Datenschutz und Systemsicherheit für die medizinische Informationsverarbeitung

Jörg Moldenhauer[1], Martin Haimerl[1], Michael Walz[2], Gerald Weisser[2]

[1] Institut für Algorithmen und Kognitive Systeme,
Universität Karlsruhe (TH),
76128 Karlsruhe
jomo@ira.uka.de,
haimerl@ira.uka.de
[2] Institut für klinische Radiologie,
Klinikum der Stadt Mannheim,
68167 Mannheim
km22@rumms.uni-mannheim.de,
weisser@ikr.ma.uni-heidelberg.de

Zusammenfassung: In dem vorliegenden Beitrag werden Sicherheitskonzepte und -mechanismen vorgestellt, die im Rahmen des Projekts Q6 des SFB 414 für den Einsatz in medizinischen Informationssystemen entwickelt wurden. Aufbauend auf einer detaillierten Analyse der sicherheitstechnischen Anforderungen sind dabei Verfahren zur Absicherung von Patientendaten in klinischen Umgebungen mit stark wechselnden Zuständigkeiten entstanden, die in einem prototypischen klinischen Informationssystem integriert wurden. Zudem wurde für das vereinfachte Szenario einer Normdatenbank nach Analyse der dafür maßgeblichen Sicherheitsanforderungen ein System zur gesicherten Übermittlung von Bilddaten realisiert.

1 Einleitung

Elektronische Informationssysteme haben sich heute in allen Bereichen des klinischen Alltags etabliert. Mit ihnen soll Medizinern und Klinikpersonal ein unkomplizierter Zugriff auf Patientendaten ermöglicht werden. Der Schutz von vertraulichen Patientendaten baut in heutigen Systemen dabei auf Standardtechniken, wie Abschottung lokaler Kliniknetze durch Firewall-Techniken oder Kontrolle des Datenzugriffs durch personen- oder gruppenbasierte Rechtesysteme, auf. Eine wirksamere Absicherung und flexiblere Zugangskontrolle scheitert bisher am häufigen Wechsel von Zuständigkeiten und Verantwortlichkeiten im Klinikbetrieb. In dieser Arbeit sollen daher die besonderen sicherheitsrelevanten Anforderungen an zukünftige Systeme aufgezeigt, die grundlegenden Methoden bei der Entwicklung beschrieben und anhand eigener im Rahmen des Projektes Q6 im SFB 414 entstandenen Implementierungen demonstriert werden.

2 Erfassung datenschutzrechtlicher Anforderungen

Wem Zugang zu welchen Patientendaten gewährleistet werden darf, ist eine der grundlegenden Fragen, die zu klären ist, wenn für einen umfassenden Schutz der Daten gesorgt werden soll. Um ein ebenso transparentes wie konsequentes Sicherheitskonzept zu entwickeln, sind zunächst die Anforderungen, die von medizinischer Seite an elektronische Informationssysteme gestellt werden, systematisch zu erfassen und hinsichtlich ihrer technischen Umsetzungsmöglichkeiten zu analysieren. Dies wurde im Rahmen dieses Projekts in [Wa00a, Wa99, Wa00b] durchgeführt.
Ausgehend von den für diesen Bereich maßgeblichen nationalen gesetzlichen Bestimmungen (Röntgenverordnung, Bundes- und Landesdatenschutzgesetze, Berufsordnung, etc.) aber auch unter Einbezug von internationalen Richtlinien (EU-Norm, US-amerikanischer Gesetzesentwurf), die sich aktuell in der Entwicklung befinden und über die bisherigen Bestimmungen erheblich hinaus gehen, wurden Grundanforderungen für die Sicherheit und die Verfügbarkeit von Patientendaten konzeptionell erfasst. Zudem wurden in [Wa00a, Wa99, WMK99] praktische Lösungsansätze für deren Umsetzung aufgezeigt.
Zentrale Aspekte waren dabei der Schutz der Vertraulichkeit der Daten in strukturierten Umgebungen (insbesondere mittels Rollensystemen), die Reduzierung der übertragenen Informationen auf die im jeweiligen Kontext unbedingt notwendigen Informationen (ausgehend vom Prinzip der minimalen Rechte), der Schutz von Sekundärinformationen wie z. B. Datenfluss (Unbeobachtbarkeit) und zusammenführbare Informationen (Unverkettbarkeit) sowie die Gewährleistung der gesetzlich vorgeschriebenen Informationskontrolle durch den Patienten. Die Lösungsansätze umfassen Maßnahmen zur technischen Umsetzung der Übertragung von Bilddaten mittels DICOM-Standard ebenso wie grundsätzliche Maßnahmen zur Absicherung von Patienteninformation mit Hilfe von Anonymisierungs- bzw. Pseudonymisierungsverfahren, die letztendlich von informatischer Seite durch geeignete kryptographische Protokollmechanismen umgesetzt werden müssen und innerhalb dieses Projekts prototypisch realisiert wurden.

3 Kryptographische Bindungen als Basis für leistungsfähige Protokollmechanismen

Bevor auf den Entwurf derartiger Protokolle eingegangen werden kann, ist zunächst das Konzept der Bindung von Personen an Daten zu erläutern. Der Schutz von Daten erfolgt in der Regel durch die Bindung der Daten an eine bestimmte Person. Dies kann auf vielfältige Art geschehen. Beispielsweise kann einem Patienten bei der Überweisung eine Röntgenaufnahme anvertraut werden, wobei durch den Besitz eine physische Bindung vom Patienten an die Aufnahme oder durch die gesetzliche Lage eine juristische Bindung besteht. Bei der Entwicklung der Informationssysteme in dieser Arbeit wurde von einer kryptographischen Bindung ausgegangen. Die Bindung eines Datensatz ergibt sich hier aus der Kenntnis eines für die Entschlüsselung benötigten Geheimnisses bzw. aus der Unmöglichkeit, das kryptographische Verfahren zu brechen, welches der Bindung zu Grunde liegt. Die Bindungen beschränken sich dabei nicht nur auf einzelne Personen, sondern können auch für Gruppen von Personen gelten.

Neben rein statischen Bindungen, bei denen die Bindung einmalig eingerichtet wird und danach nicht mehr modifiziert werden kann, sind insbesondere im Bereich der medizinischen Informationssysteme flexible Formen der Bindung von wesentlicher Bedeutung, da hier häufig wechselnde Verantwortlichkeiten und Zuständigkeiten für Datensätze notwendig werden, die nicht durch statische Bindungen zu realisieren sind. Die in [Bl01, Br00, Ni00] vorgestellten neuen Protokollmechanismen wurden gezielt zur Bereitstellung dynamischer Bindungen entwickelt. Beispielsweise können damit Bindungen auf weitere Personen übertragen werden bzw. die Bindung an die bisherige Person für eine bestimmte Zeit aufgehoben und später wieder eingerichtet werden. Auch bezüglich einer langfristigen Speicherung von Daten sind diese flexiblen Bindungen notwendig, da bei der Integration neuer Sicherheitsmechanismen in ein Informationssystem eine Übertragung der Bindungen vorgenommen werden können muss.
Einen besonderen Aspekt von Bindungen stellt die Anonymisierung dar. Hier wird eine bestehende Bindung z. B. von Patient zu Datensatz gelöst, so dass keine Zuordnung von Person zu Datum erfolgen kann. Einen ähnlichen Sonderfall bildet die Pseudonymisierung. Hier wird die Bindung nicht aufgehoben, sondern nur durch eine zusätzliche Abbildung so modifiziert, dass keine direkten Rückschlüsse über die Bindung gezogen werden können. Im Bedarfsfall ist es jedoch bei gegebener Berechtigung möglich, die Abbildung zu invertieren, wodurch sich die Zuordnung von Person zu Datensatz wieder rekonstruieren lässt.

4 Betrachtung elementarer Kommunikationsmechanismen am Beispiel der 3D-Normdatenbank

Etliche Aspekte der grundlegenden Methoden lassen sich bereits anhand der Kommunikationsmechanismen erläutern, die für die im Rahmen des SFB 414 im Projekt K1 aufzubauende 3D-Normdatenbank [SFB01] (siehe Abb. 1) entwickelt wurden. Hier genügte es, ein eingeschränktes Sicherheits- bzw. Bedrohungsmodell zu betrachten, da die Funktion des Übertragungssystems sich im Wesentlichen auf die einseitige kryptographisch gesicherte Übermittlung anonymisierbarer Patientendaten beschränkt. Bei dem Normdatenbanksystem stand vielmehr im Mittelpunkt, es einer möglichst großen Anzahl international verteilter Radiologen zu ermöglichen, Referenzdaten zum Aufbau der Normdatenbank auf einfache Weise übertragen zu können. Daher sollte aufbauend auf der Benutzung von Webbrowsern eine intuitiv zu bedienende Oberfläche erstellt werden. Die Implementierung wurde in [Ni00] in Form eines Java-Applets durchgeführt, das Daten verschlüsselt über das HTTP-Protokoll bzw. die CGI-Schnittstelle an einen Webserver schickt. Auf der Server-Seite werden die gesendeten Daten dann einem Datenbankfrontend für die Auswertung und Speicherung zugängig gemacht.

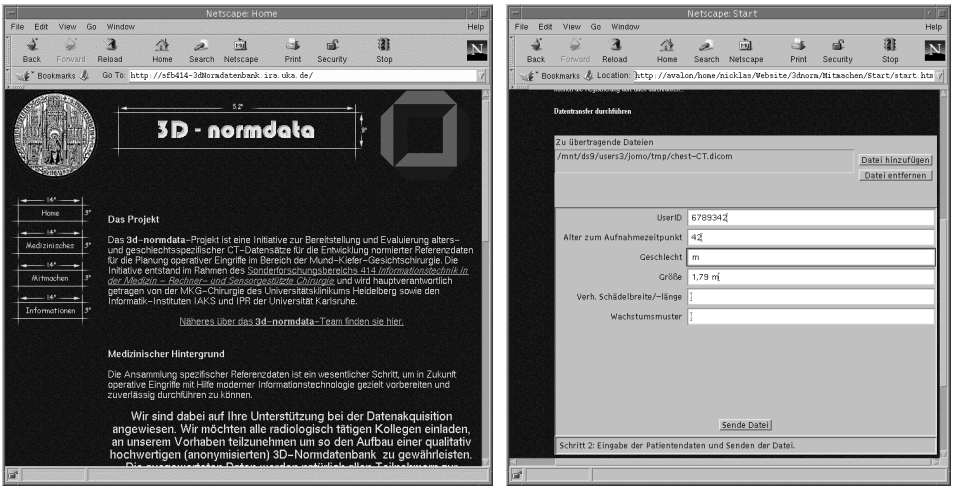

Abbildung 1:Webseite der 3D-Normdatenbank (links) mit dem Datenübertragungsapplet (rechts).

Eine Analyse der Sicherheitsbeziehungen im vorliegenden Forschungsszenario hat gezeigt, dass während der Übertragung eine statische Bindung zwischen Datensender, d. h. dem Mediziner, dem Datensatz und der Datenbank besteht. Nach der Übertragung unterliegt die Zuständigkeit und Verantwortung für die Daten beim Betreiber des Servers. Die Bindung eines Patienten an seine Daten kann vor dem Hintergrund des Forschungsszenarios bereits vor der Übertragung aufgelöst werden. Dies erfolgt mittels der gezielten Anonymisierung aller DICOM-Datenelemente, die für die Aufgabenstellung nicht benötigt werden (Prinzip der minimalen Rechte).
Eine Authentifizierung muss nur von Seiten des Betreibers der Normdatenbank erfolgen, der sich für den verantwortungsvollen Umgang mit gesendeten Daten verbürgt. Der Sender der Daten muss ausschließen können, dass seine Daten in falsche Hände gelangen. Eine Authentifizierung des Senders ist nicht notwendig, da missbräuchlich gesendetes Datenmaterial vom Server durch geeignete Filtermechanismen verworfen werden kann.
Das Protokoll zur Datenübertragung basiert auf einem hybriden Verschlüsselungsverfahren. Das zu übertragende Bildmaterial wird mit Hilfe einer symmetrischen Verschlüsselung (Triple-DES) chiffriert. Die dabei verwendeten Schlüssel werden für jede Übertragung vom Applet neu generiert. Beim Versand von DICOM-Bilddaten wird zusätzlich vor der Übertragung eine automatische Anonymisierung vorgenommen. Die Übertragung des generierten Schlüssels erfolgt mittels eines Public-Key-Verfahrens mit asymmetrischer Verschlüsselung (RSA-Verschlüsselung). Für die RSA-Verschlüsselung wird der öffentliche Schlüssel der Datenbank mit dem Applet mitgeliefert. Die Authentizität dieses Schlüssels wird durch die Unverfälschtheit des Applet-Byte-Codes gewährleistet, der durch eine digitale Signatur überprüfbar ist. Dazu ist das Normdatenbank-System bei einer eingetragenen öffentlichen Zertifizierungsbehörde zertifiziert.

5 Umfassende Sicherheitsmechanismen am Beispiel eines prototypischen klinischen Informationssystems

Die Entwicklung eines Prototyps für ein umfassendes klinisches Informationssystem geht weit über die Problematik der Bereitstellung der Basiskommunikationsmechanismen für die Normdatenbank hinaus. Insbesondere müssen in dem Informationssystem Protokolle und Mechanismen integriert sein, die den Umgang mit dynamischen Bindungen erlauben. Die primäre Fragestellung beim Entwurf von Datenzugriffsmechanismen im System ergibt sich aus der Stellung des Benutzers. Neben der einfachen Registrierung des Benutzers beim System, z. B. über gängige chipkartenbasierte Authentifizierungsdienste, ist das Problem der Verkörperung einer Rolle für die Ausführung von Aktionen von besonderem Interesse. Eine Rolle spiegelt die momentane Funktion des Benutzers wider und wird für die im Folgenden beschriebene Zugriffsregelung benutzt. Ziel ist es, über den rollenbasierten Ansatz konsequent die Organisationsstrukturen und Zuständigkeiten in der Klinik abzubilden.
Für die Verwaltung der auftretenden Rollen ist ein Rollenserver zuständig. Er dient der Registrierung und Zuordnung von Personen zu Rollen und hält die dynamisch veränderlichen Statusinformationen über die einzelnen Rollen. Ver- und Entschlüsselung bei Datenzugriffen obliegen auf Grund dieser Modellierung der Rolle und nicht einer bestimmten Person. Für Chiffrierungszwecke benötigte Schlüssel dürfen jedoch nicht dem Rollenserver bekannt sein, da er sich sonst als beliebiger registrierter Benutzer ausgeben kann und somit universellen Zugriff auf sämtliche verfügbaren Informationen erhält. Zur Bewältigung dieses Sicherheitsrisikos werden Schlüssel und Chiffriermechanismen gekapselt und in Form eines Rollenproxys in der jeweiligen Umgebung des Benutzers abgelegt.
Die Umsetzung der Organisationsstrukturen und Verantwortlichkeiten für Datensätze in einer Klinik ergibt komplexe Regelstrukturen, die für die Auswertung von Zugriffsrechten benötigt werden. Zur Spezifikation dieser Regelstrukturen wurde eine prädikatenlogische Beschreibungssprache geschaffen. Aus bereits bestehenden Regeln und grundlegenden Prädikaten wie z. B. Personenattributen oder Datensatzeigenschaften lassen sich mit Hilfe logischer Verknüpfungen Hierarchien von Regeln konstruieren.
Alle Regeln werden in einem Regelserver gespeichert. Stellt ein Benutzer eine Anfrage zu einem Datensatz muss von einem Rechteserver, der für die Erteilung eines Zugriffsrechts für die jeweilige Anfrage zuständig ist, eine Anzahl möglicher Regeln ausgewählt und einer dritten Instanz, einem Evaluierungsserver, zugeführt werden. Dieser testet die Erfüllbarkeit der Regeln zum Anfragezeitpunkt. Sobald vom Evaluierungsserver die Erfüllung einer Zugriffsregel bekannt gegeben wird, kann vom Rechteserver dem Benutzer ein zertifiziertes Zugriffsrecht für die Anfrage ausgestellt werden. Rechteserver und Evaluierungsserver müssen aus Sicherheitsgründen in zwei unabhängige Instanzen aufgespalten werden, damit sich der Rechteserver nicht eigenmächtig Zugriffsrechte für beliebige Datensätze verschaffen kann.
Für den Mechanismus des Datenzugriffs wurden verschiedene Protokolle entwickelt und jeweils eine Bedrohungsanalyse durchgeführt. Das erste Basisprotokoll (siehe [Br00, Ni00]) stellt ein zyklisches Modell dar. Hauptkomponenten bilden sogenannte Stationen, die vergleichbar mit einem herkömmlichen Server Anfragen entgegennehmen, diese aber nicht an die anfragende Instanz zurückgeben, sondern an weitere Stationen für folgende

Verarbeitungen weiterreichen bis eine vollständig bearbeitete Anfrage von einer letzten Station wieder den Initiator erreicht.
Im ersten Schritt des zyklischen Protokolls wendet sich der Benutzer mit einer Anfrage an eine Datenbankstation. Ein zertifiziertes Zugriffsrecht muss ihm bereits vom Rechteserver erteilt worden sein. Die Datenbankstation liefert in diesem Fall den geforderten Datensatz aus einer angekoppelten Datenbank. Eine Besonderheit ist hierbei, dass die Daten verschlüsselt und gegebenenfalls auch pseudonymisiert abgelegt wurden, so dass unberechtigte Zugriffe und andere Möglichkeiten der Ableitung von Patienteninformationen, insbesondere auch durch Administrationspersonal der Datenbank, ausgeschlossen werden können. Von der Datenbankstation werden die auszuliefernden Daten mit einem vom Rollenproxy des Benutzers gelieferten öffentlichen Übertragungsschlüssels chiffriert. Am Ausgang der Datenbankstation liegen die Daten somit doppelt verschlüsselt vor und werden an eine sogenannte Transferstation weitergegeben.
Die Transferstation hat die Aufgabe, die erste Chiffrierung, mit der die Daten in der Datenbank abgelegt und die mit einem zur Transferstation gehörigen Schlüssel erzeugt worden sind, zu lösen. Zu beachten ist, dass für die doppelte Verschlüsselung kommutative Chiffren eingesetzt werden müssen. Am Ausgang der Transferstation liegen die Daten nur noch einfach verschlüsselt vor und können exklusiv durch den dem anfordernden Rollenproxy zugewiesenen Schlüssel dechiffriert werden. Wie sich aus der Bedrohungsanalyse zeigt, muss für einen umfassenden Schutz der Daten eine zusätzliche, z. B. durch symmetrische Verschlüsselung erzielte, gesicherte Verbindung zwischen der Transferstation und dem Benutzer aufgebaut werden. Abbildung 2 zeigt eine schematische Darstellung des Datenzugriffs mittels des zyklischen Protokolls. Das Protokoll kann sowohl direkt zur Datenverschlüsselung als auch zur Übertragung eines Schlüssels mit einer anschließenden symmetrischen Chiffrierung des Datenstroms (hybride Technik) eingesetzt werden.

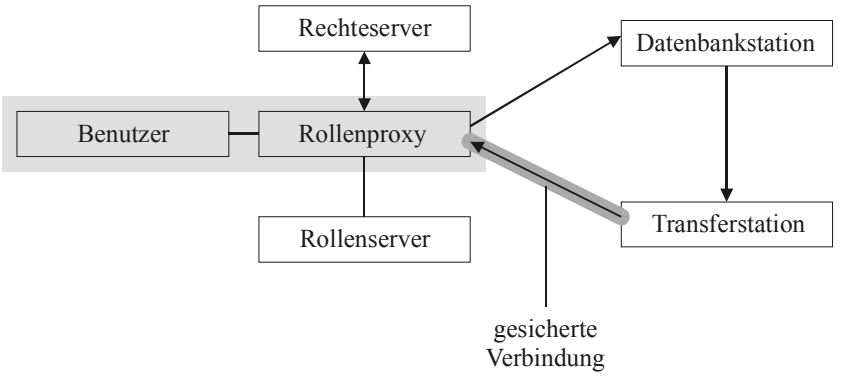

Abbildung 2: schematische Darstellung des Datenzugriffes über das zyklische Protokoll

Als Alternative zum zyklischen Protokoll wurde in [Bl01] ein Mechanismus entwickelt, der auf einem Secret-Sharing-Modell basiert. Anstelle der Stationen kommen hier konventionelle Server zum Einsatz. Die Gewährung von Zugriffsrechten und verschlüsselte Speicherung der Patienteninformationen in einer Datenbank erfolgen hier analog. Um

jedoch zu verhindern, dass eine einzelne Systemkomponente in den Besitz der zur Dechiffrierung benötigten Schlüssel gelangt, wird dieser in mehrere Teilgeheimnisse aufgeteilt und bei mehreren unabhängigen Schlüsselservern hinterlegt (Secret-Sharing-Schema). Bei Vorlage eines gültigen Zugriffsrechts kann sich der Benutzer bzw. sein Rollenproxy von Schlüsselservern die benötigten Geheimnisse einzeln holen und den Schlüssel für die Dechiffrierung des vom Datenbankserver direkt geschickten Datensatzes rekonstruieren. Zusätzlich kann das Verteilungsschema der Schlüsselserver verallgemeinert werden, so dass z. B. nur ein Teil der Schlüsselserver für die vollständige Rekonstruktion des Gesamtschlüssels benötigt wird (sogenannte (k, n)-Schwellwert-Schemata). Der Vorteil des Secret-Sharing-Protokolls gegenüber dem zyklischen Protokoll liegt in der Überschaubarkeit und Einfachheit der Mechanismen. Abbildung 3 zeigt den beschriebenen Datenzugriff über das Secret-Sharing-Modell.

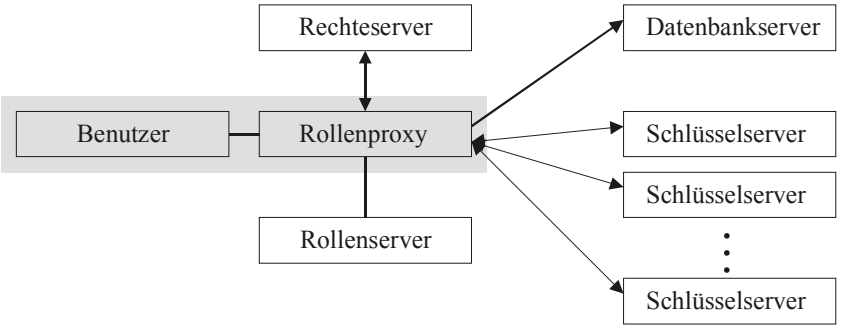

Abbildung 3: schematische Darstellung des Datenzugriffes über das Secret-Sharing Protokoll

Neben den Protokollen zum Datenzugriff wurde eine Vielzahl weiterer elementarer Mechanismen geschaffen. Ein System mehrstufiger Pseudonymisierer stellt die Grundlage für Pseudonymisierungsmechanismen dar, die beispielsweise für indirekte Zertifizierung von Zugriffsrechten bei pseudonymisierten Anfragen erforderlich sind. Eine Folge von Pseudonymisierern, wobei jeder für sich genommen eine Abbildung von Datensatzeinträgen oder Referenzen auf ein Pseudonym und gegebenenfalls die zugehörige Umkehrabbildung vornimmt, kann hintereinander geschaltet werden. Dies gewährleistet, dass das Brechen einzelner Pseudnonymisierer, eine Rekonstruktion der originalen Information noch nicht ermöglicht. Zur Protokollierung und Nachweisbarkeit der Bearbeitung von Dokumenten wurde ein Mechanismus entwickelt, der das Anfügen von Einträgen an einen Datensatz, z. B. bei einem Befundungsvorgang, ermöglicht, wobei die Verfolgbarkeit und Nachweisbarkeit der Bearbeitungsschritte mittels digitaler Signaturen nachvollzogen werden kann.

Die beschriebenen Protokolle und Mechanismen wurden in einem prototypischen Informationssystem mit CORBA und JAVA realisiert. Das Gesamtsystem gliedert sich in eine Mehrschichtenarchitektur. Auf unterster Ebene befindet sich die Realisierung der Zugriffsprotokolle. Sowohl das zyklische als auch das Secret-Sharing-Modell steht als Klassenbibliothek zur Verfügung. Die darüber liegende Schicht stellt die benötigten Instanzen für die gesicherte Datenkommunikation zur Verfügung und wickelt den

Zugriff auf Datensätze unter Zuhilfenahme des Rollen-, Rechte- und Regelsystems ab. Die oberste Schicht dient der Darstellung der Instanzen mit einer graphische Benutzerschnittstelle (Desktop). Insbesondere können hier unterschiedliche Sichten auf Datensätze z. B. in Abhängigkeit der aktuellen Rolle des Benutzers, angezeigt werden (siehe Abb. 4).

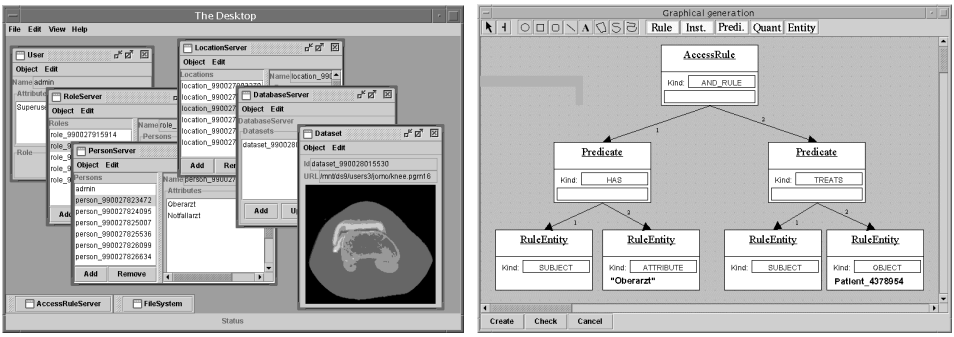

Abbildung 4: Desktop mit Sichten auf mehrere Systemkomponenten (links), Werkzeug zur Definition von Zugriffsregeln (rechts)

6 Ergebnisse und Ausblick

In einem Prototyp wurden neue Grundmechanismen zum Aufbau eines klinischen Informationssystems realisiert, das sich durch eine gesicherte Datenhaltung in Verbindung mit einer flexiblen und dynamischen Abbildung der stark wechselnden heterogenen Organisationsstrukturen im Klinikbetrieb auszeichnet. Hierzu gehört ein umfassender Schutz vor unbefugten Zugriffen auf Datenmaterial durch indirekt gesicherte Speicherung, der bis hin zu Bereichen wie Administration von Datenbanken oder Fernwartungszugriffe durch Fremdfirmen wirksam ist. Die flexiblen Verschlüsselungsmechanismen bilden die Grundlage für Mechanismen einer langfristigen Speicherung. Eine rollenbasierte Benutzermodellierung spiegelt die komplexen Organisationsstrukturen und Zuständigkeiten in der Klinik wieder, die sich sonst nur schwer durch personen- oder gruppenbasierte Benutzermodellierung abbilden lassen. Insbesondere werden die jeweils aktuellen Funktionen und Verantwortlichkeiten des Personals berücksichtigt. Die Gewährung von Zugriffsrechten erfolgt durch dynamische Auswertung spezifizierter Zugriffsregeln. Die Grundmechanismen des Systems wurden formalisiert, hinsichtlich der Sicherheitsanforderungen verifiziert und bei der Durchführung von Datenzugriffen in einfachen Beispielszenarien getestet. Vor einer praktischen Erprobung des Systems im klinischen Betrieb stehen noch der Aufbau eines umfassenden Regelwerks für die Zugriffsberechtigung, die Integration leistungsfähiger Protokollierungsmechanismen zur Verfolgbarkeit und Nachweisbarkeit von Zugriffen sowie Effizienzverbesserungen für den Zugriff auf große Datenmengen aus.

Literaturverzeichnis

[Bl01] Blass, E.-O.: Analyse, Verifikation und Realisierung kryptographischer Protokolle für flexible Zugriffe auf medizinische Datenbanken. Diplomarbeit, Universität Karlsruhe (in Vorbereitung).

[Br00] Brief, J., Däuber, S., Dambier, M., Haimerl, M., Haßfeld, S., Krempien, R., Lukhaub, H., Moldenhauer, J., Münchenberg, J., Nicklas, A., Walz, M., Weisser, G.: 3D-Norm-Data. Workshop „Informationstechnik in der Medizin“, Universität Karlsruhe (Juli 2000).

[HGM00] Haimerl, M., Geiselmann, W., Moldenhauer, J., Walz, M.: Zugriffsregelung in dynamischen Umgebungen – ein Modell für die Medizin. Workshop „Informationstechnik in der Medizin“, Universität Karlsruhe (Juli 2000).

[HW00] Haufe, G., Walz, M.: Anforderungen und Lösungen zur standardisierten und datenschutzkonformen Teleradiologie. In: Jäckel, A. (Hrsg.): Telemedizinführer Deutschland 2001, Minerva KG, Darmstadt (2000) 216–219.

[Ni00] Nicklas, A.: Modellierung und Realisierung gesicherter Datenzugriffe in medizinischen Informationssystemen. Diplomarbeit, Universität Karlsruhe (November 2000).

[Wa00a] Walz, M.: Technikfolgenabschätzung Teleradiologie: Analyse der Rahmenbedingungen und Anforderungen. Habilitationsschrift der Ruprecht-Karls-Universität Heidelberg, Fakultät für Klinische Medizin Mannheim (2000).

[Wa99] Walz, M., Bolte, R., Reimann, C., Haimerl, M., Westermann, M., Georgi, M.: Patientenversorgungs- und datenschutzgerechte Bildkommunikation – ein Widerspruch? 80. Deutscher Röntgenkongress Wiesbaden 1999 in RöFo, Band 70, April 1999, Thieme Verlag (1999).

[Wa00b] Walz, M., Brill, C., Bolte, R., Cramer, U., Wein, B., Reimann, C., Haimerl, M., Weisser, G., Lehmann, K. J., Loose, R.: Teleradiology Requirements and Aims in Germany and Europe: Status at the Beginning of 2000. In: European Radiology **10** 9 (2000) 1472–1482.

[WCB00] Walz, M., Cramer, U. H., Bolte, R.: Rahmenbedingungen elektronischer Bildkommunikation. Geburtshilfe und Frauenheilkunde **60** (2000) M189–M194.

[WMK99] Walz, M., Mildenberger, P., Klose, K. J.: Standardisierte Bildübertragung: Ein wichtiger Schritt in Richtung Teleradiologie und Telemedizin. Radiologe **39** (1999) M77–M79.

[SFB01] Webseite der 3D-Normdatenbank: http://sfb414-3dNormdatenbank.ira.uka.de.