SOLL-Spezifikation aus Sicht der Sicherheit

Malte Grosse
Uni Ulm

Holger Hufschmidt
Uni Saarbrücken

Technischer Bericht A 07/93

Im Rahmen des vom Bundesministeriums für Forschung und Technologie (BMFT) geförderten Projektes KORSO (Korrekte Software) wurden in der Fallstudie HDMS–A (Heterogenious Distributed Management System – Abstract Version) Teile der funktionalen Essenz eines Patientendatenverwaltungsprogramms formal spezifiziert. In diesem Bericht werden Anforderungen an diese funktionale Essenz formuliert, die sich unter dem Aspekt der Sicherheit des Systems ergeben. Hierbei werden auch die gesetzlichen Bestimmungen berücksichtigt.

Introduction

The following report is part of the complex case study HDMS-A, which was done in the KORSO-Project[1] to investigate the algebraic methods for software engineering. HDMS-A is an abstraction of a heterogeneous distributed information management system (HDMS), which is going to be implemented by the PMI[2] for the German Heartdisease Centre in Berlin (DHZB). There exists a complete system analysis [EHK+89] for this medical information system. In the abstraction the modelling was reduced to several medical documents and reports and some of the courses of events.

The investigation was done by several groups; a complete overview gives the report [CHL94]. Due to brewity of this introduction only the main topics are mentioned. Starting from the analysis of the existing courses of events and documents [CKL93] a functional essence [SNM+93] was derived. This together with aspects of safety and security [GH93, Ren94] yield to the requirements specification. In several papers [Nic93, Het93] the courses of events have been inspected and modified, because the use of an information system made former paper charts and reports obsolete. Other aspects of interest were the user interface [Shi94, MZ94], the communication part [BS93] and the development of a data base system for HDMS-A [Con93b, Con93a].

Further results of this case study can be found in [CHL94], there exists as well a complete list of references to the reports, which have been done in this case study and a hint how to obtain them.

---

[1] KORSO stands for Correct Software. This project was funded by the German Ministry of Research and Technology (BMFT).

[2] PMI is the abbreviation for the project group of medical computer science at the TU Berlin.

SOLL-Spezifikation aus Sicht der Sicherheit

Malte Grosse
Uni Ulm

Holger Hufschmidt
Uni Saarbrücken

Dezember 1993

1 Einführung

Mit diesem Paper soll für die SOLL-Spezifikation aus Sicht der Sicherheit eine Grundlage gelegt werden. Es werden zunächst die Anforderungen, die schon von Michael Löwe in der IST-Analyse [Löw92] angegeben wurden, aufgeführt und daraufhin untersucht werden, inwieweit diese in eine SOLL-Spezifikation übertragen werden können. Desweiteren werden die gesetzlichen Bestimmungen behandelt, sowie die Konsequenzen, die sich aus diesen ergeben, aufgelistet. Um die zu erstellende Modellierung gegenüber dem Gesamtsystem abzugrenzen, werden zunächst die Anforderungen an die Hardware und Software aufgeführt. Abschließend wird das Modell von Abadi [ABLP91] vorgestellt, womit eine Modellierung der Zugriffsrechte gemacht wurde.

2 Die Anforderungen aus der Sicht des Anwenders

In dem Handout [Löw92] von Michael Löwe am 23.10.92 wurden eine Reihe von Punkten, die die Sicherheit des Systems betreffen, aufgelistet. Im folgenden soll auf die Anforderungen eingegangen werden. Dazu werden sie noch einmal wieder aufgelistet. Die grundsätzlichen Anforderungen an einen medizinischen Arbeitsplatz sind nach [EHBH89]:

1. Persönlicher Datenschutz muß gewährleistet sein.

2. Die Funktionalität eines computergestützten Arbeitsplatzes muß aus der medizinischen Tätigkeit des Arztes in einer Klinik ableitbar sein.

In [Löw92] wird der Widerspruch aufgezeigt, daß *aus dem ersten Grundsatz sich ableitet, daß elektronisch gespeicherte Patientendaten möglichst nicht kopiert werden dürfen, wie das schon heute für Papierakten gesetzlich geregelt ist.* Ferner leite sich aus dem zweiten Grundsatz ab, daß die Daten auch über Netz verfügbar sein sollen, also damit ständig kopiert werden.
Dieses ist kein großes Problem, da sicherlich ein System modelliert werden kann, daß sicherstellt, daß immer nur ein Original existiert und jeder an seinem Datensichtgerät eine Kopie sieht. Zudem sollte sichergestellt werden, daß kein Benutzer sich eine Kopie anlegen kann, also entweder ausdrucken oder in ein eigenes Verzeichnis hinein (auf letzteres muß auch aufgrund von Zugriffsrechten[1] verzichtet werden).
In einem geschlossen Gebäudekomplex, wie in einem Krankenhaus, können obige Anforderungen sicherlich einfacher realisiert werden, als bei externen Praxen, wo der Arzt sein eigener Systemverwalter ist und damit natürlich in sein System in jeder beliebigen nicht kontrollierbaren Weise eingreifen könnte[2]. Normalerweise wird der Arzt sein dortiges System auch für seine Patienten nutzen: er hat also ein Gesamtsystem mit Abrechnung, Arztbrieferstellung und Dokumentation. Hier ist eine erhebliche Sicherheitslücke für das interne System, die auch nicht einfach in einem Modell abgefangen werden kann.

2.1 Die Anforderung aus Sicht medizinischer Tätigkeiten

In dem Papier von Michael Löwe [Löw92] werden vier Punkte aufgeführt, die aus Sicht der medizinischen Tätigkeit Anforderungen an das Gesamtsystem stellen.

[1] Da solcherart angelegte Dateien nicht mehr den globalen Zugriffsrechten unterliegen, bedeuten solche Dateien ein mögliches Sicherheitsloch.

[2] Nichtsdestotrotz ist ein Arzt zur Verschwiegenheit verpflichtet nach §2 Berufsordnung der Ärztekammer Berlin. Aber nach §11 Absatz 5 er ist zu besonderen Schutz- und Sicherungsmaßnahmen bei der Verwendung von elektronischen Datenträgern verpflichtet.

- **ad II.1**
  Patientenbezogene medizinische Daten müssen immer in den Kontext ihrer Entstehung eingebettet werden können. D.h. Alle Daten müssen zumindest auf einen Patienten und den Zeitpunkt sowie die Methode ihrer Entstehung bezogen sein. (Stichwort: Nachvollziehbarkeit von Entscheidungen)
  Dieser Punkt besagt, daß alle zu einem beliebigen Zeitpunkt zur Verfügung gestellten Daten auch später noch zur Verfügung stehen müssen, damit Entscheidungen nachvollzogen werden können. Hierbei sollte auch berücksichtigt werden, daß dieses System ein Dokument darstellt: in einem Dokument dürfen keine Löschungen vorgenommen werden, sondern nur Streichungen und Ersetzungen (d.h. alle Änderungen müssen mitprotokolliert werden, und der vorherige Zustand ist immer noch rekonstruierbar).

- **ad II.2**
  Alle Daten müssen jederzeit eindeutig der richtigen Person zugeordnet werden können.
  Es bleibt nur anzumerken, daß es schwierig ist, eine Fehleingabe eines Benutzers im nachhinein automatisch zu korrigieren.

- **ad II.3**
  Alle zu einer Person vorhandenen Daten müssen jederzeit schnell auffindbar und einsehbar sein (falls die Zugriffsberechtigung besteht, vgl. I.2)
  Die Forderung dieses Punktes kann nur so aufgefaßt werden, daß Ausfälle (auch von Teilsystemen) mit äußerst geringer Wahrscheinlichkeit passieren können. Neben doppelter oder dreifacher Buchführung (vgl. Flugbuchungssysteme) — und deren komplizierten Updateprozedur — verlangt das auch ein schnelles System (vgl. auch Punkt III.6). Neben dem Bottleneck Kommunikation kann auch die Verschlüsselung von Daten zur Herabsetzung der Geschwindigkeit führen. Daher ist es wichtig, die kritische Zeit in einer Klinik festzustellen, unter Umständen sind Anfragen aus dem OP schneller zu beantworten, als solche auf der Normalstation. (Schätzungsweise dauert es bei der Suche nach einem bestimmten Röntgenbild im Archiv zur Zeit auch mindestens ein halben Tag!). Es wäre auch möglich, die Daten eines OP-Patienten vor

Beginn des Eingriffs lokal zu kopieren, um damit unbegrenzten Zugriff zu gewährleisten: vielleicht muß auch zur Sicherheit ein Ausdruck der wichtigsten Daten eines OP-Patienten in Papierform bereitliegen.
Falls eine Anfrage nur unvollständig erfüllt werden kann, sollte dem Benutzer angezeigt werden, daß noch Daten fehlen. Dieses kann bei verteilter Datenhaltung sicher auftreten.

- **ad II.4**
  Auf der Grundlage eines digitalen Systems muß die Forderung II.3 auch an mehreren Orten einlösbar sein.
  Dieser Punkt betrifft die Verteiltheit und verlangt, daß nicht an örtlich gebundene Sichtgeräte, sondern eher an die Bediener an einem Sichtgerät ausgeliefert wird. Das kann aber auch implizieren, daß sich die Benutzer bei jeder Anfrage immer wieder zu erkennen geben müssen.

2.2 Die Anforderung aus Sicht der sicheren Benutzung

In dem Papier von Michael Löwe [Löw92] werden sechs Punkte aufgeführt, die aus Sicht der sicheren Benutzung als Anforderungen an das Gesamtsystem gestellt werden.

- **ad III.1**
  Eine Fehlbedienung darf unter keinen Umständen zum Verlust von Daten führen (vgl. I.7).
  Der Normalbenutzer hat keine Löschfunktion zur Verfügung. Ein Superuser darf auch nur mit Protokollierung Daten löschen, d.h. diese Daten sind dann auch nicht mehr sichtbar für die Allgemeinheit. Dieses ist z.B. notwendig, wenn ein Benutzer richtige Fieberwerte beim falschen Patienten einträgt. Trotz allem muß auch hier diese Änderung mitprotokolliert werden. Mit Punkt I.7 müssen auch Daten sehr lange verfügbar sein.

- **ad III.2**
  Die Funktionsfähigkeit des Systems sowie sein aktueller Status und die voraussichtliche Dauer der in Arbeit befindlichen Aufgabe muß für den Benutzer jederzeit festzustellen sein.
  Damit ist die Anforderung nicht an ein interaktives System, sondern

an ein batch system gestellt. Der Benutzer darf nicht eine Anfrage abschicken und auf die Antwort warten, sondern soll währenddessen weiterarbeiten können. Solch eine Forderung hängt von der Reaktionszeit des Systems ab. (Wer garantiert nämlich, daß der Anforderer eines Datensatzes noch mit dem momentanen Benutzer übereinstimmt? Sonst muß zweifach identifiziert werden!)

- **ad III.3**
  Ein Ausfall von Teilkomponenten des Systems darf die medizinische Tätigkeit in der Klinik nicht unzumutbar erschweren.
  Der Ausfall sollte nahezu ausgeschlossen werden (vgl. Punkt II.3). Falls dennoch Daten nicht zur Verfügung stehen, sollte dieses dem Benutzer angezeigt werden, so daß er weiterarbeiten kann. Durch mehrfache Buchführung kann der Ausfall von Teilkomponenten fast nahezu ausgeschlossen werden.

- **ad III.4**
  Die Benutzeroberfläche soll modernen ergonomischen Erkenntnissen entsprechen.
  Finden wir auch wichtig, hat aber unseres Erachtens nur periphär was mit Sicherheit zu tun: abgesehen davon, daß ergonomische Arbeitsplätze sicherer zu handhaben sind und Übersichtlichkeit gerade für den Arzt sehr wichtig ist, um gegebenenfalls auch schnell Entscheidungen treffen zu können.

- **ad III.5**
  Die am medizinischen Arbeitsplatz ausgeführten Funktionen müssen weitgehend umkehrbar sein.
  Sind sie nicht, zum Eintragen ist Löschen die umkehrbare Funktion, aber genau das wollen wir nicht, weil aufgrund von eingetragenen Daten bereits Entscheidungen getroffen sein können. Hier gibt es jetzt zwei Möglichkeiten, diese Anforderung zu erfüllen:

  - Derjenige, der Daten eingetragen hat, darf diese wieder löschen, solange kein anderer diese Daten gelesen hat. Das erfordert, für jeden Datensatz ein Eintrag, ob die bereits angeschaut wurden und von wem. Letzteres ist auch unter Datenschutzaspekten bedenklich, weil jetzt die Ärzte überwacht werden können, aufgrund

welcher Daten sie Entscheidungen treffen[3]. Dieses ist sicherlich auch ein nicht zu unterschätzendes Kriterium.

- Derjenige, der Daten einträgt, bekommt eine Maske und kann die Daten einfügen. Sobald er jetzt mit dem Eintragen fertig ist und die Daten dem System zur Verfügung stellt, kann er sie nicht mehr ändern.

Gerade letztere Möglichkeit scheint mir praktikabel und auch ausreichend flexibel für den Benutzer und auf der Systemseite mit nicht zuviel Verwaltungsaufwand verbunden.

- **ad III.6**
  Die Reaktionszeit des Systems muß akzeptabel sein.
  Der Benutzer sollte zu jeder Zeit sehen können, was das System gerade tut (vgl. Punkte II.3 und III.2), da überlange Reaktionszeiten zu Verwirrung und fehlerhafter Benutzung führen können.

3 Aus Gesetzessicht

Gegenstand dieses Kapitels sind die gesetzlichen Rahmenbedingungen, die für das Projekt entscheidend sind. Es wird dieses bewußt getrennt von den offensichtlichen Anforderungen der Benutzer aufgeführt, weil

- die Benutzer nicht mit den Datenschutzbestimmungen vertraut sind
- die Benutzer deswegen auch Anforderungen stellen, die entweder aufgrund der Technik obsolet geworden sind oder den Datenschutzbestimmungen entgegenlaufen
- die Datenschutzbestimmungen bei der momentanen Implementierung zu Diskussionen und Schwierigkeiten des Sicherheitsmodells beitragen [Kut92]

Gerade der letzte Punkt zeigt, daß die Relevanz der gesetzlichen Bestimmungen für solch ein Projekt unterschätzt wird. In den nächsten Abschnitten werden die einzelnen wichtigen Rahmenbedingungen vorgestellt und zum Abschluß zusammengefaßt. Zunächst wird aber auf die Forderungen aus der IST-Analyse eingegangen [Löw92].

[3] Es kann sein, daß die Datenschutzrechte der Ärzte in diesem Fall zurückstehen müßten.

3.1 Die Anforderungen aus Gründen des Datenschutzes

Im folgenden wird auf die einzelnen Punkte der IST-Analyse eingegangen [Löw92].

- **ad I.1**
  Es müssen Mechanismen vorgesehen werden, die eine eindeutige Identifizierung jedes Benutzers dem System gegenüber ermöglichen.
  Eine eindeutige Identifizierung ist nicht nur ein Passwort, sondern es ist mehr: z.B. Scheckkarte oder Stift, der am Datensichtgerät abgelesen wird. Damit kann auch schon rein physikalisch verhindert werden, daß sich jemand an zwei Orten **gleichzeitig** einloggen kann. Soetwas ist sehr sinnvoll, damit kein Benutzer sein Datensichtgerät unbeaufsichtigt läßt und auch nicht mehrere gleichzeitig belegt und somit für andere blockiert(vgl auch die Ausführungen zu Punkt III.2).

- **ad I.2**
  Die Zugriffsrechte auf die Datenbestände im System sind für jeden Benutzer zu regeln und deren Einhaltung sicherzustellen auch über Kommunikationsschnittstellen hinweg.
  Die Zugriffsrechte sind sicher so zu regeln, daß ein Benutzer nur auf die für ihn vorgesehenen Daten zugreifen kann. Dieses muß natürlich auch in einem verteilten System gelten. Eine Frage hierbei ist, ob physikalisch auch Einzelbereiche (z.B. Labore) generell mit eingeschränkter Berechtigung versehen werden. (Dieses würde die Sicherheit erhöhen, weil *a priori* die Geräte mit einer begrenzten Funktionalität ausgestattet sind).

- **ad I.3**
  Die Vertraulichkeit von Patientendaten muß gewährt sein, auch wenn diese in den Besitz nicht autorisierter Personen gelangen (z.B. durch Verschlüsselung). Insbesondere müssen die Wege von und nach außen verschlüsselt werden, führt aber zu einer Herabsetzung der Geschwindigkeit, weil ver- und entschlüsselt werden muß. Aber eigentlich sollten die Daten ja gar nicht in den unautorisierten Besitz gelangen, insbesondere sollten die Benutzer nicht direkt, sondern nur mittels Werkzeugen (Tools) auf Daten zugreifen können.

- **ad I.4**
  Es muß für jeden Benutzer jederzeit nachprüfbar sein, ob die Daten, mit denen er umgeht, korrekt, manipuliert oder verfälscht sind.
  Gemeint ist hier, daß die Authentizität der Daten gewährleistet sein muß, dieses geschieht mit Elektronischen Unterschriften. Wenn die Benutzer nur mittels Werkzeugen auf Daten zugreifen können, müßten sie diese manipulieren, bevor sie Daten manipulieren können. Letzteres ist aber einfacher zu unterbinden, da es sich hier nicht um ein Betriebssystem, sondern nur um ein Informationssystem handelt, so daß den gewöhnlichen Benutzern die Manipulation von Werkzeugen unmöglich gemacht werden kann. Die Systemadministration wäre allerdings in der Lage, hier zu manipulieren, aber das kann nie ausgeschlossen werden.

- **ad I.5**
  Es muß für alle Benutzer zu jedem Zeitpunkt eindeutig feststellbar sein, wer die Daten, mit denen sie umgehen, erzeugt hat (Verfahren in Papierakten z.B. durch Unterschrift).
  Ein Verfahren einer elektronischen Unterschrift böte sich hier an. Damit läßt sich eindeutig feststellen, wer die Daten eingetragen hat und für die Korrektheit verantwortlich ist.

- **ad I.6**
  Patientenbezogene medizinische Daten sollen an dem Ort aufgehoben werden, wo sie angefallen sind, und möglichst selten kopiert werden.
  Diese Forderung soll auf der Papierseite verhindern, daß doppelte Exemplare, die nicht beide fortgeschrieben werden, existieren. Ein Original wird elektronisch schon fast nicht ausreichen (vgl. dreifache Datenbank), läßt sich aber auch einfacher fortschreiben. Jede Kopie, die auf einem Datensichtgerät angezeigt wird, wäre sonst nicht möglich. Warum soll hier auch eine Begrenzung der Resourcen erfolgen? Die Verteiltheit und einfache Duplizierbarkeit ist gerade der Vorteil einer EDV, sonst könnte weiterhin Papier verwendet werden.
  Allerdings muß hier eine Art *elektronisches Original* definiert werden, das die eindeutige und einzige Referenz darstellt. Dieses führt auch dazu, daß jedem Benutzer, der gerade auf ein Dokument zugreift, mitzuteilen ist, daß Daten aktualisiert wurden.

- **ad I.7**
  Die Aufbewahrungszeit patientenbezogener medizinischer Daten muß geregelt sein und vom System in Hinsicht sowohl auf minimale als auch auf maximale Aufbewahrungszeiten eingehalten werden. Nach §11 Absatz 2 der Berufsordnung der Ärztekammer Berlin sind ärztliche Aufzeichnungen mindestens bis zehn Jahre nach Abschluß der Behandlung aufzubewahren. Maximale Aufbewahrungszeiten sind nicht geregelt.

3.2 Das Landeskrankenhausgesetz

An dieser Stelle soll nicht lang und breit das Landeskrankenhausgesetz (LKG) kommentiert werden, sondern nur die für die Sicherheitsanforderungen wichtigen Punkte. §26 Absatz 2 LKG [Dat91] besagt: *Die Krankenhausleitung gewährleistet, daß im Krankenhaus auf Patientendaten nur im erforderlichen Umfang zugegriffen wird. Im Rahmen der Aus-, Fort- und Weiterbildung von Ärzten und Medizinfachpersonen ist zu gewährleisten, daß auf Patientendaten nur insoweit zugegriffen wird, als dies für die dem Berufsbild entsprechenden Funktionen erforderlich ist.* Damit ist gefordert, daß der Zugriff auf die Patientenakte nur denen erlaubt ist, die damit auch wirklich arbeiten.

3.3 Das Landesdatenschutzgesetz

An dieser Stelle soll auf das Berliner Datenschutzgesetz eingegangen werden. Es ist an dieser Stelle insofern wichtig, auf dieses Gesetz einzugehen, weil die folgenden zehn Punkte zu technischen und organisatorischen Maßnahmen in diesem Gesetz §5 Absatz 3 [US91] explizit gefordert werden:

1. Zugangskontrolle
   Unbefugten ist der Zugang zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet werden, zu verwehren.
2. Datenträgerkontrolle
3. Speicherkontrolle
4. Benutzerkontrolle
5. Zugriffskontrolle

6. Übermittlungskontrolle

7. Eingabekontrolle

8. Auftragskontrolle

9. Transportkontrolle

10. Organisationskontrolle
    Die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, daß sie den besonderen Anforderungen des Datenschutzes gerecht wird.

Gerade der erste Punkt läßt vermuten, daß Datensichtgeräte in einem Krankenhaus überhaupt nicht frei, das heißt in einem nicht abgeschlossenen Raum, stehen dürfen. Dieses führt gerade auf einer Station zu erheblichen Komplikationen und einer Arbeitserschwernis, ist aber nach dem 10. Punkt vorgeschrieben. Durch den begrenzten Zugang zu einem Krankenhaus läßt sich vielleicht diese Kontrolle auf den Zutritt zum Krankenhaus verlagern. Solch eine Kontrolle täte dem Datenschutz vielleicht genüge und schränkt die Arbeit im Krankenhaus nicht wesentlich ein.

3.4 Das Bundesdatenschutzgesetz

Durch die obigen Abschnitte ist den Bestimmungen des Bundesdatenschutzgesetzes Rechnung getragen worden, daher werden in diesem Abschnitt keine weiteren Bestimmungen behandelt.

3.5 Die Relevanz der Gesetze

Wie in den vorangegangenen Abschnitten aufgezeigt wurde, sind viele Bestimmungen durch den Einsatz der EDV hinzugekommen, während andere Anforderungen obsolet werden. Auch wenn vom Benutzer die gesetzlichen Anforderungen nicht gestellt werden, müssen diese erfüllt werden. Deshalb sind die gesetzlichen Bestimmungen ein wichtiges Designkriterium und bestimmen nachhaltig, genauso wie die weiteren Sicherheitsanforderungen, die SOLL-Spezifikation. Die gesetzlichen Bestimmungen sollten schon aus dem Grunde beachtet werden, weil eine Änderung im nachherein sehr schwierig, zeitaufwendig und kostenintensiv ist.

4 Voraussetzungen für Hardware und Software

In den bisherigen Abschnitten ging es in der erster Linie darum, die möglichen Lösungsansätze zu den gesetzlichen Bestimmungen und den Anforderungen des Benutzers vorzugeben. Im folgenden werden jetzt konkret die Forderungen angegeben, die für die Sicherheit relevant sind. Im nachfolgenden Abschnitt wird dann die Abgrenzung der Modellierung vorgenommen.
Es wird in diesem Abschnitt eine informelle Festlegung der Funktionalität erfolgen, die für Sicherheitsaspekte relevant ist.

4.1 Physikalische Voraussetzungen

Zu den physikalischen Voraussetzungen zählen sowohl Hardware als auch räumlich bedingte Voraussetzungen. Im folgenden gehen wir davon aus, daß folgende Gegebenheiten vorliegen:

- **Glasfaserkabel**
  Da Ethernet nicht abhörsicher ist [Pom91], sollte eine Medium gewählt werden, das sicherer ist. Zudem hat Glasfaser den Vorteil, daß es eine sehr viel höhere Transportleistung gewährleistet, was beim Transport der Röntgenaufnahmen ohnehin nötig ist. Da der Zugang in ein Krankenhaus relativ gut überwacht werden kann, ist davon auszugehen, daß Glasfaserkabel ausreichend sicher sind. Zudem könnten diese Kabel auch in Überdruckrohren verlegt werden.

- **Workstations**
  Da die Daten verschlüsselt über das Netz laufen sollen, muß jedes Datensichtgerät mit einem Decoder ausgestattet sein. Da auf Hardwaredecoder seitens der USA Exportbeschränkungen[4] existieren, muß dieses Entschlüsseln und Verschlüsseln von Daten mittels Software geschehen. Die Software muß daher in dem Gerät selber vorhanden sein, da sonst die Daten in Klartext übers Netz wandern. Der Benutzer darf aber nicht in den Besitz dieser Software kommen, also muß verhindert werden, daß ein Benutzer Herr über eine Maschine wird, also scheiden vernetzte PCs aus. Die Scheckkarte der Systemverwaltung wird

[4] Exportbeschränkungen werden auf der sogenannten Cocomliste aufgeführt.

benötigt, um einen Rechner wieder zu booten. Dieses ist ein nötiger Eingriff in die Hardware von Workstations.

- **Abgeschlossene Räume oder eingeschränkter Zutritt**
  Sämtliche stationären Datensichtgeräte müssen sich in abgeschlossenen Räumen befinden, oder der Zutritt zum Krankenhaus muß überwacht werden. Ob überhaupt mobile Datensichtgeräte verwendet werden können, ist nicht klar, da jeder Funkverkehr einfach abgehört und auch gestört werden kann, auch wenn er verschlüsselt wird. Zudem wird die Erlaubnis der Bundespost benötigt[Fri].

- **Scheckkarte oder Stift**
  Zur eindeutigen Identifizierung eines Benutzers wird neben einem Passwort eine Scheckkarte oder Stift ausgegeben, die bei der Benutzung eines Datensichtgerätes eingelesen wird und solange darin verweilt, wie der Benutzer arbeitet. Damit ist gewährleistet, daß jeder Verlust der Scheckkarte oder des Stiftes schnell entdeckt wird, und dann gesperrt werden kann, weil der Benutzer nicht arbeiten kann. Auch kann ein Benutzer nur an einem Datensichtgerät zur selben Zeit arbeiten. Es wird somit auch verhindert, daß Benutzer vergessen sich auszuloggen. Durch die Scheckkarte oder den Stift wird die Weitergabe von Kennungen und von Passwörtern verhindert, beziehungsweise zwecklos. Dadurch ist die eindeutige Identifizierung des Benutzers gut gegeben.

- **Dreifache Buchführung**
  Um den Ausfall des Gesamtsystems nahezu unwahrscheinlich zu machen, sollte innerhalb des Gebäudes doppelte Buchführung gemacht werden (vgl. Flugbuchungssysteme). Ferner sollte außerhalb (des Schuttkegels) ein weiteres System auch alles mitprotokollieren. Notstromaggregate sind für eine Klinik eine Selbstverständlichkeit, nur müssen eben auch die Datensichtgeräte und das Rechensystem an diese angeschlossen sein.

- **Externe Benutzer**
  Die Schwierigkeit, externe Benutzer in die Sicherheitsmodellierung einzubinden, wurde schon in den vorherigen Abschnitten beschrieben. Auch werden wohl kaum sämtliche externe Arztpraxen mit Glasfaser angeschlossen werden können, daher müssen die Daten verschlüsselt

werden, die über das Netz nach außen gelangen sollen.
Da über die Geräte der externen Benutzer keine Aussagen gemacht werden können, sollten zusätzliche Schutzmaßnahmen getroffen werden. Z.B. Zugriff auf Daten nur, indem vorher telefonisch/elektronisch eine Anfrage nach bestimmten Daten gemacht wurde, und dann diese Daten von Hand freigegeben wurden, also eventuell auch an den externen Benutzer verschickt wurden.

Diese Bedingungen liefern den Rahmen für die Software-Anforderungen, die im folgenden beschrieben werden. Offensichtlich sind die physikalischen Anforderungen unabhängig von der zu erstellenden Software, allerdings lassen sich gewisse Anforderungen der Benutzer wirksam mit obigen Voraussetzungen erfüllen.

4.2 Software Anforderungen

In diesem Abschnitt sollen die Anforderungen, die an die Funktionalität der Software gestellt werden, beschrieben werden.

- **Dokument**
  Da es sich um ein Dokument handelt, dürfen in diesem System keine Löschungen vorgenommen werden. Es darf nur eingetragen werden und gestrichen werden. Falls falsche Einträge reinkommen, können diese nur mittels des Superusers ungültig, d.h. unsichtbar gesetzt werden, sollten aber immer noch vorhanden sein, aber z.B. der Wert soll nicht sichtbar sein.

- **Einträge in das Dokument**
  Um im nachhinein immer feststellen zu können, wer wann irgendwelche Einträge gemacht hat, sollten bei jedem Eintrag Datum und Urheber mitvermerkt werden. Da mit den Scheckkarten oder Stiften eine eindeutige Identifizierung möglich ist, muß diese nur auf dem Rechner auch umgesetzt werden. So etwas geschieht mit digitalen Unterschriften.

- **Zugriffsrechte**
  Auf die einzelnen Dokumente und auf Operationen, um mit den Dokumenten zu arbeiten, müssen Zugriffsrechte existieren. Gegebenenfalls müssen diese Zugriffsrechte auch vererbbar sein. Keinesfalls dürfen

diese Rechte einmal festgelegt werden und nicht einfach änderbar sein. Vielmehr müssen die Veränderungen auch von Personen, die nicht Superuser sind, vornehmbar sein. Dieses ist z.B. für die Rechte des Nachtpersonals notwendig.

- **Dokumentensystem**
  Das Dokumentensystem darf nicht als aufrufbares Subsystem in einem System existieren, weil dann nämlich die Benutzer Patientendaten in ihre Accounts kopieren könnten und sich damit jeder Sicherheitskontrolle und -stufe entziehen könnten. Es ist daher erforderlich, daß dieses Dokumentensystem für sich alleine existiert, es darf also nicht ein Teilsystem einer für den Benutzer sichtbaren Betriebssystemkomponente sein, sondern muss für den Benutzer das einzige System sein, das er nutzen darf. Somit müssen gegebenenfalls Werkzeuge für Arztbrieferstellung und statistische Auswertung dem Dokumentsystem untergeordnet werden.

- **Verteiltheit**
  Da auf eine Patientenakte von mehreren Datensichtgeräten gleichzeitig zugegriffen werden kann, muß bei Einträgen gewährleistet sein, daß keine zwei Versionen entstehen, sondern immer nur eine. Eine Möglichkeit wäre, die Einträge nur auf Antrag einzufügen und diese auf dem zentralen Rechner zu machen, der diese Anträge sequentialisiert. Je nach Geschwindigkeit wird der Benutzer am Datensichtgerät nicht merken, daß er nicht unmittelbar auf die Patientenakte zugreift.

Der letzte Punkt ist sicherlich strittig und muß diskutiert werden. Es ist auch eine Frage, inwieweit solch eine Anforderung nicht schon auf die Implementierung zielt und nicht ein Teil der SOLL-Spezifikation ist. Die Verteilheit kann zu einem möglichen Sicherheitsloch führen, deshalb ist diese Anforderung an die Software zu stellen und muß unseres Erachtens auch schon in der SOLL-Spezifikation berücksichtigt werden.

5 Die Abgrenzung der Modellierung

Die Modellierung der Sicherheit, die im Rahmen von KORSO vorgenommen werden soll, muß gewisse Gegebenheiten voraussetzen, die dann nicht mitspezifiziert werden. Zu diesen Voraussetzungen gehören alle physikalischen

Anforderungen. Desweiteren sollen Verschlüsselungsalgorithmen und elektronische Unterschriftsalgorithmen nicht mitmodelliert werden, diese werden nur abstrakt als gegeben vorausgesetzt, denn diese Algorithmen lassen sich auch austauschen[5]. Spezifiziert werden sollen die Zugriffsrechte, sowie alle Operationen zum Verändern von Zugriffsrechten. Ferner müssen die Operationen auf den Dokumenten mit den Zugriffsrechten verknüpft werden.

5.1 Software-Architektur

Damit ergibt sich die im folgenden dargestellte globale Software-Architektur, die der Sicht aus Sicherheitsapekten entspricht. Im Detail werden hier nicht die einzelnen möglichen Operationen aufgeführt, sondern nur die verschiedenen Ebenen dargestellt. Die Zugriffsrechte werden an die Tools - oder Toplevelfunktionen - angehängt. Im einzelnen gibt es die folgenden vier Ebenen bei der Software-Architektur (vgl. Abbildung 1):

Abbildung1: Globale Software-Architektur aus der Sicht der Sicherheit

- **Datensichtgeräte**
  Hiermit ist die Verwaltung der Ein-/Ausgabegeräte gemeint.
- **IO-Verwaltung**
  Die Aufgaben der IO-Verwaltung umfaßt die Zugangskontrolle, die Rechtevergabe für die Tools , sowie die Ver- und Entschlüsselung der Daten.
- **Toolbox**
  In der Toolbox werden alle möglichen Tools, die für die verschiedenen Benutzer zur Verfügung stehen, gehalten. Dadurch sind hier einfach neue Tools hinzufügbar. An die Tools werden die Zugriffsrechte geheftet, so daß der Benutzer nur überhaupt solche Tools aufrufen kann, für die er eine Berechtigung hat. Über die Abhängigkeiten der Tools untereinander wird an dieser Stelle nichts ausgesagt, da dieses nicht

[5] Auf gewisse Algorithmen liegt eine Ausfuhrbeschränkung seitens der USA vor. Es ist nicht klar, was das für die konkrete Anwendung bedeutet.

sicherheitsrelevant ist: gemeint ist hiermit, der Benutzer kann nur die Tools direkt aufrufen, für die er eine Berechtigung hat, falls diese sich auf andere Tools abstützen, für die er keine direkte Berechtigung hat, darf er sie auch nur indirekt benutzen[6].

- **Datenbasis**
  Mittels der Tools kann auf die verschlüsselte Datenbasis zugegriffen werden. Wie die Datenbasis organisiert ist, ob verteilt oder zentral, ist für diese Sichtweise aus Sicherheitsgründen irrelevant. Nichtsdestoweniger darf ein Benutzer nur von den Patienten Daten erfahren, für die eine Berechtigung hat.

Mittels dieser globalen Software-Architektur und der Modellierung der Zugriffsrechte mittels des im folgenden Abschnitt dargestellten Modells von Abadi [ABLP91] lassen sich die Forderungen der Zugriffskontrolle beschreiben.

6 Das Modell von Abadi

Abadi stellte in [ABLP91] eine theoretische Grundlage zur Modellierung von Zugriffskontrollmechanismen auf der Basis einer auf einer Auftraggeberalgebra aufbauenden Modallogik vor. Zwei Grundfragen stehen bei der Kontrolle von Zugriffsrechten im Vordergrund :

- Wer spricht ?
- Wer ist berechtigt ?

Die Antwort auf diese Fragen ist üblicherweise ein einfacher *Auftraggeber* (Benutzer oder Maschine). In verteilten Systemen erweitert man den Begriff des Auftraggebers auf

- Kanäle
- Gruppen von Auftraggebern
- Auftraggeber in Rollen

[6] Viele Betriebssysteme erlauben nicht die direkte Benutzung der Verschlüsselungsprozedur, aber beim Eintragen eines Passwortes wird sie indirekt benutzt.

- Auftraggeber als Delegierte von anderen Auftraggebern

Insbesondere werden also Benutzer, Maschinen und Kanäle zunächst nicht unterschieden. Abadi entwickelt eine Auftraggeberalgebra , in der Gruppenbildung, Rollenannahme und Delegation auf formaler Ebene behandelt werden können. Diese wird erweitert durch eine parameterisierte Modallogik, in der *A says s* die informale Aussage *A sagt s* repräsentiert. *s* kann ein Befehl sein (*delete file F*) oder auch nicht (*C's public key ist K*). Diese Logik liegt auch einer Theorie von *Access Control Listen (ACL's)* zugrunde. Eine ACL stellt eine Liste von Auftraggebern dar, die zu einer bestimmten Operation berechtigt sind, und ist gebunden an eine Aussage *s*. Zugriffsrechte werden also an Funktionen und nicht an Dokumente gebunden.

Dieser abstrakte Ansatz stellt nach unserer Meinung aus mehreren Gründen die adäquate Sicht des Problems dar :

- Durch das hohe Abstraktionsniveau werden ad-hoc-Argumente für spezielle Implimentierungen vermieden, was besonders bei heterogenen Systemen wie HDMS-A von Bedeutung ist.

- Eine Spezifikation des in [ABLP91] vorgestellten Algorithmus kann weitgehend unabhängig von der Spezifikation der funktionalen Essenz von HDMS-A erfolgen, lediglich die Möglichkeit des Anhängens von Access Control Listen muß in der Sollspezifikation vorgesehen werden.

- Diese Vorgehensweise bei der Modellierung von Sicherheitsaspekten trägt zu einer möglichst hohen Modularisierung der Gesamtspezifikation von HDMS-A bei und läßt auch den Aspekt der Wiederverwendbarkeit nicht unberücksichtigt.

- Der Artikel von Abadi ermöglicht eine einheitliche Behandlung der durch die Sicherheitsanforderungen I.1 — I.5 auftretenden Aufgaben.

7 Weitere Arbeiten

Die Arbeit der Sicherheitsgruppe stützt sich auf die folgende weitere Arbeiten. Der in [ABLP91] skizzierte Algorithmus wurde konkret in der Arbeit von Renzel beschrieben [Ren94]. Diese Arbeit ist auch mittels des KIV-Systems [Rei92] verifiziert [Ste93] worden. Desweiteren wurde ein Spezifikation von ACLs in Obscure [LZ92] gemacht [Huf93].

8 Danksagung

Wir möchten uns bei allen bedanken, die uns bei der Erstellung dieses Berichtes geholfen haben, insbesondere Felix Cornelius*, Markus Klar* und Ralf Kutsche†. Ferner gilt unser Dank auch Michael Löwe*, Martin Strecker‡, und Andreas Dyballa‡, die uns mit ihren Anregungen und Kritiken zu Vorversionen entscheidend unterstützt haben.

Literatur

[ABLP91] M. Abadi, M. Burrows, B. Lampson, and G. Plotkin. A calculus for access control in distributed systems. In *Proceedings CRYPTO 91*, 1991.

[BS93] J. Bohn and M. Schulte. Entwicklung von Spezifikationen für das HDMS-A Basismodell aus einer gegebenen Anfangsspezifikation mittels Transformation. Interim Report of the Diploma Thesis, 55 pages, Universität Oldenburg, December 1993.

[CHL94] F. Cornelius, H. Hußmann, and M. Löwe. The KORSO Case Study for Software Engineering with Formal Methods: A Medical Information System. Technical Report 94-5, Technische Universität Berlin, February 1994. to appear.

*TU-Berlin
†PMI Berlin
‡Universität Ulm

[CKL93] F. Cornelius, M. Klar, and M. Löwe. Ein Fallbeispiel für KORSO: Ist–Analyse HDMS-A. Technical Report 93-28, Technische Universität Berlin, 1993.

[Con93a] S. Conrad. Einbindung eines bestehenden Datenbanksystems in einen formalen Software–Entwicklungsprozeß — ein Beitrag zur HDMS-A–Fallstudie. In H.-D. Ehrich, editor, *Beiträge zu* KORSO- *und TROLL light–Fallstudien*, pages 1–14. Technische Universität Braunschweig, Informatik–Bericht 93–11, 1993.

[Con93b] S. Conrad. Spezifikation eines vereinfachten Datenbanksystems — ein Beitrag zur HDMS-A–Fallstudie. In H.-D. Ehrich, editor, *Beiträge zu* KORSO- *und TROLL light–Fallstudien*, pages 15–26. Technische Universität Braunschweig, Informatik–Bericht 93–11, 1993.

[Dat91] Berliner Datenschutzbeauftragter. *Gesetze zum Datenschutz.* Kupijai und Prochnow, Berlin, 1991.

[EHBH89] E.Fleck, H.Hansen, B.Mahr, and H.Oswald. Anforderungen an computerunterstützte medizinische Arbeitsplätze. Research Report 89-01, PMI-Berlin, 1989.

[EHK+89] M. Eiermacher, H. Hansen, R. Kutsche, H. Ogrodowczyk, C. Ohm, D. Paparoditis, C. Rost, and C. Strzyz. Auswertung der Systemanalyse. Technical Report 89-17, PMI - Technische Universität Berlin, 1989. internal working report.

[Fri] M. Frieling. Der Computer kommt ans Krankenbett. Süddeutsche Zeitung vom 23. November 1992.

[GH93] M. Grosse and H. Hufschmidt. SOLL–Spezifikation aus Sicht der Sicherheit. Technical Report A/07/93, Universität des Saarlandes, Saarbrücken, December 1993.

[Het93] R. Hettler. Übersetzung von E/R-Modellen nach SPECTRUM. Technical Report TUM-I9333, Technische Universität München, 1993.

[Huf93] H. Hufschmidt. Spezifikation eines Zugriffs–Kontroll–Algorithmus in OBSCURE . Interner Arbeitsbericht WP 93/44, Universität des Saarlandes, July 1993.

[Kut92] R.D. Kutsche. Personal communication, Dezember 1992.

[Löw92] M. Löwe. Ein Fallbeispiel für KORSO: — IST-Analyse für HDMS-A —. Verteilt auf dem KORSO-Treffen am 23.Oktober 1992 in München, Oktober 1992.

[LZ92] J. Loeckx and J. Zeyer. Das OBSCURE-System. Working Paper, Uni des Saarlandes, April 1992.

[MZ94] M. Mehlich and W. Zhang. Specifying Interactive Components for Configuratiing Graphical User Interfaces. Technical Report 9401, Ludwig-Maximilians-Universität München, 1994.

[Nic93] F. Nickl. Ablaufspezifikation durch Datenflußmodellierung und stromverarbeitende Funktionen. Technical Report TUM-I9334, Technische Universität München, 1993.

[Pom91] K. Pommerening. *Datenschutz und Datensicherheit.* BI-Wissenschaft, Mannheim, 1991.

[Rei92] W. Reif. The KIV-System: Systematic Construction of Verified Software. In D. Kapur, editor, *11th Conference on Automated Deduction (CADE).* Springer LNCS, 1992.

[Ren94] K. Renzel. Formale Beschreibung von Sicherheitsaspekten für das Fallbeispiel HDMS-A. Technical Report 9402, Ludwig-Maximilians Universität Munich, January 1994.

[Shi94] H. Shi. Benutzerschnittstelle und -Interaktion für die HK-Untersuchung. Technical Report at the Universität Bremen, to appear, February 1994.

[SNM+93] O. Slotosch, F. Nickl, S. Merz, H. Hußmann, and R. Hettler. Die funktionale Essenz von HDMS-A. Technical Report TUM-I9335, Technische Universität München, 1993.

[Ste93] K. Stenzel. A Verified Access Control Model. Technical Report 26/93, Fakultät für Informatik, Universität Karlsruhe, Germany, December 1993.

[US91] U.Dammann and S.Simitis. *Bundesdatenschutzgesetz(BDSG) mit Landesdatenschutzgesetz und Internationalen Vorschriften.* Nomos Verlagsgesellschaft, Baden-Baden, 1991.