektronischer Reiseführer informiert den Nutzer z.B. über ein Gebäude, sobald dieser davor steht. Die Interaktion zwischen Nutzer und Dienst ist asynchron. (siehe Abbildung 5)

[6] Vgl. Küpper (2005), Seite 1

Abbildung 5: Proaktive LBS

5 Sicherheit in Location Based Services

In Kapitel 5.1 wird eine Zugriffskontrollstrategie erläutert, die eine Einteilung der Zugriffsrechte aufgrund des Ortes möglich macht. Diese wird als Grundlage für das Security Framework verwendet, das in Kapitel 5.2 vorgestellt wird.

5.1 Spatial Role Based Access Control

Spatial Role Based Access Control (SRBAC) bedeutet ortsabhängige, rollenbasierte Zugriffskontrolle.
Wie auch das traditionelle RBAC, das im Grundlagenkapitel 3.3 vorgestellt worden ist, hat SRBAC eine Rollenhierarchie. Im Gegensatz zum RBAC hängt die Zugriffsberechtigung eines Benutzers nicht mehr nur von der Rolle sondern zusätzlich noch vom Sicherheitskontext (dem Ort) ab.[7] Siehe Abbildung 6.

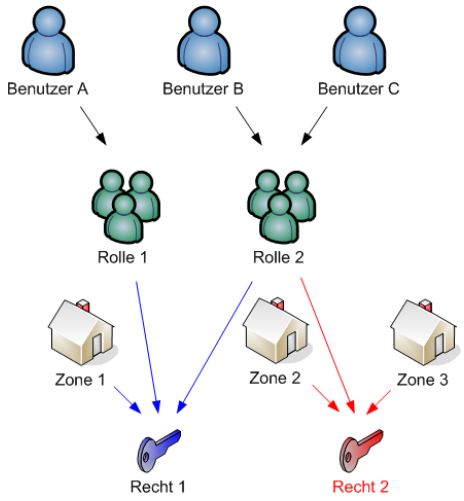

Abbildung 6: Ortsabhängige, rollenbasierte Zugriffskontrolle

Obwohl das traditionelle RBAC bei vielen Anwendungen nützlich ist um die Zugriffskontrolle zu modellieren, kann es oftmals nicht alle sicherheitsrelevanten Zusammenhänge sicherstellen,

[7] Vgl. Hansen und Oleshchuk (2006)

die ebenfalls Einfluss auf die Zugriffsentscheidungen haben. In manchen Fällen darf der Zugriff auf Daten z.B. nur von bestimmten Orten aus geschehen.[8]

Im traditionellen RBAC hat ein Benutzer die Rechte, die seiner aktuellen Rolle zugeordnet worden sind. Durch SRBAC kann ein größeres Maß an Flexibilität erreicht werden, da Kenntnisse über den Ort, an dem sich der Benutzer aufhält, vorhanden sind.

Beispiel:
Ein bestimmter Bereich kann in verschiedene Zonen eingeteilt werden (*Zone1*, *Zone2*, *Zone3*), an denen verschiedene Sicherheitsbestimmungen gelten. Die Rechte, die an eine bestimmte Rolle (*Rolle1*) in Abhängigkeit des Ortes gebunden sind, können in einer ortsbezogenen Rechteliste (Location Permission Assignment List - LPAL) aufgelistet werden. (siehe Tabelle 1).

Rollen	**Orte**	**Rechte**
Rolle1	*Zone1*	*Recht1*, *Recht2*, *Recht3*
Rolle1	*Zone2*	*Recht4*
Rolle1	*Zone3*	⊘

Tabelle 1: Ortsbezogene Rechteliste

Die Rechte der *Rolle1* variieren mit dem jeweiligen Ort. In *Zone1* hat der Nutzer die Rechte *Recht1*, *Recht2* und *Recht3*. In *Zone2* nur das *Recht4* und in *Zone3* hat keine Rechte.[9]

SRBAC bietet, genau wie das in Kapitel 3.3 vorgestelle RBAC, die Möglichkeit eine Trennung der Aufgaben vorzunehmen. Die bekannten SSD- und DSD-Relationen weden hierbei um die Ortsprüfung erweitert. Man spricht nun von Spatial SSD (SSSD) und Spatial DSD (SDSD).[10]

Spatial Static Separation of Duty (SSSD)
Eine Relation zwischen Rollen wird in Abhängigkeit des Ortes definiert. Wenn ein Benutzer einer bestimmten Rolle an einem bestimmten Ort zugeordnet worden ist, dann kann er keiner anderen Rolle an diesem Ort zugeordnet werden, wenn diese in der SSSD-Relation stehen.

In der Beispielumgebung (Abbildung 7) gibt es zwei Rollen, Rolle1 und Rolle2, in der ein Benutzer allen Rollen zugeordnet werden kann, außer wenn er sich in Zone3 befindet.
`((Rolle1,Rolle2);Zone3) ∈ SSSD`
Im klassischen SSD würde diese Einschränkung für alle Orte gelten.
`((Rolle1,Rolle2);Zone1,Zone2,Zone3,Zone4) ∈ SSSD`

[8] Vgl. Zhang u. a. (June 2002)
[9] Vgl. Hansen und Oleshchuk (2003)
[10] Vgl. Hansen und Oleshchuk (2003)

entspricht
`((Rolle1,Roll2)) ∈ SSD`

Spatial Dynamic Separation of Duty (SDSD)
Wie bei SSSD wird eine Relation zwischen Rollen in Abhängigkeit des Ortes definiert. Bei SDSD bedeutet diese Relation, dass diese zwei Rollen in einer Benutzersitzung nicht gleichzeitig aktiv sein können. Die Einschränkungen werden also zur Laufzeit überprüft.

In Abbildung 7 ist es keinem Benutzer erlaubt, beide Rollen, Rolle1 und Rolle2, in der Zone3 in einer Benutzersitzung zu aktivieren.
`((Rolle1,Rolle2);Zone3) ∈ SDSD`
Für die anderen Zonen existiert diese Einschränkung nicht. Im klassischen DSD würde diese Einschränkung für alle Orte gelten.

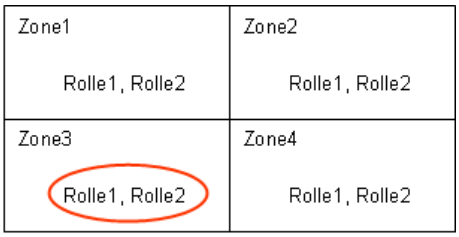

Abbildung 7: Beispiel für SSSD und SDSD

Durch die zusätzliche Abhängigkeit des Ortes ist somit eine viel feingranularere Einschränkung möglich. Es wird somit nicht generell für alle Orte eingeschränkt. Abbildung 8 veranschaulicht die ortsabhängige Trennung von Aufgaben.

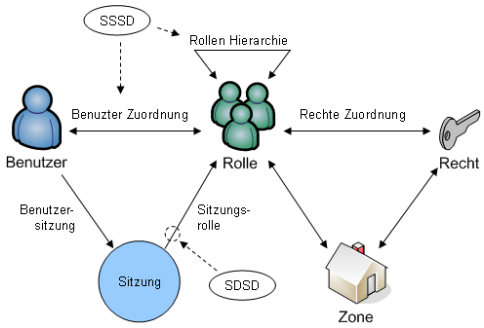

Abbildung 8: Ortsabhängige Trennung von Aufgaben

5.2 Security Framework

In diesem Kapitel wird ein Rahmenwerk für die Nutzung von mobilen Geräten vorgestellt. Dieses Modell unterstützt das SRBAC-Modell, das in Kapitel 5.1 vorgestellt worden ist. Es besteht aus folgenden Einheiten: Mobile terminal, User Monitor Agent, Authorizer, Location Server und Role Server (siehe Abbildung 9).

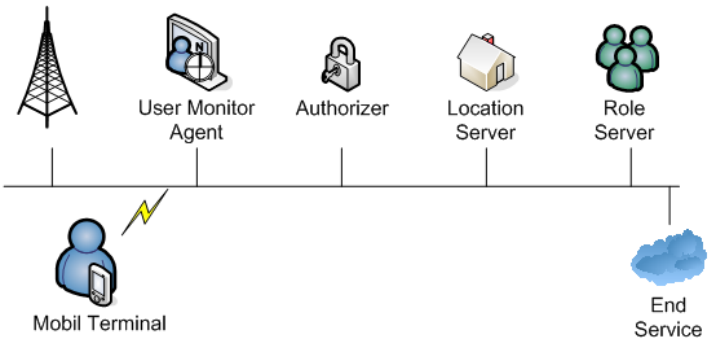

Abbildung 9: Security Framewok für die Nutzung von mobilen Geräten

Mobile Terminal (MT):
Das MT repräsentiert einen Benuzter, der ein mobiles Gerät benutzt, um einen vom System angebotenen Dienst zu nutzen. Der Zugriff muss von einer sicheren Ausführungsumgebung getätigt werden, die die laufenden Dienste während einer Sitzung kontrolliert. Diese Umgebung ermöglicht schwache und starke Sicherheit.
Bei schwachen Sicherheitsanforderungen genügt es oft, dass die Benutzersitzung bei Bedarf eingefroren wird und die laufende Anwendung einfach vom Bildschirm des Benutzers verschwindet und später wieder erscheint.
Bei starken Sicherheitsanforderungen würde die gesamte Benutzersitzung beendet und das Dokument vom Gerät gelöscht werden.

User Monitor Agent (UMA):
Der UMA erfasst die Position von aktiven Benuztern indem er die Daten von den Locationssensoren der Geräte einsammelt.

Authorizer:
Der Authorizer kümmert sich um die Anfrage, die vom MT gemacht werden. Wenn ein Benutzer eine Anfrage an einen Dienst startet, fordert er einen aktuellen Rechtesatz, der im Entscheidungsprozess verwendet wird, vom RS an.

Location Server (LS):
Der LS sammelt physikalische Positionsdaten von aktiven Benuztern vom UMA. Er bildet die

physikalischen Ortsdaten auf logische Ortsdaten ab. Diese Informationen werden anschließend an den RS weitergegeben, sofern sich der logische Aufenthaltsort des Benutzers geändert hat (location update message).

Role Server (RS):
Der RS beinhaltet eine Tabelle mit der Zuordnung der Benutzer zu Rollen, der Rechte zu Rollen, der aktiven Benutzersitzungen und Einschränkungen der SRBAC-Komponente. Er beinhaltet Statusinformationen aktiver Rollen, wie z.B. die gültigen Rechte der aktiven Rollen in einer Benutzersitzung. Er empfängt die logischen Ortsinformationen vom LS um die Rollen und Zugriffsstatus zu aktualisieren und sendet eine aktuellen Rechtesatz für aktive Benutzer an den Authorizer.

6 Zusammenfassung und Ausblick

In dieser Ausarbeitung wurde ein Framework vorgestellt das sicheren Zugriff auf Daten von mobilen Geräten ermöglicht. Für die Zugriffsentscheidungen werden Ortsinformationen benutzt um die Rechte einer Rolle am aktuellen Ort zu bestimmen. Es erweitert die traditionellen Sicherheitsvorschriften eines Unternehmens und ermöglicht flexible und sichere Lösungen für mobile Geräte als ein natürlicher Teil des Systems.

Durch dieses Framework kann die Sicherheit des Systems erhöht werden, da es eine feingranularere Rechtevergabe ermöglicht. Bestimmte Aktionen können nur von bestimmten Orten ausgeführt werden. Somit reicht es für einen Angreifer nicht, sich nur die Identität bzw. das Gerät eines autorisierten Benutzers anzueignen um in ein IT-System einzudringen. Er muss den Angriff zusätzlich noch von einem bestimmten Ort aus vornehmen, der durch zusätzliche (nicht zwingent IT-Technisch) Maßnahmen geschützt sein kann.
Sollte es dennoch zu einem unberechtigten Zugriff auf das System kommen, kann der autorisierte Benutzer, dessen Identität bzw. Gerät verwendet wurde, einfacher einen Unschuldsnachweis erbringen. Er muss lediglich nachweisen, dass er sich zum Zeitpunkt des Angriffs an einem anderen Ort aufgehalten hat. Dies erhöht die Sicherheit für den Benutzer.
Zusätzlich können durch diese Art der Zugriffskontrolle in einigen Bereichen Flüchtigkeitsfehler vermieden werden. Am Beispiel eines Krankenhauses: Ein Arzt kann die Medikation eines Patienten nur ändern, wenn er sich in dessen Raum aufhält. Somit kann ein Medikament, das für Patienten A bestimmt ist nicht versehentlich dem Patienten B verordnet werden.

Im nächsten Semester soll ein Framework für Spiele im LBS-Umfeld entwickelt werden. Dieses 'Pervasive Gaming Framework' soll die Entwicklung von LBS-Spielen unterstützen und vereinfachen. Prototypisch soll ein konkretes Spiel auf Grundlage dieses Frameworks implementiert und getestet werden.

In die Entwicklung des Frameworks werden verschiedene Interessengebiete der jeweiligen Entwickler einfließen. Ich möchte mich speziell mit der Sicherheit (insbesondere mit den Zugriffskontrollmöglichkeiten) dieses Frameworks befassen.

Literatur

[BDSG 1977] BDSG: *Bundesdatenschutzgesetz (BDSG)*. Namos-Verlag, Baden-Baden, 1977

[BSI 1992] BSI: *IT-Sicherheitshandbuch - Handbuch für die sichere Anwendung der Informationstechnik*. Bundesamt für Sicherheit in der Informationstechnik, 1992. – URL http://www.bsi.bund.de/literat/sichhandbuch/sichhandbuch.zip

[Eckert 2001] ECKERT, Claudia: *IT-Sicherheit Konzepte-Verfahren-Protokolle*. Oldenbourg Verlag München Wien, 2001

[Ferraiolo u. a. Apr. 2003] FERRAIOLO, David F. ; KUHN, D R. ; CHANDRAMOULI, Ramaswamy: *Role-Based Access Controls*. Artech House, Apr. 2003

[Hansen und Oleshchuk 2003] HANSEN, Frode ; OLESHCHUK, Vladimir: Spatial Role-Based Access Control Model for Wireless Networks. In: *IEEE* (2003). – URL http://ieeexplore.ieee.org/iel5/9004/28570/01285394.pdf?arnumber=1285394

[Hansen und Oleshchuk 2006] HANSEN, Frode ; OLESHCHUK, Vladimir: Location-based Security Framework for use of Handheld Devices in Medical Informaiton Systems. In: *IEEE* (2006). – URL http://ieeexplore.ieee.org/iel5/10656/33623/01599047.pdf?tp=&arnumber=1599047&isnumber=33623

[Küpper 2005] KÜPPER, Axel: *Location-Based Services Fundamentals and Operation*. John WILEY & Sons, Ltd., 2005

[Schiller und Voisard 2004] SCHILLER, Jochen ; VOISARD, Agnés: *Location-Based Services*. Elsevier Inc. - Morgan Kaufmann Publishers, 2004

[Zhang u. a. June 2002] ZHANG, Longhua ; AHN, Gail-Joon ; CHU, Bei-Tseng: A Role-Based Delegation Framework for Healthcare Information Systems. In: *ACM* (June 2002). – URL http://portal.acm.org/ft_gateway.cfm?id=507731&type=pdf&coll=ACM&dl=ACM&CFID=71947297&CFTOKEN=29858843