NTNU
Innovation and Creativity

Access Control in Heterogenous Health Care Systems

A comparison of Role Based Access Control Versus Decision Based Access Control

Gaute Magnussen
Stig Stavik

Master of Science in Computer Science
Submission date: May 2006
Supervisor: Torbjørn Skramstad, IDI
Co-supervisor: Inger Anne Tøndel, SINTEF IKT

Norwegian University of Science and Technology
Department of Computer and Information Science

Problem Description

In hospitals there are a myriad of different IT-systems (often several hundreds), and many of these systems have different access control regimes and security levels. Several hospitals work on integrating the most important systems, and this results in new challenges which are also present within other domains. This task aims at analyzing access control mechanisms in existing systems at health institutions. This will result in an overview which can be used to model integration strategies with a focus on access control. The methodology will be based on both quantitative and qualitative analysis methods. The task will also consist of an introductory literature study. The task is part of the research project iAccess (Integrated Access Control for Health Care Information Systems) iAccesswhich is performed by SINTEF, NTNU and UiO. iAccess is cooperating with HEMIT and Rikshospitalet/Radiumhospitalet, and the student will have the opportunity to collect information from these organisations.

Assignment given: 2006-01-20
Supervisor: Torbjørn Skramstad, IDI

Access Control in Heterogenous Health Care Systems

A Comparison of Role Based Access Control Versus Decision Based Access Control

Gaute Magnussen
<gaute.magnussen@idi.ntnu.no>

Stig Stavik
<stig.stavik@idi.ntnu.no>

Teaching Supervisor:
Inger Anne Tøndel
<inger.a.tondel@sintef.no>

May 31, 2006

Department of Computer and Information Science
Norwegian University of Science and Technology

Abstract

Role based access control (RBAC) is widely used in health care systems today. Some of the biggest systems in use at Norwegian hospitals utilizes role based integration. The basic concept of RBAC is that users are assigned to roles, permissions are assigned to roles and users acquire permissions by being members of roles. An alternative approach to the role based access distribution, is that information should be available only to those who are taking active part in a patient's treatment. This approach is called decision based access control (DBAC). While some RBAC implementations grant access to a groups of people by ward, DBAC ensures that access to relevant parts of the patient's medical record is given for treatment purposes regardless of which department the health care worker belongs to.

Until now the granularity which the legal framework describes has been difficult to follow. The practical approach has been to grant access to entire wards or organizational units in which the patient currently resides. Due to the protection of personal privacy, it is not acceptable that any medical record is available to every clinician at all times.

The most important reason to implement DBAC where RBAC exists today, is to get an access control model that is more dynamic. The users should have the access they need to perform their job at all times, but not more access than needed. With RBAC, practice has shown that it is very hard to make dynamic access rules when properties such as time and tasks of an employee's work change. This study reveals that pretty much all security measures in the RBAC systems can be overridden by the use of emergency access features. These features are used extensively in everyday work at the hospitals, and thereby creates a security risk. At the same time conformance with the legal framework is not maintained.

Two scenarios are simulated in a fictional RBAC and DBAC environment in this report. The results of the simulation show that a complete audit of the logs containing access right enhancements in the RBAC environment is unfeasible at a large hospital, and even checking a few percent of the entries is also a very large job. Changing from RBAC to DBAC would probably affect this situation to the better. Some economical advantages are also pointed out. If a change is made, a considerable amount of time that is used by health care workers to unblock access to information they need in their everyday work will be saved.

Preface

This report is the result of a master thesis written during the spring semester of 2006 by two students at The Norwegian University of Science and Technology, Department of Computer and Information Science.

Original Assignment

In hospitals there are a myriad of different IT-systems (often several hundreds), and many of these systems have different access control regimes and security levels. Several hospitals work on integrating the most important systems, and this results in new challenges which are also present within other domains. This task aims at analyzing access control mechanisms in existing systems at health institutions. This will result in an overview which can be used to model integration strategies with a focus on access control. The methodology will be based on both quantitative and qualitative analysis methods. The task will also consist of an introductory literature study. The task is part of the research project iAccess (Integrated Access Control for Health Care Information Systems) [6] which is performed by SINTEF, NTNU and UiO. iAccess is cooperating with HEMIT and Rikshospitalet/Radiumhospitalet, and the student will have the opportunity to collect information from these organisations.

Changes

During our investigation we realised that several hospital are dissatisfied with the existing access control regime, and are planning new solutions in order to improve the situation. In agreement with SINTEF, the assignment was focused on comparing the typical solutions of today with a new and upcoming model - Decision Based Access Control (DBAC). To quantify some of the differences between the access schemes would be an appreciated contribution both to the iAccess project and to the hospitals trying to predict the impact of this transition.

Contents

List of Figures

List of Tables

Part I

Theory

CHAPTER 1
INTRODUCTION

The increase in computerization means that health information about patients often are available in electronic form. As systems dealing with medical technology often is notoriously heterogenous in nature, an increase for solutions that can cope with this distributed heterogeneity is required. Information resides in different, nonintegrated systems and shared delivery of health care services depends to a large extent on the ability to share information between health professionals and the ability to support shared access to health care records. In such an environment, the physical limitations of the paper based record that restrict access to a single user in a single location at one time quickly becomes an obstacle.

There are a lot of different clinical systems in use by different health care institutions today. The ability to collect health data that is distributed across heterogeneous computing systems is therefore an important task in modern hospitals. A lot of effort is made to be able to implement access control mechanisms which reflect the diversity of these systems and information they provide. There are however difficulties related to implementing access control mechanisms which are both efficient to use while ensuring the legal framework stated by the different laws connected to health care services is followed.

Comparing the expressive power of of different access control models is recognized as a fundamental problem in information security, and is studied extensively in the litterature [49]. Studies related to different access control models' impact on time and cost in health care institutions is however sparsely documented. This report will therefore give a comparison of two different access control mechanisms. Based on a set of key attributes, two different scenarios will be covered in order to investigate the impact on time and cost related to choice of access control scheme depending on the size of the institution.

1.1 EXCHANGE AND DISTRIBUTION OF HEALTH CARE INFORMATION

Patients who are admitted to Norwegian hospitals have a number of options which in turn implies that health care workers at different locations are in need of certain parts of the subject's medical record in order to provide the right services and care. Patients can choose what hospital they want to go to when they are admitted. In addition, different hospitals are specialized in different fields. This results in transfers of admitted patients both scheduled and when something acute occurs to the patient which requires special treatment offered elsewhere. Hospitals tend to share responsibility and treatment for patients in need of special medical treatment. This is for example sometimes the case when dealing with patients who are being treated for cancer, and in acute situations when an admittance is made on another hospital than the patient normally would be brought to.

1.2 LEGAL ISSUES RELATED TO PATIENT INFORMATION

There are several things that are yet to be sorted out with regards to current health care regulations and laws in Norway [1]. Client confidentiality is however fundamental and must be maintained by all health care personnel. Any information handed over or shared by a health care worker to another is considered a breach in conformity. Exceptions are made in cases where cooperation between multiple health care professionals are required to offer treatment. Approval from the patient itself can also give the health care worker the option to share parts of the information needed by other health care workers during the period of treatment.

The legal framework in Norway states a series of paragraphes which dictates how much information a health care worker is entitled to. There is an ongoing debate [44] which rises the finger on the fact that health care personnel get more access to patients records than necessary.

1.3 OVERRIDING THE BASIC ACCESS CONTROL LEVELS

In the health sector, there is also a need of enhancing access levels some times. In emergency situations, patient records may be needed in a hurry to ensure the well being of a patient. In such occurrences the systems in use should have a way to override the basic access control levels. Such a mechanism does require extensive logging and checking of logs, to ensure there is no misuse of the feature. This feature will for example be needed when a patient is moved to a new ward in a hurry because of an acute matter. Patient records then need to be accessed even when there is no time to transfer the patient on the computer system. There is also a need for an extensive follow up of this feature, so that users are unable to exploit it, for instance to read the records of their neighbours or friends. This is explained further in section 3.4.

1.4 CONTRIBUTION TO THE IACCESS PROJECT

The iAccess project [6] is founded by The Research Council of Norway [13] and is a part of their security program. iAccess is a research project which looks into how different access control mechanisms in health care systems can be integrated. The parties involved in this project are:

- The Norwegian University of Science and Technology, The Department of Computer and Information Science
- The University of Oslo, Section for Information Technology and Administrative Systems
- SINTEF, Department of Information and Communication Technology

1.4.1 The aim of the report

The contribution this assignment offers to the iAccess project, is the comparison of two access control mechanisms in hospitals of different sizes. The role based access control (RBAC)

described in section 2.1.5 mechanism is used in large health care systems in use at Rikshospitalet such as Klinisk portal, presented in section 5.2.1. The expressive power of a basic RBAC model has proved itself not to be powerful enough to comply with the work flow and legal framework which apply in Norwegian hospitals. A new decision based access control (DBAC) model has therefore emerged in order to offer better conformance with the work processes at the institutions. By making a comparison methodology for these access models in terms of time used on administrating the systems and the time spent in everyday use, a clarification to possible benefits and drawbacks in the two mechanisms may be revealed.

1.4.2 Who can benefit from our work?

Hospitals using electronic health care record (EHR) systems or hospitals on the edge of doing so, may find this report useful when an evaluation of systems or special implementations are made. The concept of DBAC is not a mature area, and few publications cover this concept. The methodology represented in this report may therefore be one step in the direction of getting this mechanism recognized as an alternative to other access control mechanisms implemented in current systems.

1.5 REPORT OUTLINE

We have divided this report in eleven different chapters within three parts. These are:

Part 1 – Theory
Chapter 1 – Introduction
This first chapter discusses the project background, our main motivation and our research goals.
Chapter 2 – Access Control and Access Distribution
The goal of this chapter is to point out some of the principles of how access control mechanisms work.
Chapter 3 – Access Control in Health Care Systems
This chapter discusses access control in the health care environment. It describes what the health care sector needs from it's access control mechanism.
Chapter 4 – The RBAC Model Versus the DBAC Model
In this chapter a description of how a change from role based access control (RBAC) to decision based access control (DBAC) will affect users, administrators and cost. We also explain a motivation for changing access control mechanism.
Chapter 5 – Current attempts on integration of access control in heterogenous systems
Different software implementations and models aimed at the health sector are discussed in this chapter.

Part 2 – Methodology
Chapter 6 – Defining areas to evaluate
This chapter describes which areas we have chosen to look for changes when changing access control models and why we chose them.
Chapter 7 – Identifying evaluation parameters

In this chapter we take a look at which parameters are needed to get results in the chosen areas described in the previous chapter.

Chapter 8 – Simulation

This chapter looks at two scenarios in two hospitals, and show how different RBAC and DBAC will perform at different hospitals.

Part 3 – Discussion and Conclusion

Chapter 9 – Discussion

The main focus in this chapter is a discussion of how a change of access model will affect different hospitals.

Chapter 10 – Conclusion

This chapter summarizes and concludes our work.

Chapter 11 – Future work

The last chapter of this report discusses future work within this field. It also suggests how the findings in our report can be used in further research.

CHAPTER 2
ACCESS CONTROL AND ACCESS DISTRIBUTION

An access control system enforces a policy on who may access what resources and in what manner on a system [49]. This chapter will cover some common access schemes and protocols frequently used in systems on the marked today. A short explanation on how these work and their use is described to give an introduction on how they work and what operations they perform.

2.1 COMMON ACCESS SCHEMES

Within the field of computer security, there are some well known access schemes which are relevant to this project report. Some of the most relevant to this project are described here.

2.1.1 The Principle of Least Privilege

The principle of least privilege is an old administrative practice of assigning permissions to users which holds that each principal should be accorded the minimum access needed to accomplish its task [43]. This avoids the problem of users having the ability to perform unnecessary, unwanted or harmful actions. Clearly, richer notions of "minimum access" allow the principle of least privilege to discriminate better between those actions that should and those that should not be allowed. An administrator may want to have the powers of a normal user most of the time, and exercise his extraordinary powers only when needed. For example, users of the UNIX operating system with system manager privileges typically run with their own, normal identity when that suffices, in order to avoid costly mistakes. When a principal wishes to run a piece of untrusted software, he should be able to invoke it with reduced powers [17]. It is important that the untrusted code should not be able to increase its powers beyond those granted initially. This is done in capability systems by restricting capabilities before passing them across address spaces and by passing as few capabilities as possible. In timesharing systems it is common for untrusted software to be tested with unprivileged user accounts that are used for no other purpose [45].

Figure 2.1 illustrates very simplified how the principle of least privilege may be implemented at a hospital. The clinician needs access to medical records, but the reception clerk does not and is therefore not able to access them. However the clerk at the front desk needs access to the complete list of employees at the institution, and so does the people dealing with accounting. The accounting person also needs access to the employees' salaries to be able to manage

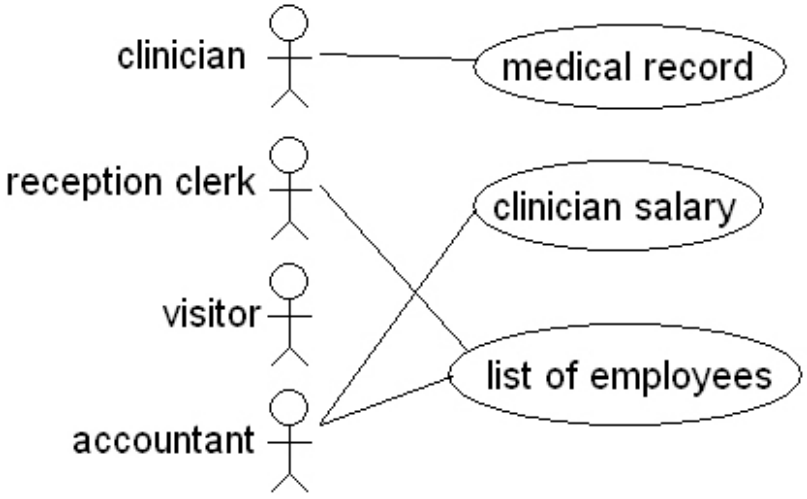

Figure 2.1: The principle of least privilege applied to a health care environment.

payment. The visitor does normally not need access to any of the mentioned objects, and is therefore denied access if he should request them.

2.1.2 Domain Based Access Control

Traditionally, a domain is a limited area or community which share some properties or special interests. In computer science, the definition expresses that a domain is a group of computers linked together in the same virtual or non-virtual network [47], and the concept can be extended to contain the people in it as well. The heart of the arrangement is a directory database containing information on user accounts, groups of users and computer accounts. That database controls the users' access to shared resources. Each user has an account in the domain database, instead of an account on each server. This simplifies user access because when the user logs on to the domain, the permissions assigned to the user is valid across the entire domain. The need to log on separately to each server in the domain is therefore eliminated. Administrators benefit as well as they create and manage one set of accounts in the domain instead of multiple accounts on multiple servers [47].

2.1.3 User Based Access Control

The notion of user identity is probably the most pervasive concept in access control modelling. When access based on user accounts is used, permissions is given directly to each user. Each user has a distinct set of permissions and they do not rely on groups that may be changed. Access based on user accounts are easy to make, but can be very complex to maintain in large systems [31].

Figure 2.2 illustrates how the user based access control authorization maps each subject into an equivalence class based on their user attributes. Based on these equivalence classes and the

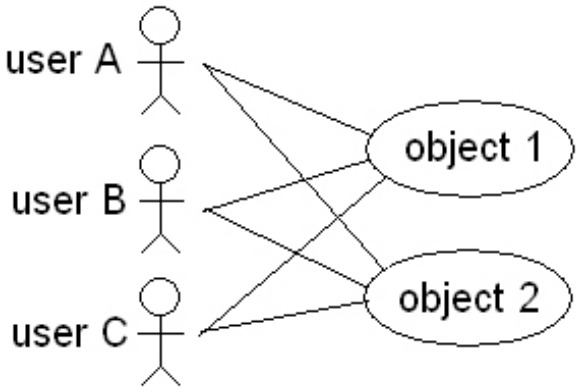

Figure 2.2: Generalized user based access control

object identity, permission to system resources are granted [48]. This results in a higher workload for the administrators of the system. If all normal users have access to a new program, the administrator has to add each user to the program's access list.

2.1.4 Group Based Access Control

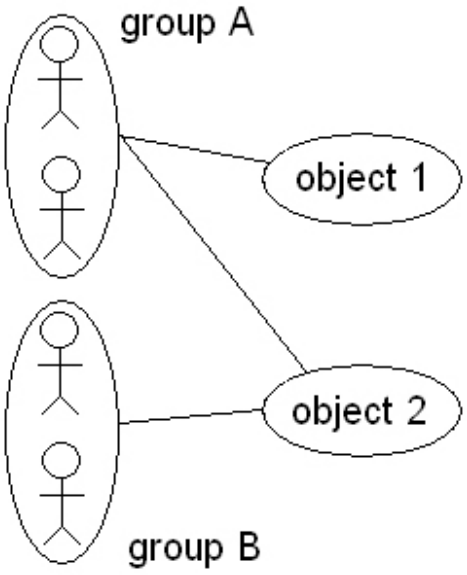

Figure 2.3: Group based access control

In group based access control, users are organized into different groups [50]. Figure 2.3 illustrates how a user inherits all the privileges of the groups he is a member of. This makes maintenance of user privileges easier than for user based access, since an administrator can change the access rights of multiple users by changing the privileges of the groups they belong to.

Access permissions on documents and other relevant parts of the system are granted to user

groups for specific operations. User groups can be used to model roles by, for instance, assigning a job function name to a group and defining many subgroups for various tasks [50].

2.1.5 Role Based Access Control (RBAC)

RBAC is widely used in health care systems today [6]. Some of the biggest systems in use e.g. DocuLive [2] uses a role based integration. This is why this concept is more thoroughly discussed here than some of the other access control mechanisms.

The concept of RBAC is relatively simple and is similar in many ways to the group based access control discussed in section 2.1.4. Access to different parts of a computer system is based on a user's role in the organization.

Simple forms of handling access this way dates back to the 1970s, when implementations were made in business organizations and commercial computer applications [26]. Today RBAC is a widespread and well known concept. A role exists as a structure separate from the structure which describe the user. The different roles should adhere the principle of least privilege in which a role is created with minimum permissions in specification of duty requirements as described in 2.1.1. The basic concept of RBAC is that users are assigned to roles, permissions are assigned to roles and users acquire permissions by being members of roles [26].

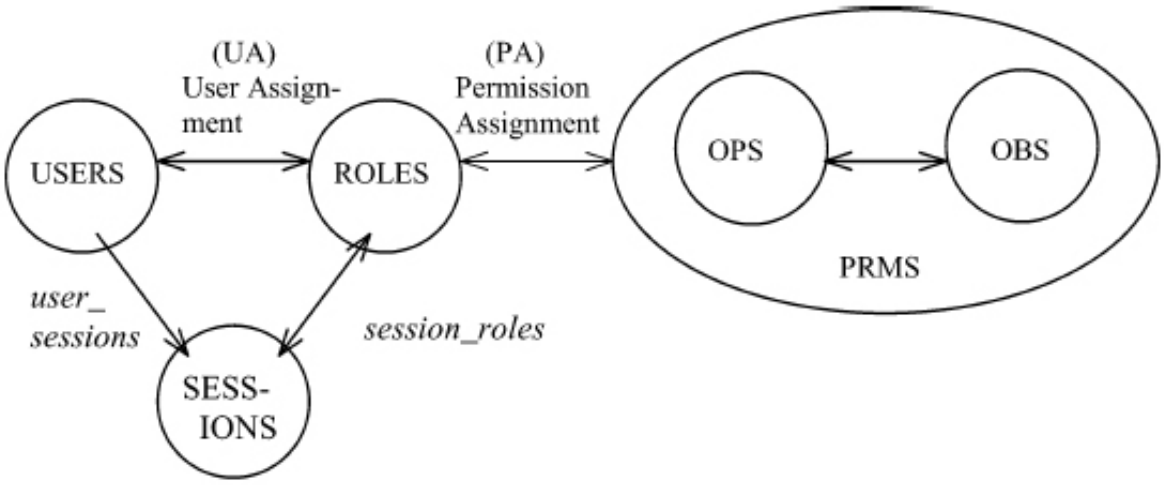

Figure 2.4: The core of the RBAC model [25]

The core RBAC model relations are defined in figure 2.4 as a part of the proposed standard [25] by Ferraiolo et al. The core includes sets of five basic data elements called users (USERS), roles (ROLES), objects (OBS), operations (OPS) and permissions (PRMS). The model as a whole is fundamentally defined in terms of individual users being assigned to roles and permissions being assigned to roles.

Figure 2.5 can be found in a draft [37] presented by the RBAC Task Group [9]. It illustrates the relationship between role groups, work profiles and functional roles consistent with the established standard for role base access control [22].

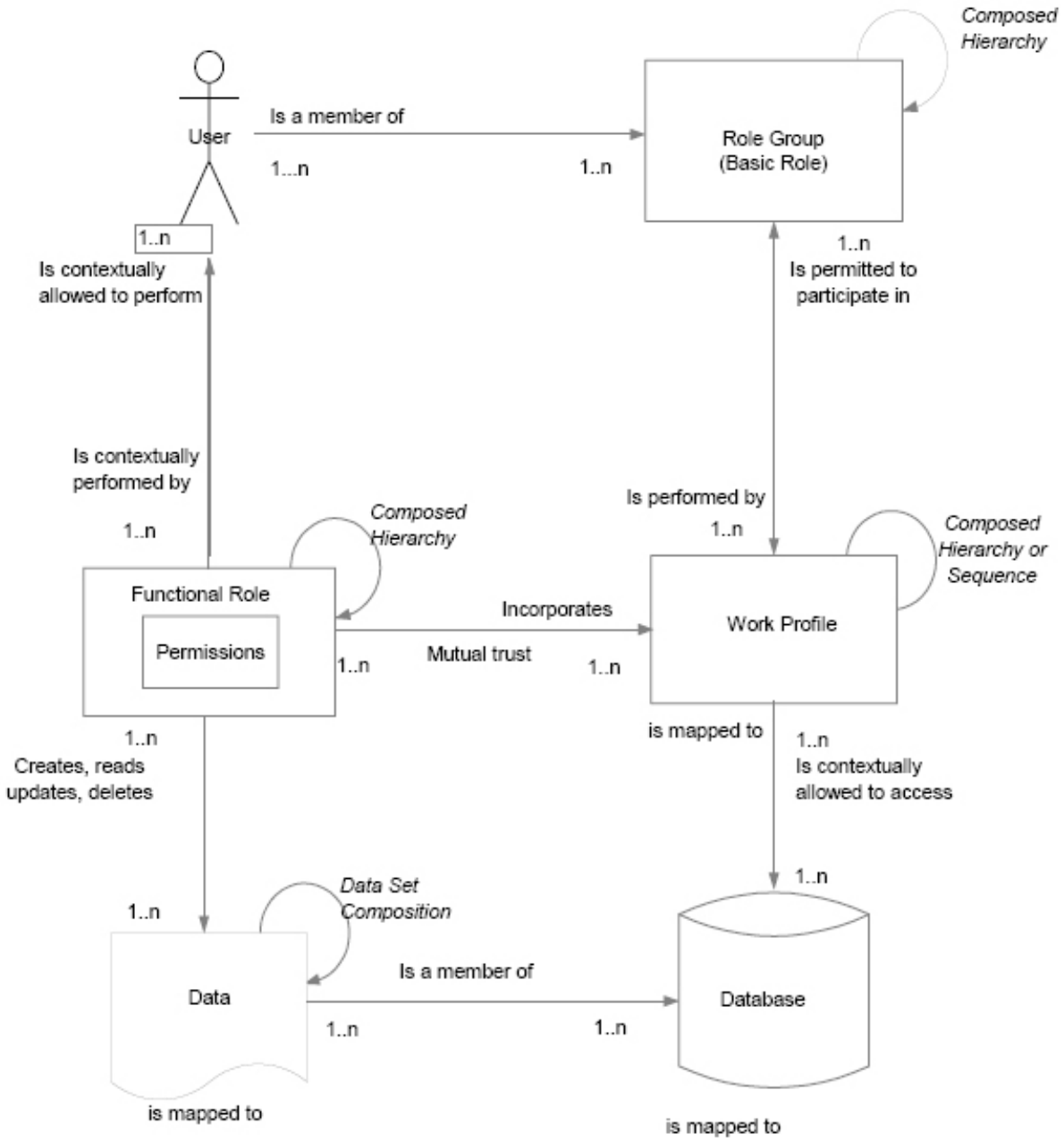

Figure 2.5: Role Engineering Model [37]

The ASTM Standard Guide for Information Access Privileges to Health Information [20] represents healthcare basic roles suitable for use in the proposed draft. Some healthcare basic role examples include: Physician, Pharmacist, Advanced Practice Registered Nurse, and Ward Clerk. These are basic roles that do not necessarily specify what the user can do in the system. While these ASTM standards are oriented to healthcare, the concepts pertain to any business area.

Role Hierarchies

There are three primary kinds of role hierarchies which might exist in an organization [36].

- The *isa* role hierarchy, based on generalization.
- The *activity* role hierarchy, based on aggregation.
- The *supervision* role hierarchy, based on the organizational hierarchy of positions.

The *isa* relationship also known as generalization, is covered in detail in an article by *Sandhu et al.* [42]. An example of generalization would be that a **PrimaryCarePhysician *isa* Pysician *isa* HealthCareProvider**. Every one of the roles mentioned are more general than the previous one, and they constitute a partial order.

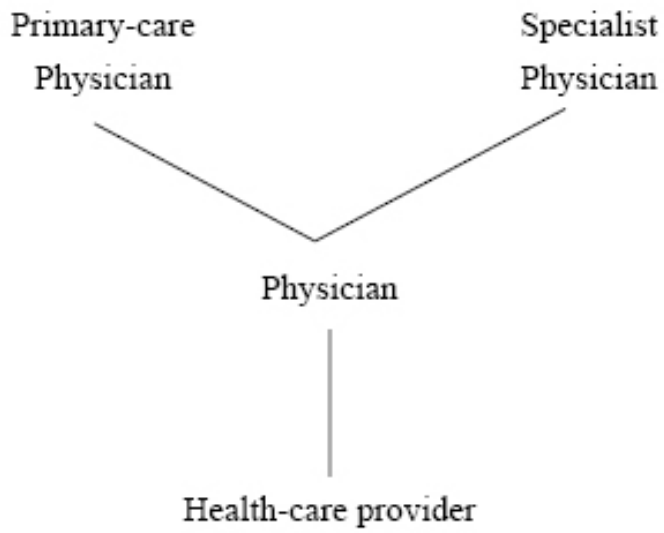

Figure 2.6: RBAC hierarchies [42]

Figure 2.6 gives an example of a hierarchy consisting of health care personnel. The `Physician` role is superior to `Health-care provider` and inherits all of this role's permissions. The `Physician` role can have permissions in addition to those inherited from the `Health-care provider` role. Inheritance of permissions is transitive so, the `Primary-care physician` role inherits permissions from the `Physician` and `Health-care provider` roles. `Primary-care physician` and `Specialist physician` both inherit permissions from the `Physician` role, but each one of these will have different permissions directly assigned to it.

Assigning multiple roles to an identity

In the RBAC standard [22] the requirements that user role and permission role assignment can be many-to-many are included. The same user can be assigned to many roles and a single role can have many users. Similarly, for permissions, a single permission can be assigned to many roles and a single role can be assigned to many permissions. Finally, it is required that users are able to simultaneously exercise permissions of multiple roles. This precludes products that restrict users to activation of one role at a time.

Temporal constraints in RBAC

In some systems, it is important only to allow a role access to a resource in a restricted time interval. This kind of time based access restriction is well suited for use in the health care sector. There are two time related concepts of temporal constraints. The first one is a periodic time constraint, and the other one is a duration constraint. It may be useful to restrict access to patient records to the time interval in which a health care employee is assigned to a shift to ensure that patient privacy is as tight as possible. An example of a periodic constraint is stated in a book by Ferraiolo et al. [26] with the following syntax:

```
(([1-Feb-2006,31-Mar-2006], 22-06), enable doctor-on-call)
```

This would indicate that this particular doctor role only can be enabled between 10 P.M. and 6 A.M. during the period February 1st to March 31st during 2006.

An example of the other constraint related to time is the duration type. If a nurse is on training, the person may be in need of a special role. However, this role may only be needed for some limited amount of time.

```
(4 hours, enable NurseInTraining)
```

These are just two scenarios where such constraints would seem appropriate. Another example would be if a doctor's neighbour is admitted to a hospital at this doctor's department. If the doctor is indeed not the one responsible for the wellbeing of the neighbour, this special relation should prohibit the doctor from looking at the patient's medical record [27].

```
((patient X, doctor Y), enable neighbourConstraint)
```

2.1.6 Decision Based Access Control (DBAC)

An alternative approach to access distribution, is that necessary and relevant information should be available only to those who are contributing and taking active part in a patient's treatment. In a report funded by The Research Council of Norway [1] it is pointed out that an EHR system's access mechanisms should be organized by this scheme instead of the traditional organizational hierarchy. While other access implementations such as RBAC grant access to a groups of people by ward, DBAC ensures that access to relevant parts of the patient's medical record is given for treatment purposes regardless of which department the health care worker belongs to.

The Norwegian Centre for Informatics in Health and Social Care have published a standard [28] to be used when implementing this kind of access control in health care systems in Norway. The general principles are collected from the laws concerning the handling of health care records belonging to patients in Norway.

The requirements for any system implementing the standard are listed in table 2.1 as they appear in the standard [28].

Until now the granularity which the legal framework describes has been difficult to follow. The practical approach has been to grant access to entire wards or organizational units in which the patient currently resides. Due to the protection of personal privacy, it is not acceptable that any medical record is available to every clinician at all times. To solve this, the

Number	Description	Support
K7.1	The system supporting EHRs must ensure that access to any given record is restricted in such way that only authorized personnel can get to it. The ones who are authorized to view the information are pledged to professional secrecy which is stated in the legal framework dealing with health care personnel [40].	Mandatory
K7.2	The ones providing the treatment must be given the opportunity to register assessments in the patients record [40].	Mandatory
K7.3	Health care personnel who provide medical services are entitled to all of the information contained in the medical record to be able to give proper treatment, unless the patient resists [40].	Mandatory
K7.4	The patient or a representative has the right to see the contents of his own medical record [39]. This means giving direct access to the EHR.	Recommended
K7.5	Access to medical information contained in the EHR may also be handed over in cases of patient administration and quality assurance of the care the patient is receiving [40].	Mandatory
K7.6	Access to information contained in the EHR is only to be made available when it is necessary in order to provide care. Disclosure is only to be given in accordance with client confidentiality [41].	Mandatory
K7.7	Access to the contents of medical records shall only be granted when an impartial explicit purpose exists [41].	Mandatory

Table 2.1: DBAC - requirements supporting the legal framework [28]

standard states that access to medical information and records is only to be made available when a determined measure is carried out. Compliance with this requirement would satisfy `K7.7` in table 2.1.

Efficient use of DBAC in EHRs requires a set of standardized decision templates. The templates are dynamic in the sense that they can be edited, deleted or new ones added. For smaller institutions, fewer general measures templates will probably have to be defined than at a larger hospital.

Table 2.2 shows the minimum number of templates required by the standard [28].

Included in the standard is also a mechanism to ensure necessary access in emergency situations. The use of this mechanism is restricted to be available only to those who are entitled to initiate measures.

2.1.7 Action Control Lists (ACL)

The most common method of implementing access control in a computer systems is through access control lists [26]. All system resources, such as files and printers have a list of authorized users attached. The motivation for introducing access control lists is to enforce privilege

Number	Description	Support
K7.32	1. Measure registration 2. Medical treatment 3. Patient administration 4. A patient's inspection of own record 5. Information to patient 6. Editing of information 7. Deletion of information 8. Editing of medical record 9. Inspection of the medical personnel's activity	Mandatory

Table 2.2: DBAC - minimum requirements to decision templates

separation. In the system, access is granted to objects based on the identity of the user. To illustrate how this access scheme works an example is shown using NTFS[1] developed by Microsoft. This file system uses access control lists to enforce security.

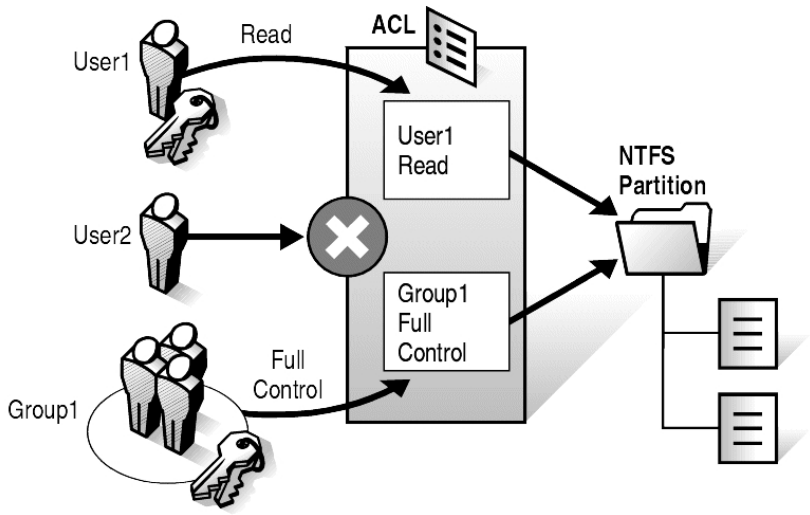

Figure 2.7: Access Control Lists exemplified by the NTFS file system [35]

Figure 2.7 shows that `User1` is able to read the selected files on the partition. `User2` does not appear in the ACL, and is therefore denied access to the resource, while the entities in `Group1` have full control over the selected resource.

This mechanism makes it easy for each and every object to check whether or not the user in question is allowed to manipulate or view its contents.

It is however much more time consuming to check what objects a specific user of the system can access. This requires scanning all objects available on the system, and record all their access control lists. Taking into account that a system may hold millions of files, this may take days [26]. Adding permissions in a system that uses access control lists are therefore quick and easy, but revoking selected privileges held by a user may be hard.

[1]New Technology File System

2.2 COMMON ACCESS AUTHENTICATION PROTOCOLS

Some knowledge about authentication protocols used in computer systems is needed to understand the underlying components used in the field of computer security. This section gives an introduction to common protocols and their operation.

2.2.1 Kerberos

In the book Network Security Essentials [46] three threats in particular are identified in this context:

- A user may gain access to a particular workstation and pretend to be another user operating from that workstation.
- A user may alter the network address of a workstation so that the requests sent from the altered workstation appear to come from the impersonated workstation.
- A user may eavesdrop on exchanges and use a replay attack to gain entrance to a server or to disrupt operations.

The outcome of each of these scenarios is that an unauthorized user may be able to gain access to resources and data which this user is not authorized to access. After a client and server has used Kerberos to prove their identity, they can encrypt all of their communications to assure privacy and data integrity.

One of Kerberos' key features is the *ticket service* which enables the end users to use other protected services in the network without having to log in every time a new request is made. The bottom line is that end users are able to communicate with other servers and entities within the same realm[2] in a single session. Each server does its own authorization. When a user presents a ticket to a server, the server can be sure of that it is this particular user who sent it - no one else. Precisely what this user is allowed to do is up to the server. Figure 2.8 illustrates how the authentication protocol works.

The client authenticates itself to the *authentication server*, then demonstrates to the *ticket granting service* that it is authorized to receive a ticket for a service, then demonstrates to the *print server* that it has been approved to use the service.

Kerberos is available in may commercial products including Windows 2000 [47], and is often used together with the Lightweight Directory Access Protocol (LDAP) to form a secure directory service.

[2] A realm is the scope of a Kerberos deployment. Specifically, the organization domain for which the Key Distribution Center (KDC) is trusted to authenticate principals [46].

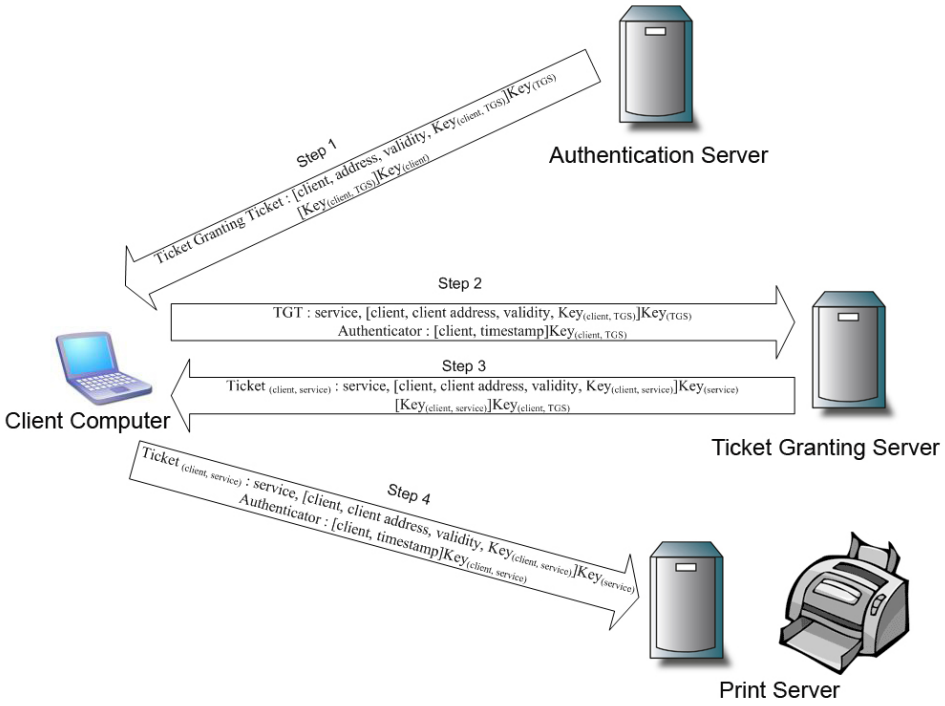

Figure 2.8: Kerberos Operation.

2.2.2 Lightweight Directory Access Protocol (LDAP)

LDAP[30] is an open network protocol for querying and modifying directory services[3]. LDAP was made as a lightweight alternative to the X.500 directory service, making it simpler and easier to adapt to meet custom needs. Unlike X.500, it also supports TCP/IP which is the most used protocols on the internet.

LDAP has many of the same features as a common database, but unlike an SQL-database, which can process thousands of changes per minute, an LDAP directory is optimized for read performance, and therefore most used to store data which do not change too often. As an example, it would work great as a telephone and address directory, but would be unsuited as a database to store a high number of patient records changing many times a day.

2.2.3 Microsoft Active Directory

Microsoft Active Directory is an implementation of LDAP which is described in section 2.2.2. Active Directory was previewed in 1996, released first with Windows 2000, and saw some revision to extend functionality and improve administration in Windows Server 2003 [21]. Active Directory provides services for use in Windows environments. As in LDAP, Active

[3]A directory service is a software application, or a set of applications, that stores and organizes information about a computer network's users and shares, and that allows network administrators to manage users' access to the shares.

Directory allows administrators to assign enterprise wide policies, deploy programs to many computers as well as applying updates to an entire organization [21].

An Active Directory stores information and settings relating to an organization in a central accessible database. Active Directory networks can vary from a small installation with a few objects, to installations holding thousands of objects.

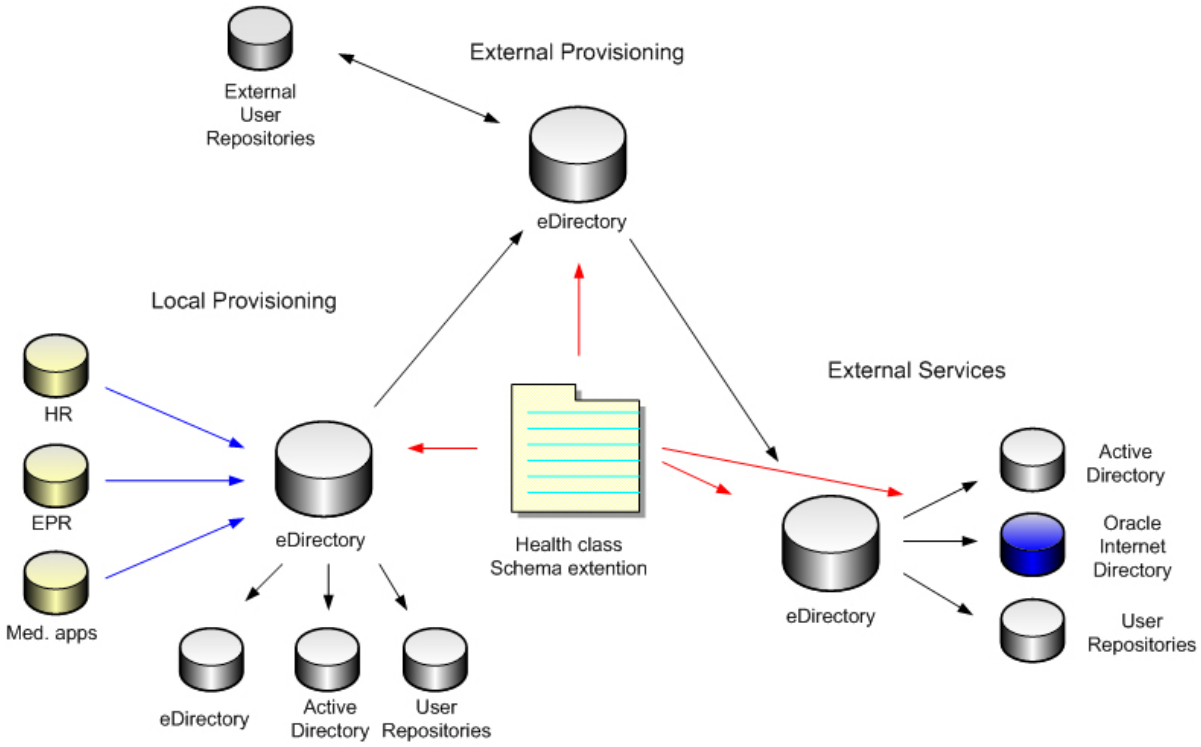

Figure 2.9: The use of Microsoft Active Directory in Klinisk Portal [19]

Figure 2.9 illustrates the use of Microsoft Active Directory in Klinisk Portal 5.2.1 at Rikshospitalet. Klinisk portal is described in more detail in section 5.2.1.

2.2.4 Novell eDirectory

Novell eDirectory is Novells directory server implementation. It supports the X.500 standard [10] and is also one of the directory servers used in Klinisk portal [19]. eDirectory has been in production since 1993, and has become a trusted back-end in many critical services. This server is known for it's compatibility and runs on a lot of plattforms, such as Windows, AIX, HP-UX, Linux, NetWare and Solaris, making it well suited for deployment in a heterogeneous network environment.

eDirectory is a hierarchical and object oriented database that represents all the assets in an organization in a logical tree. Assets can include people, positions, servers, workstations, applications, printers, services, groups to mention some. The use of dynamic rights inheritance and equivalence allows both global and fine grained access controls to be implemented. eDirectory supports partitioning at any point in the tree and replication of that partition to any

number of servers. Referential integrity, multi-master replication and the modular authentication architecture are other advantages to Novell eDirectory [10].

CHAPTER 3
ACCESS CONTROL IN HEALTH CARE SYSTEMS

Some of the key points regarding access control in health care systems are discussed in this chapter. Some of the areas of interest may be summed up by the following questions:

- How should access to information in EHRs be given when it is not clear in advance precisely what information is needed?
- When is it needed to distribute the health information, and when is it possible only to grant access for a period of time?
- How should the technical solutions be designed so that both availability and confidentiality are maintained?

3.1 ELECTRONIC HEALTH RECORD (EHR)

The patient record in its original form is a work tool which is used by health care personnel to perform all forms of health care services [28]. The record contains details about a patient's condition, the assessments made and the treatment related measures taken.

The patient record is also an important medium of communication between clinicians. This is both related to the everyday treatment and care different medical personnel provide in a particular case, as well as serving the purpose when information is transferred to be used at a later time if the need for subsequent treatments arises.

Another intention in addition to the former described primary use, is that they may be accessed by patients in order to get knowledge about own medical state and the treatment they are receiving [41].

The content of a medical record is also used in notifications which health care institutions are obligated by law to pass to social security services and health registries [28].

An EHR is en electronic form of the regular paper based patient record. The specifications are given in a standard [28] published by Norwegian Centre for Informatics in Health and Social Care which forms the base for a nation wide transition to the use of EHRs in medical care. The standard lists a vast number of criteria regarding the use and implementation of this type of medical record and is covered in table 2.1.

The contents of such a record is stored in such a way that it may be retrieved and edited with the appropriate software. An EHR must be able to store at least the same kind of information objects as would be possible in a paper based record. In addition to this, there should also

be possible to attach information which is is normally not enclosed in paper based records such as X-ray images, audio recordings and video recordings. The information objects may be of a variety of different formats, amongst objects designed to be used with other clinical or administrative systems in supplement to word processing programs and image manipulation programs to mention a few. This measure is taken to ensure a flexible standard which will not be outdated due to some change in a third party standard or format.

The paramount goal is to design an access control model which follows the legal framework fully without having the need to sacrifice usability and performance [28].

What kind of information enclosed in a patient's record another person is permitted to view is very situation dependent. Except for the patient himself, no access should be granted to anybody not taking active part in the treatment regardless of position, function or employment. Access to someone's medical record should solely depend on the work related to a patient's medical treatment.

3.2 Finding the Right Access Model To Fit the Domain

Today there are a variety of access models which are more or less suited to fit the needs of the different organizations in which they are implemented. One of the great challenges in systems which are deployed in organizations with complex structure, is the ability to tune the access mechanisms to fit the organization's need, not the other way around.

Currently there are systems in use in the health sector which are partially or fully role based[2]. It can be pointed out that this scheme does not fit the current patterns of which a patient moves around in the health care systems [6]. A patient in the modern health care system may move around frequently between different wards. A form of dynamic access control system would therefore seem appropriate to fulfil the requirements of this work flow. The idea of this kind of system is that the personnel responsible for the patient's treatment is given access regardless of where the patient has been transferred to or from.

3.3 The Balance Between Availability and Confidentiality

There are some typical conflicts between patient privacy and patient safety. This is pointed out in an article written by a group from SINTEF [34] which concentrates on two scenarios on this subject. The first one describes the scenario where a new employee needs access to the system to be able to perform his duties, while the other scenario describes an employee who misuses his access to retrieve information about patients just for curiosity or any other non legitimate reason.

Assigning access rights in hospitals is in nature a difficult task due to the complexity of the organizations. Clinicians may have duties in other wards than the one the organizational chart says they belong to. When access is granted on the ward level, the clinician is able to access information about patients residing on this specific ward, but no other. This improves patient privacy, but lowers patient safety because it decreases the availability of information.

In cases of emergency availability should outdo confidentiality. There is however room for debate on this question, which has been pointed out in the report from The Research Council of Norway [1]. There are however occasions when a clinician may need to override confidentiality restrictions both in the interests of the patient and to be able to save lives. Such occasions might include emergencies where the patient is incapacitated and unable to communicate. In these particular cases, it is important that the usage of an override is recorded and possibly an electronic notification is sent automatically to all parties involved in the patients clinical governance [33].

3.4 Acquiring Access to Blocked Records

Enhanced access rights can be granted in electronic patient record systems such as the DocuLive system presented in section 5.2.2 by the use of an *emergency access* mechanism and a feature called *actualization*. By using these features, the user is granted a higher level of access than during normal operation. These kinds of events are logged in more detail than other events [2] to prohibit misuse and enable more fine grained backtracking of the information retrieved. There are several problems related to this improvised method of obtaining access. In most cases the kinds of requests to use this feature are perfectly legit and serve a well documented reason. However, this feature was originally meant as a last resort rather than an everyday mechanism by which to handle access control. This makes it difficult to handle the amount log data these events produces in the system, and the task of auditing them as thoroughly as wanted [34] would take a lot of resources.

3.4.1 Emergency Access

When a patient is treated in cases of emergency, information is needed to be able to give proper treatment. Emergency incidents are always unplanned, and in cases where lives are at stake, the patient is not always able to explicitly express the authorization which is needed by a doctor to read the patient's record. Without the proper background information, the doctor may not be able give the right treatment at the given time. This override mechanism is therefore meant as a precaution and is supposed to serve the patient's best interest. Access to elements which the person acquiring the access normally have no business looking at is therefore granted [6].

3.4.2 Actualization

The actualization feature is used in situations where a patient is located at a different ward than the person in need of access is. This feature enables the health care worker to view the patient's EHR, usually for one week at the time [6]. There are some occurrences where data is entered into EHR by nurses or secretaries, not by the clinicians themselves. If this person has the ability to perform an actualization in the system, the feature is used to perform read or write operations. The actualization feature is therefore frequently used regardless of the ward the patient belongs to [6].

3.5 Automatic Detection of Access Violations

The health care sector is a domain which traditionally is complicated when it comes to access control. Therefore, it is very difficult to meet the standard of high rate of detections with a low rate of false alarms when using regular access control mechanisms. A health care system should not prohibit health care personnel to save lives due to some security restriction enforced by the system. A system should therefore support some kind of emergency mechanism if an accident occurs that gives the one who is giving treatment access to relevant information about the patient who is being treated.

To be of practical use, a system for detecting access violations should report a substantial percentage of violations while keeping the false alarm rate at an acceptable level [46]. If the access control mechanisms are designed in such way that irregularities happens at large rates, it can be difficult to detect actual misuse. However, if only a modest percentage of actual violations are detected, the system will provide a false sense of security. On the other hand, if the system frequently triggers an alert when no violation has occurred, the people responsible for auditing the logs will either begin to ignore the them, or waste a considerable amount of time analyzing alarms triggered by perfectly legit actions.

To some extent, detecting misuse of health care systems is similar to the problem of detecting access violations and intruders on any other software system. The main difference in health care systems is that there *should* be possible to expand your own access levels to some extent in case of emergency. In the context of computer security in general, intrusion detection is based on the assumption that the behavior of the intruder differs from that of a legitimate user in ways that can be quantified [46]. Of course, it cannot be expected that there will be a crisp, exact distinction between the actions of a legit user, and the ones that of someone who are misusing the system.

Figure 3.1 illustrates that although the behavior of someone who is misusing the system may differ from the typical behavior of a legit user, there will often be an overlap in these patterns of behavior. The adjustment of the level of interpretation on this gray area has major implications on how well this mechanism is working.

3.6 The Legal Framework

The requirements dictated by the legal framework regarding access to medical information can be divided into two groups as we see it.

- **General principles which will hold in most cases**. The fundamental client confidentiality and the use of the patient's approval is described by the legal framework and forms the basis for access control according to the legislation.
- **Exceptions**. When the patient or others with the right to do so have instructed special conditions to what is to be disclosed and to whom disclosure may be granted. There are also emergency situations and other acute situations where the requirement for patient approval for information handling may be derogated.

According to the Norwegian law which dictates how to handle medical records, only personnel responsible for handling patient records are allowed access to information disclosed in

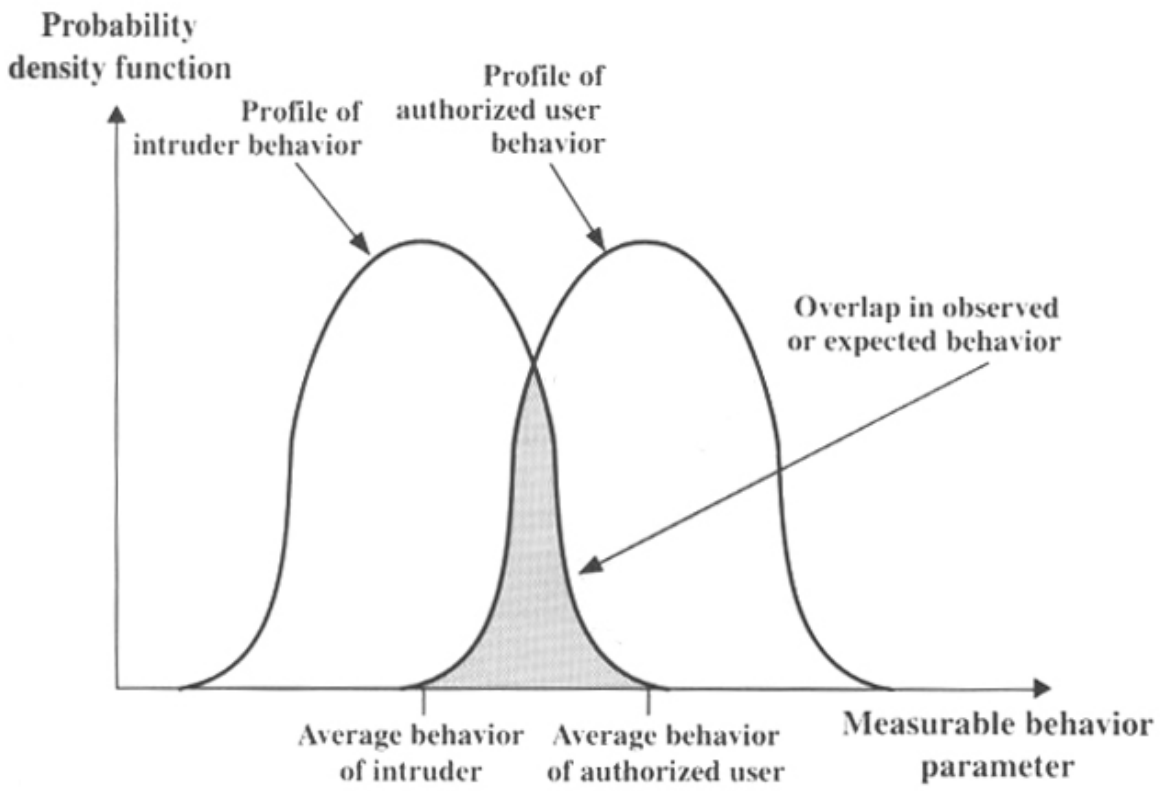

Figure 3.1: Profiles of behaviour of legit and non-legit users [46]

the records [41]. The Directorate for Health and Social Affairs in Norway is working to establish a committee which task is to evaluate if an alteration of the legal framework is needed to support the way information is distributed in modern health care systems. Under any circumstances it is of interest to illuminate to what extent patient information may be given the current legal framework which exist today. The report funded by The Research Council of Norway [1] points out that there is convenient to blame the legal framework whenever difficulties around access control emerges. An interesting thing worth noticing, is however that even though the current revision of the legal framework regarding the health care sector was published in the year 2000, electronic forms of communication is completely omitted in this publication [1].

3.7 DISTRIBUTION OF HEALTH CARE INFORMATION

Today there are standards for some selected areas like references and epicrisis. There exists some standard ways to exchange health care information between EHR systems[4], but they are not much used in Norwegian systems, and manual ways such as fax machines are frequently used to transfer information from one hospital to another [1]. The main challenge is to be able to hand out requested information across hospitals so that relevant information can be accessed regardless of who is needing it to be able to treat a patient.

Aksnes [1] gives an outline of what is required by a service like this.

- It must be possible to deliver a complete copy of the relevant information.
- The original information must not be subject to change or be made inaccessible as a result of the distribution.
- There must be kept track of the information which has been handed out, to whom it has been delivered and when the delivery was made.
- The receiver must log what is received, when it was received and by whom the delivery was made.
- All transactions of personal information which are done outside a defined secure domain must be encrypted to prohibit non authorized access.
- The sender must be absolutely sure that the receiver in fact is the one he claims to be. This can be done by various forms of authentication.

Chapter 4
The RBAC Model Versus the DBAC Model

This chapter describes some of the key differences between the traditional RBAC scheme and the DBAC model. How we believe these models differs in cost, security and the user and administrator experience will be covered in order to examine the positive and negative effects of changing from RBAC to DBAC.

4.1 Motivation For Introducing the DBAC Model

It is the medical treatment and decisions related to a patient which should build the foundation for which medical personnel should be able to view the medical details of the patient. The goal to achieve for access control in health care would be to aim towards a system where the ones responsible for any given patient's treatment would be granted access regardless of which department they belong to. This would require EHR systems to offer functionality to accommodate this.

The most important reason to implement DBAC where RBAC exists today, is to get an access control model that is more dynamic. The users should have the access they need to perform their job at all times, but not more access than needed. With RBAC, practice has shown that it is very hard to make dynamic access rules when properties such as time and tasks of an employee's work change [6]. Patients are often transferred between wards and doctors, and access to the patient journals belonging to the patient are often left behind. This creates a problem, and when access is needed, it is enforced by overriding current access rights by using features such as the emergency access described in section 3.4.1 or the actualization mechanism described in 3.4.2. This creates a security risk, and to maintain some sort of control, there has to be a great deal of auditing of the logs to find security breaches. The more people use the override mechanisms, the more auditing has to be done to find possible abuse. When emergency access and actualization gets used enough in everyday work, a very low percentage will in fact be abuse, and massive resources will have to be put in to reveal the hopefully few cases that occur. If the percentage of discovered abuse is neglectable, the practical use of having access control will be of less importance.

To users who don't have the ability to use acquire extra access and in systems that don't have such features, the transition from RBAC to DBAC will give users a more detailed access control scheme. They will have all the access they need and access to everything else becomes much more restricted. This will eliminate the cases where users lend out their credentials to other users. This is both time consuming to the users and creates a big security challenge because the integrity of the identities in the system will be impaired.

If DBAC was to be adopted in full scale, there would be little or no use for the actualization feature [1]. Even though a patient has left the ward, treatment which has yet to be documented must be entered into the patient's record. This is done by the personnel responsible for this particular patient and as long as there exists a measure related to this patient which is not completed, access to the medical record will still be granted.

4.2 Impact on Users

The ideal way for a access control mechanism to work is to allow users to get all the information they need, and deny everything else. The user should notice the access control as little as possible when they do their job as normal, and if any sort of abuse is attempted, it should be denied and the attempt should be reported. So as long as users behave as they are supposed to, a DBAC is superior to RBAC from a users point of view, since they will get access to all the patients they are treating, regardless of the ward they are admitted to or other parameters that limit a users access beyond their needs. By introducing multilevel access in the EHRs as will be introduced in section 5.2.5, access to read from or write to certain parts of a record can be done by a secretary or nurse on a doctor's order without the need to acquire extra permissions. Roaming specialists such as physiotherapists and nutritionists will also be granted access to perform their assignments without having to spend time enforcing access to the EHRs of the patients they are treating.

4.3 Impact on Administrators

Administration of a system using DBAC will have advantages when it comes to administration. Since rights management pretty much takes care of itself during normal operations after initial settings are configured, less time and effort will be used to change and check users rights. Other tasks related to management of users will probably emerge, and the possibility that other parts of the organization will be given a higher work load after a transition is made is considered likely [6].

Less use of the enhanced access mechanisms results in smaller logs, which again results in less time used on auditing the logs to find abuse. The complexity of a DBAC system can however lead to some negative effects, such as less uptime and more time spent on an initial configuration.

4.4 Impact on Cost

A DBAC system is more complex than an RBAC system and requires all EHRs to be integrated in one system to work flawlessly. This gives a higher development cost than the traditional role based approach. A more complex system will also include more bugs which again will result in a greater need for system updates.

The cost advantages of a deployed DBAC system compared to an RBAC system will be visible in administration related costs. Since the administrators no longer need to spend as much time auditing logs and changing users access rights, the administration costs will decreased in this area.

4.5 IMPACT ON SECURITY

Although DBAC requires more complexity which gives room to more bugs, the transition from RBAC to DBAC would in theory be a great security improvement and comply better with the current health care legislation in Norway.

A transition from RBAC to DBAC will give the users less rights in the system in general, and the less access a user has, the less access he has to information that compromises security as stated in section 2.1.1. Less use of the emergency access and actualization features will make the logs smaller and more comprehensible. This in turn will provide a greater chance to uncover cases of abuse. When a user has all the information he needs to do his work, there will be no need for some users to borrow credentials or accounts from others, which again can be used to get unauthorized information at a later time.

4.6 REALIZATION OF A DBAC SYSTEM

This section will describe a possible solution to how a database designed for basic RBAC can be modified and extended in order to coalesce a DBAC scheme.

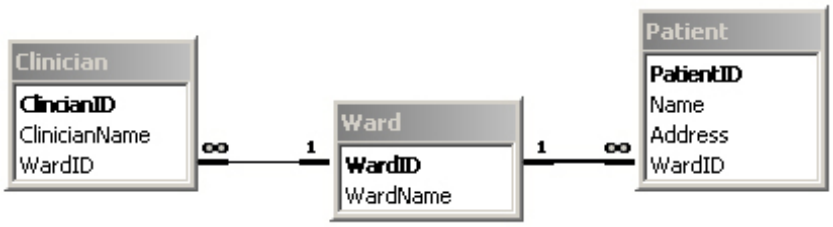

Figure 4.1: ER diagram showing an RBAC database implementation

Figure 4.1 gives an outline of what the basic entities in a database used to enforce RBAC policies may be. As the figure illustrates, the relationship between a patient and a clinician is manifested in the relationship tied to a specific ward. For the simplicity of the example and to be able to emphasize the differences in the implementations, the schematics suggests that all clinicians belonging to a specific ward have access to all patients residing in this ward. Administration of this policy is fairly low due to the restricted expressibility this model offers, but it generates much overhead to the clinicians using the system. The scheme reflects the actual work process poorly, and the use of enhanced access is therefore often needed in order to do routine tasks.

A database layout of an access control system that coincide with the actual work processes in a hospital is sketched out in figure 4.2. The schema quickly becomes a bit more complex compared to the one implementing the basic role based approach in figure 4.1, but it recognizes the fact that a clinician often carry out duties on patients residing in wards other than the one the clinician belongs to.

The schema also gives room for clinicians working shifts. The basic idea of this database layout is to follow the thoughts behind the standard defining EHRs [28] in Norway. This states that any treatment a patient receives during hospitalization should be part of a concrete measure. The layout of figure 4.2 reflects the relationship between a patient and a doctor's decision to carry out a specific measure. The different kinds of measures are held by the

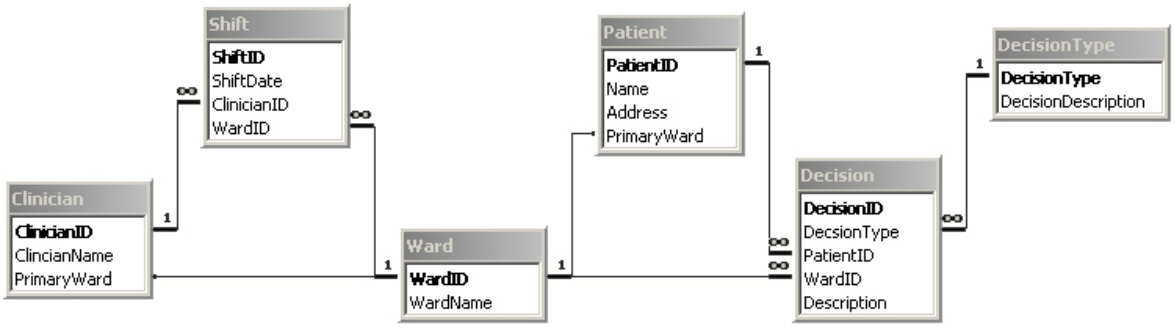

Figure 4.2: ER diagram showing a DBAC database implementation

`DecisionType` table. If a a cardiac examination is needed, the clinician who performs the examination needs to put results into the patient's medical record. To edit the record as described in the requirement specification in table 2.2, access is granted to this clinician because of the decision that has been made to perform this specific task. As opposed to the basic RBAC scheme shown in figure 4.1, the relationship is no longer the between the patient and the ward in which he is currently staying, but rather between the patient and any clinician located at a ward being able to perform the required measure. In a sense, the course of events related to the treatment gets more service oriented rather that person oriented.

The loose coupling between a patient and a clinician belonging to a specific ward, the schema in figure 4.2 also enables shift workers working on other wards than their primary to complete tasks dispatched to the ward in which they are currently working their shift. The amount of time used to obtain access to the incoming patient's records is therefore reduced, and the need to obtain access by using emergency mechanisms is dramatically decreased.

CHAPTER 5
CURRENT MODELS AND IMPLEMENTATIONS

The amount of prior work done in the field of integration of access control mechanisms in health care information systems is quite sparse. There are few publications on the subject [32][18][24][29] and the ones published are either in depth technical and describe one small subset of problems and how an implementation is made to solve this problem, while the other portion contain guidelines or ideas on how integration could be made possible.

Relevant publications are often dated sometimes in the late nineties, and their correlation to ongoing approaches to integration may therefore be of less relevance.

5.1 MODELS

Models made to improve access control in the health sector are presented in short here. As far as we know, they have not been implemented or tested in hospitals. And as mentioned earlier, some of the publications are a bit outdated.

5.1.1 A Role Based Delegation Framework for Healthcare Information Systems

The Role Based Delegation Framework for Healthcare Information Systems [32] was proposed by Longhua Zhang et al. to address the issue of how to advocate selective information sharing in role based systems while minimizing the risks of unauthorized access and to provide a fully integrated EHR. One of the biggest problems addressed is how to enable selective information sharing without the risk of exposing additional information that needs to be protected. To solve this, they introduce a systematic approach to specify delegation and revocation policies using a set of rules.

The role based delegation framework was first developed to provide means of decentralizing user assignment in large distributed role based systems. The framework includes a delegation model and a rule based language for specifying and enforcing delegation and revocation policies.

This paper points out a number of issues where adequate solutions are still to be seen, but to implement the delegation model to be used in a system to solve the current mismatch between the legislation and the current practice would seem difficult. Our opinion is that the issues related to the granularity of the access distribution to the users not will be solved under this framework.

5.1.2 Role Based Authorization in Decentralized Health Care Environments

In the paper Role Based Authorization in Decentralized Health Care Environments[18], Gail-Joon Ahn and Badrinath Mohan has made an overview of how DCOM[1] and RBAC can be used in health care environments to simplify access control and provide administrative convenience to decentralized environments.

DCOM is used within a local network, but they believe that their approach can be extended to be used on the internet as well.

Gail-Joon et. al. describes a well known problem related to authorization in distributed environments and offers a very specific technical solution on a low level. The article describes a solution where administrating users in a decentralized is simplified. Administration of users in a decentralized environment is only part of the problem we are investigating, so we consider the solution this article provides as less relevant in the sense of finding a solution to the access granularity problem.

5.1.3 Combining Access Models

Versatile access control mechanisms are often needed to be able to ensure the security policy of a system. As mentioned in chapter 2 there exists many different access controls models. All of these models have the same paramount goal, namely to ensure the process of automated administration related to the definition and limitation of which systems users can perform which system operations on which system processes. Each organization has a unique set of policies that dictate the circumstances and conditions under which specific users are permitted access to specific resources. The access control mechanisms come in a wide variety of forms, and often each of them has their individual and proprietary attributes, functions and methods for configuring policies. In the pursuit of a standardized access control mechanism, NIST[2][8] has initiated a project referred to as the *Policy Machine*. The *Policy Machine* is able to enforce generalized arbitrary and organizational specific attribute based access control policies through changes only in its configuration. Included among the machine's enforceable policies are combinations of policy instances such as RBAC and MLS[3]. In its protection of objects under one or more policy instances, users and objects with their respective attributes are categorized into policy classes and transparently enforced through a series of fixed functions that are invoked in response to the user's access requests [24].

The need to address specific and ad hoc requirements within an organization's security policy is often needed. There may be a need to consult multiple policies in order to ensure correct access. For example, in order to gain access to a blocked medical record, it may be required to enforce an MLS policy to prevent direct and indirect compromise of classified data. There may also be needed to enforce an RBAC policy to ensure that the users are qualified in addition to an Identity based Access Control policy to protect patient privacy [24].

[1] Distributed Component Model
[2] National Institute of Standards and Technology
[3] Multi Level Security

The policy machine which is introduced by Ferraiolo et al.[24] is not an extension of any other access control model, but instead an attempt to specify the policy machine in terms of access control abstractions, functions and properties basic to access control in general. This includes the ability to generically represent arbitrary user and object attributes which are associated with subjects. The representation allows the policy to be enforced by the policy machine whenever a subject requests access to an object.

5.2 IMPLEMENTATIONS

This section describes a selection of implementations of systems in the health sector and describe their use and access model. *Klinisk portal* described in section 5.2.1 are in use at Rikshospitalet, while *DocuLive* described in section 5.2.2 is one of the systems incorporated into *Klinisk portal*.

The Synapses Project is a project using CORBA to be able to integrate different electronic health care systems using a middle ware approach. The aim of incorporating many heterogenous systems which can be accessed in one place is similar to what *Klinisk portal* does.

Unique SamPro is included in this section because it is an monolithic system which at a later time is supposed to incorporate medical data from external sources of medical information. The use of access control mechanisms which enforces the legal framework when this system extends the amount of information available is highly important.

The section deling with *openEHR* focuses on the solution offered in respect on dividing the EHR into levels in which access is dependent on who is accessing the record.

5.2.1 Klinisk Portal

Klinisk Portal[3] or Clinical Systems All Merged (CSAM) is a portal developed by Rikshospitalet in Norway. It is a portal to six already used systems. Klinisk portal was deployed in October 2004 and has a single sign-on mechanism that logs into and combines data from all the integrated systems. Klinisk Portal is based on roles, but it also has extended functionality to support more dynamic access rights. The user's access rights can be based on a large set of different settings such as work functions, work assignment and responsibilities among many. More systems can be added at a later time to give added functionality or be deployed in another hospital which uses different subsystems.

Systems combined in Klinisk portal:

- DocuLive - System to handle documents in medical records.
- PiMS - Patient's administrative data.
- NetLab - Data from immunology, pharmacology and clinical biochemistry labs.
- Sympathy - Data from the pathology lab.
- Miclis - Data from the microbiology lab.
- RISWeb - Data from the radiology lab.

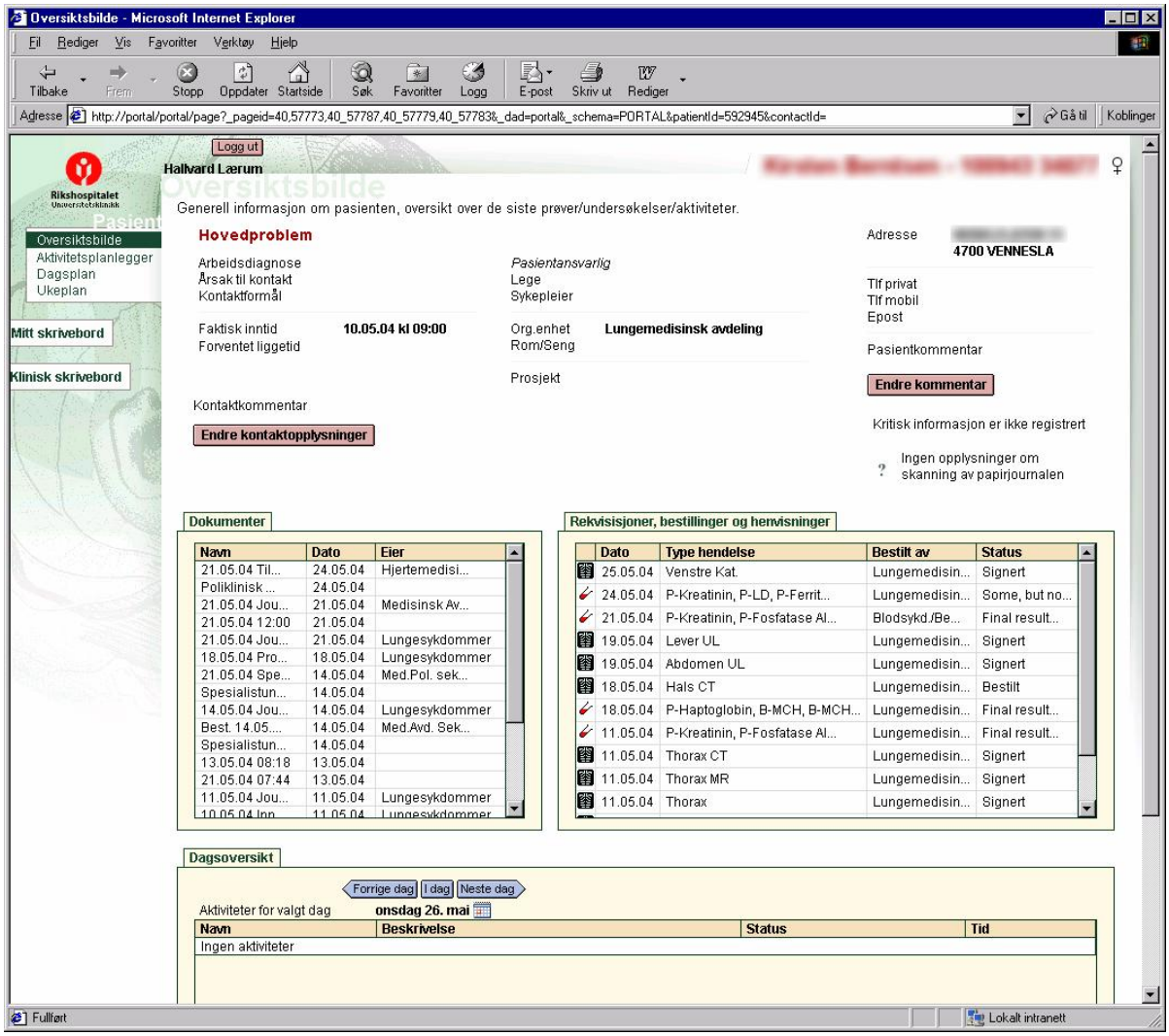

Figure 5.1: A screen shot of Klinisk portal showing a patient record.

Figure 5.1 shows an example of an EHR in Klinisk portal.

5.2.2 DocuLive

DocuLive [2] is an EHR system made by Siemens. It is developed for the Norwegian health care environment. It has over 30 000 users which makes it the most used EHR system in Norway. DocuLive's access model is role based, but it has advanced features so that it can support DBAC if wanted. The system also has possibilities for two way communication with the most common patient administrative systems and uses standard message formats, such as XML[4] and EDIFACT[5], to be able to communicate with other systems as well. This makes

[4]EXtensible Markup Language - A metalanguage that allows one to design a markup language, used to allow for the easy interchange of documents on the World Wide Web.

[5]Electronic Data Interchange For Administration Commerce and Transport - An ISO standard for electronic data interchange that was proposed to supersede both X12 and TRADACOMS as the worldwide standard.

it usable in new systems where a DBAC is implemented. Figure 5.2 shows an example of

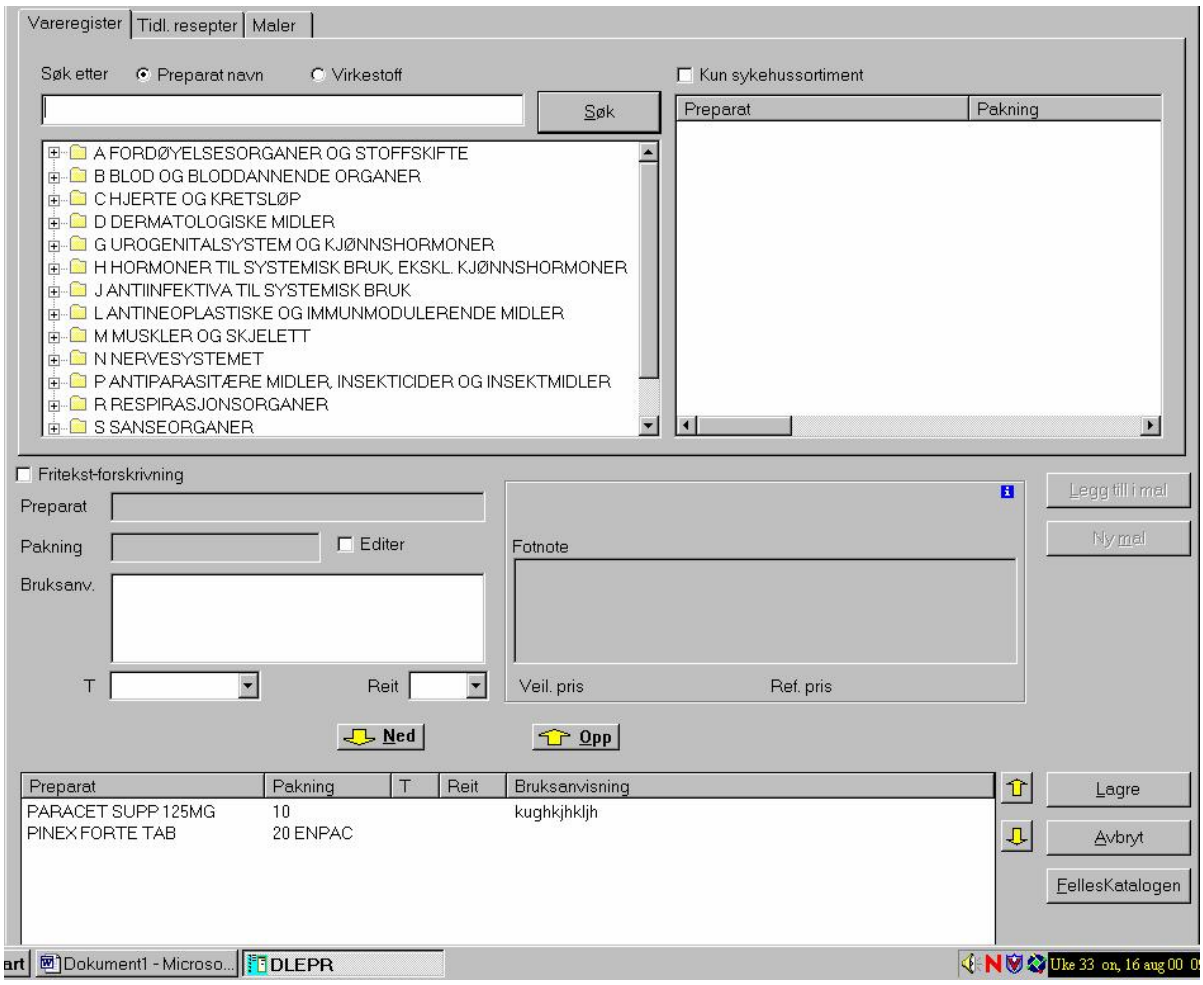

Figure 5.2: A screen shot of DocuLive showing prescriptions [2]

prescriptions in DocuLive.

5.2.3 Synapses - an integration of systems using CORBA

To provide a truly open system in which it is possible to select best-of-breed applications and be able to use this to exchange data with other systems in a meaningful way, Grimson et al. [29] suggest that a CORBA[6][11]-based integration would help solve this problem. Their project is called *Synapses*. By using a middleware approach, the basis for sharing electronic records between heterogenous health care information systems would be possible to achieve. With a collection of independent, autonomous database systems each with their own set of global users which form an alliance, global users are able to access data across the participating systems in a transparent manner. This is called a *federated* database system and the aim of this particular implementation was to develop an open and generic solution for sharing health care records and medical data in a secure and consistent way. A federated health care

[6]Common Object Request Broker Architecture

record is supposed to work in an analogue manner. It is defined as an "*integrated, communicable, combinable and comprehensible health care record that is based on a object model*" [29].

The communication between the different heterogenous systems is encrypted and a uniform encryption policy is used by all components. End users are only required to identify themselves once in a single sign on manner. Once a user has signed on to the Synapse server, their identity is passed on to the respective feeder systems when data is requested. Authorization is done by the different feeder systems as they are the owner of the data requested.

5.2.4 Unique SamPro

Unique SamPro [15] is a project which aims to develop an architecture and pilot software which supports cooperation related to *Individual Plan*[7]. It is a collaboration between SINTEF [14], Helse Midt-Norge [5] and Visma Unique [16]. The project has developed solutions which enable access control and secure communication between different institutions such as medical offices, health care institutions, unemployment offices and social services. Future versions of SamPro is also supposed to incorporate health care data from external sources other than the databases used in the implementation today [6].

An architectural overview of the SamPro system is shown in figure 5.4 and a screen shot is shown in figure 5.3.

The SamPro system uses RBAC and enables people working at different institutions to access only the parts of the record which is of relevance to them.

The authentication process which enables SamPro access will require some form of one time validation code or mobile PKI[8] solutions in addition to user name and password.

The application offers a web interface to the user, and the sensitive information submitted from health care databases is protected by SSL public key cryptography.

5.2.5 *open*EHR

*open*EHR is the outcome of an EU research project called *Good European Health Record*, later changed to *Good Electronic Health Record* with strong participation from Australia. Currently it is maintained by a non-profit organization called *openEHR Foundation*. The foundation is an online community whose "*aim is to promote and facilitate progress towards EHRs of high quality, to support the needs of patients and clinicians everywhere*" [12].

The most noteworthy concept introduced by *open*EHR is the archetype concept. This approach uses a two level methodology to model the EHR structure [23]. In the first level, a generic reference model that is specific to the health care domain but still very general is developed. The model contains only a few classes and they must be stable over time. The classes will typically

[7]The norwegian government requires that all patients in need of long term and coordinated health services are entitled to an individual plan. Patients emitted into psychiatric health care may also require an individual plan [39, 38].

[8]Public Key Infrastructure

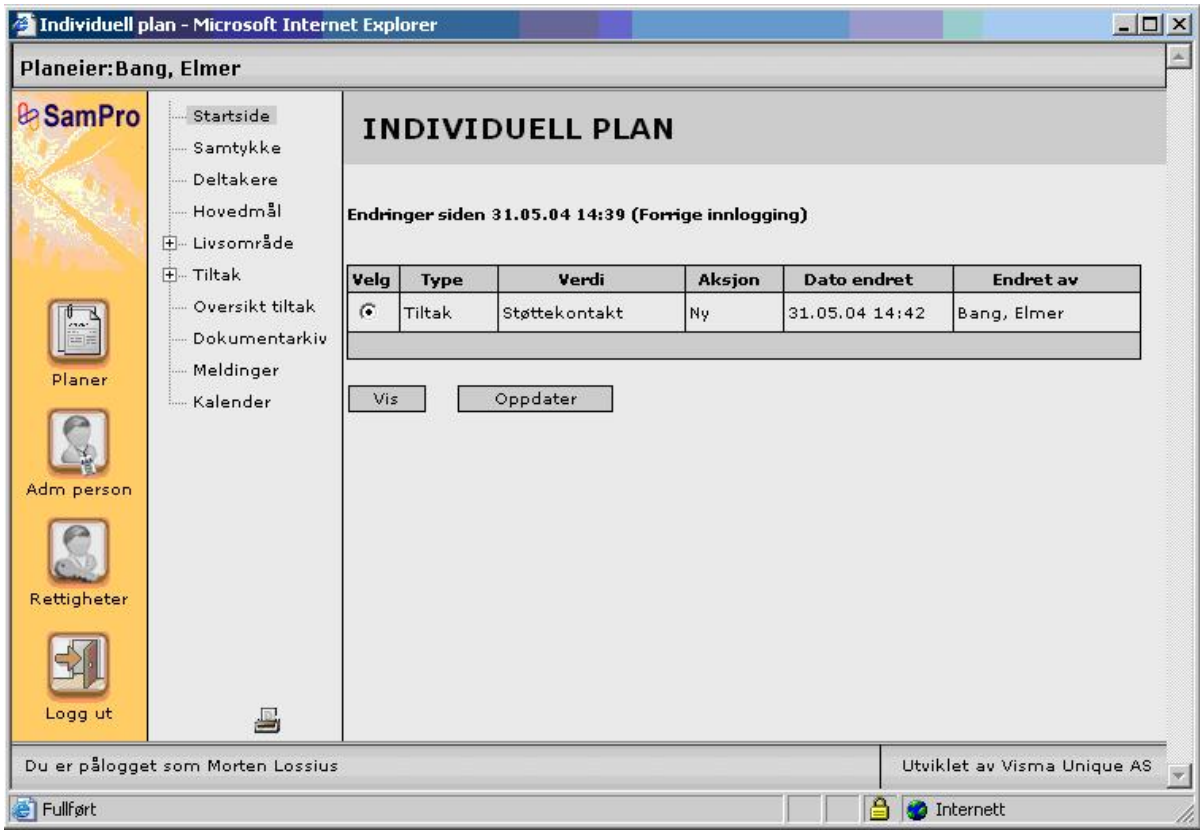

Figure 5.3: A screen shot of SamPro showing measures taken in the Individual plan [6]

be *role*, *act*, *entitiy* and *participation*. The second level contains health care and application specific concepts such as blood pressure and other lab results modeled as archetypes. This means that constraint rules that specialize the generic data structures can be implemented using the reference model [23]. As an example a constraint may restrict a specific class only to be able to view and edit the blood pressure archetype.

The archetype approach requires three building blocks. Figure 5.5 shows these blocks. An editor for creating and maintaining archetypes, a validator that enforces the constraints at runtime and a browser component that allows for an optimized display of specific archetypes must be offered by the EHR system.

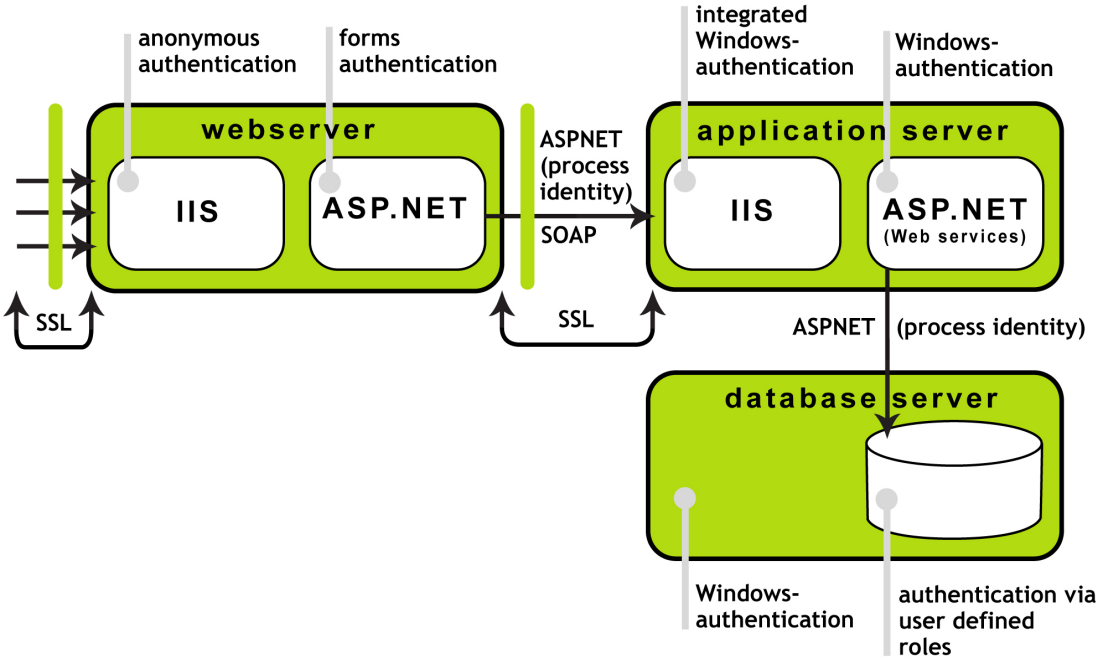

Figure 5.4: An overview of Sampro's architecture [16].

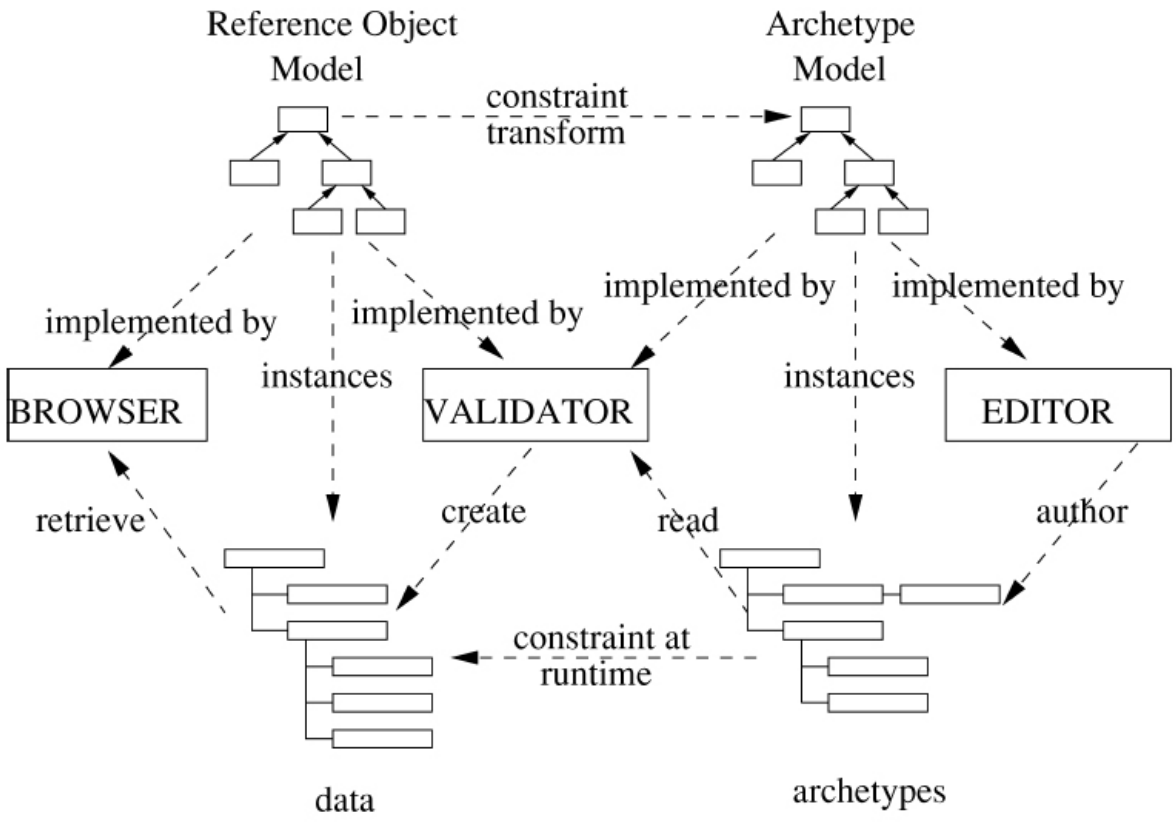

Figure 5.5: openEHR archetype methodology [23]

Part II

Methodology

CHAPTER 6
DEFINING AREAS TO EVALUATE

The first step in order to compare the two access schemes is to determine the area of interest. There are several interesting factors that may be investigated and compared. We have identified three paramount areas which can be used to evaluate different access schemes.

- Time consumed by employees with different work tasks when using the system.
- Cost related to implementation, deployment and maintenance.
- Security enforcements which influences availability and the ability to detect exceptions and prohibit exploits.

The areas listed are described in the following sections.

6.1 TIME SPENT BY EMPLOYEES PERFORMING DIFFERENT TASKS WHEN USING THE SYSTEM

When talking about time as an area of evaluation, we are interested in the amount of time different parts of the staff use when dealing with access issues in their everyday work. These are again divided in three, the time spent by health care workers, the time spent by administrators on maintenance and the time spent by administrators on log auditing. We believe a great deal of time can be saved in this area by changing the access scheme.

6.1.1 Time Spent by Health Care Workers on EHRs

One interesting thing to observe, is how different access schemes affects health care workers everyday ability to carry out their jobs in an efficient manner. A change from RBAC to DBAC will most likely influence the time spent by health care workers to access, modify and create patient records.

6.1.2 Time Spent by Administrators on System Maintenance

Another important factor is the time, thus the cost involved to keep an up-to-date system. The need to quantify the work done by system administrators when new user accounts are added

and prepared is of importance, and the time spent by administrators to change user privileges is also of importance when such actions are appropriate.

6.1.3 Time Consumed to Study Logs in Order to Reveal Abuse

To be able to enforce the legal framework, there must exist a consistent source of information which reflects the usage of resources on the system. This type of information is gathered in log files and can be examined in order to reveal abuse or professional misconduct of medical information. Depending on the events entered in the logs and how extensive each entry is, a considerable amount of time may be needed if the logs are to be reviewed manually and the amount of logged data is large.

6.2 Cost Related to Implementation, Deployment and Maintenance

The cost related to implementation, deployment and maintenance is huge in complex computer systems. When changing a computer system as big as the entire EHR system and the belonging components, it is going to cost a great amount of both money, time and extra effort from the users. If these costs are large compared to the savings in the other areas, it may not be economically justifiable to replace the existing systems until a replacement is needed for other reasons than economical profits.

6.2.1 Implementation Cost

Different access mechanisms may have different implementation costs due to their differences in scope and complexity. A DBAC scheme will probably require a more complex integration of components in the system than a RBAC scheme will, due to the greater demands in knowledge of the users working habits and the patients' transfers. This makes a DBAC scheme more expensive to implement.

6.2.2 Deployment Cost

Deploying a whole new access control system is not something that is done over night in large organizations. The staff is most likely going to be in need of training, and it may take some time for the benefits of making the changes are visible. The deployment of a new system often requires new servers, workstations, terminals and other expensive hardware. New procedures may also be required, and to users who are used to an old and familiar system, a new system tends to cause frustrations and requires a closer followup on the users.

6.2.3 Maintenance Cost

The cost related to system maintenance after implementation is also something that must be considered carefully. The long term cost of having made a cheap implementation which is expensive and time consuming to maintain may result in an overly expensive solution in the end. However a complex system may also require more maintenance since it requires more hardware and consist of more code, hence more bugs that need fixing down the line adding to maintenance costs.

6.3 SECURITY

Security is one of the most important reasons to change to DBAC. Since security is very hard to measure in time and cost, an own area on security has to be included in order to cover the gains and losses in this area. Security gets more necessary to include in systems as the systems are expected to become available in different locations. When the system gets available on publicly available networks, a higher grade of security is required, also with respect to authorized users' access levels.

6.3.1 The Ability to Enforce the Security Policy

There is only a subset of the clinicians working at a hospital who should have access to a given patient's medical record. The health care sector is required by law to enforce a strict policy regarding this matter [41]. If one security mechanism is better suited to enforce this policy than the other, this is important to investigate and emphasize.

6.3.2 System Usability

Depending on how strict the security mechanisms in a system are and how it is implemented, users may find the system bothersome to use. If the security enforced is too strict, users may find it convenient to borrow the credentials of colleagues in order to to their job without having to fiddle with authorization issues.

6.3.3 The Ability to Uncover Security Exceptions

The ability to uncover breaches in the security policy is of great importance. The DBAC model allows for more efficient auditing of log material, since it reduces the need to acquire extra access. This is one of the places where this access scheme really excel compared to the role based access model used in Norwegian hospitals today.

6.4 Choosing the Area to Be Evaluated

The areas which are identified in the introduction to this chapter may all be used to compare and evaluate different access mechanisms. We have chosen to focus on the area which covers the time consumption described in section 6.1. The reason for making this choice is that we believe that this would illustrate some important differences between the two access control mechanisms. By pointing out some key consequences of the time spent by the different parts of the staff in relation to the different access mechanisms, some aspects of both cost and security are also covered. For instance, if an access mechanism makes a clinician be less efficient and use more time to fiddle with access control, fewer patients get treated, and the cost per patient overall rises.

If a clinician have to use work hours to figure out how to access material and medical records in order to give treatment to patients, the access scheme probably poorly reflects the work flow of everyday work or it may be poorly implemented. This will also be reflected in the time spent by a clinician in order to do his work. Again there is a balance between effectiveness of the users and security protecting the system.

System administrator's time use will also reflect the access control model enforced by the system to some extent. If the access model is well suited and tuned for it's purpose, the task to audit logs of exceptions in security will be a less time consuming one. The ability to uncover abuse is also proven easier and thereby less time intensive to sort out under some access mechanisms than other.

Choosing time as a basis for evaluation may therefore give tangible results which could say something about both cost, effectiveness, and the efforts used to maintain the system.

CHAPTER 7
IDENTIFYING EVALUATION PARAMETERS

This chapter contains a description of the parameters evaluated in order to get results on the systems in hospitals today in the areas we are interested in. There is also a list and descriptions of the formulas used to get results and a brief summary of why they are included and what information they produce.

7.1 PARAMETERS OF WHICH TO PERFORM AN EVALUATION

In order to compare the areas described in chapter 6, a set of key parameters is defined. This section describes some possible parameters to map hospitals, and why they may be interesting. A wider range of parameters than the collection finally presented by which to do the evaluation is also presented here. The parameters we find most interesting are picked out in section 7.2.

7.1.1 Number of Patients

This parameter is chosen to be able to see how hospitals are affected when more patients are admitted. In order to find out how much access fumbling there is per patient, the number of accesses enhancements performed per patient and how they are affected by the size of the hospital, this parameter needs to be considered. The number of patients is therefore needed in able to calculate other adjacent parameters relevant to the study.

7.1.2 Number of Clinicians

What is the number of users a change of access control mechanism will affect? If a vast number of clinicians use large amounts of time on unnecessary access issues, their job become more frustrating and time is being spent on solving problems which does not benefit anyone. This parameter is needed to get information about how each clinician is affected by access enhancements, how many patients a clinician accesses, and how much time each spend on unnecessary work in order to access EHRs.

7.1.3 Total Number of EHR Queries

In order to know how many queries each patient record and each clinician has in average, the total number of EHR queries is needed. To know the percentage of queries made using enforced access, the total number of EHR queries is needed.

If the number of enforced accesses increase linear when the number of total queries increase is an interesting thing to investigate. Quantifying the time spent accessing each EHR in average, average time spent by each clinician to access EHRs and how total time is spent on EHRs are all interesting numbers to establish.

7.1.4 Number of Accesses to Blocked Records

To measure the number of accesses to blocked records is important because a overly frequent use of this mechanism will undermine the legal framework which intends to protect the privacy of the patients. The more often this mechanism is used in legit everyday work, the more difficult it is to reveal abuse by auditing logs. The number of accesses to blocked records is also were we predict to see the biggest differences between RBAC and DBAC, since the need to access blocked records in a DBAC scheme will occur rarely. By reducing the number of accesses to blocked records, the possibilities to check logs and find abuse using this feature increases. Since the feature in theory always provide the correct access needed to perform the required measure, auditing logs to keep the privacy of the patients intact is feasible because enforced accesses to blocked record content are reduced.

7.1.5 Number of Wards

Counting the number of wards in a hospital is an easy way to find out how the hospital is organized, and thereby give an assumption on how many patients and clinicians there are in each ward in average. The number of wards is also easy to find, so it should be possible to find the number of wards in a hospital and include it in the survey.

7.1.6 Log Complexity

The more complex logs are, the more time consuming the task to audit them will be. If legit mechanisms frequently used by clinicians in their everyday work also may be used to acquire information they are not supposed to get, the task to discover this in endless logs containing legit actions is difficult. Depending on the amount of data and the type of logs created, extensive work may be needed in order to make sense of them and be able to retrace the course of events if this is needed.

As figure 7.1 suggests, much time and effort can be saved by reducing the complexity of logs. The ability to do this is closely related to how tuned the access scheme is to the domain in which it is deployed. The time needed to audit logs will be considerable if the system is large

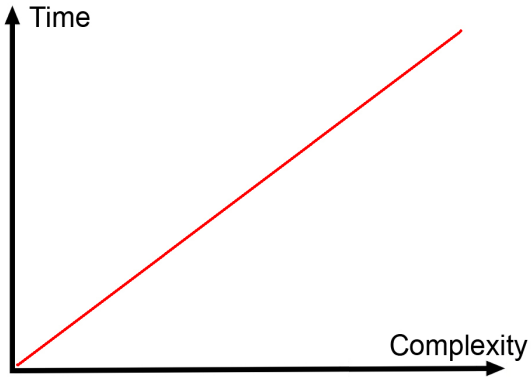

Figure 7.1: Time used to audit logs as a function of their complexity.

enough. As figure 7.1 indicates, a linear growth is assumed. Depending on the type of logs this function may well be exponential, but the assumption of linear growth is made in this assignment.

7.1.7 Time Spent to Check One Acquiring of Access to a Blocked Patient Record

To be able to give an estimate of how much time is needed to do complete log audit, some data on the time spent on checking a single entry in a log. Since each acquiring of access to blocked records creates an entry, it would be informative to know how much time is needed to check all log entries, or if it's even feasible to do a complete log audit. By getting this information it can also be calculated how much time can be saved on auditing by reducing the number of emergency accesses use when implementing a DBAC mechanism.

7.1.8 Time Spent Obtaining Access to Blocked Patient Information

The time it takes for a health worker to obtain access to information about a patient in cases where access already should be granted represents a total waste of time. Figure 7.2 illustrates the linear growth connected to the increase of time used when a clinician have to use to get the access they need to do everyday routine work.

Figure 7.3 illustrates the time used to access patient records under a DBAC system. Acquiring access to blocked records will in most cases be unnecessary.

If the clinician has any business viewing or editing a medical record, access is already granted by the person by whom the patient was referred. Therefore, as figure 7.3 illustrates, a minimal amount of time is needed by the clinician to perform queries on the current medical record.

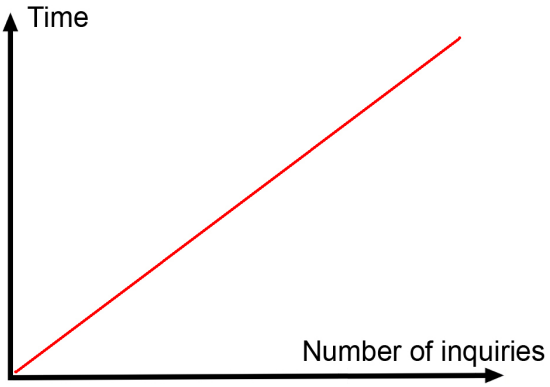

Figure 7.2: Time used to access patients records by the use of the access enhancement.

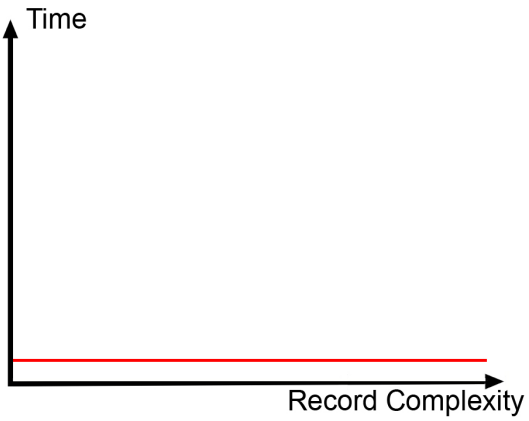

Figure 7.3: Time used to access patients records under a DBAC system.

7.1.9 Time Used to Access a Patient's EHR

The time it takes to access and read a user's record may be interesting to compare to the time spent reading and modifying records. This can be used to see how much time is spent on access fiddling instead of patient treatment. There is probably spent unnecessary time accessing, reading and writing patient records, and there should be room for improvements by making access easier and more intuitive.

7.2 Choosing the Parameters Needed to Make a Comparison

To compare a decision based acces control system with a role based access control system, we have to select the parameters needed to find the information we are looking for. In this case, the parameters should be of such nature that it is possible to extract comparable data about time spent by health care workers and system administrators in their every day work when using the different access schemes. To be able to compare the traditional RBAC mechanism to

the DBAC mechanism, it is important that the key parameters can be used to illustrate some important differences between the two. We will also benefit from some basic knowledge [6] about how a hospital is organized and data on how many clinicians are needed to serve a set of patients.

Number of patients, clinicians and wards are numbers that are easy to measure and give us insight in how big a hospital is, how many clinicians are organized in one ward, and how many patients can be handled by a set of clinicians.

The number of access acquirings to blocked records and an estimate of the average extra time spent when doing this compared to regular access is useful information. An estimate on how much extra time is spent getting the right amount access in order to get the information needed can then be made. Time spent to audit a single log entry is needed to be known in order to find out how much time is spent on checking logs. An indication on whether it is even feasible to check through the logs for abusive behavior can also be established.

The number of log lines produced in one log entry and time used to access a patients record are parameters we have decided not to include. These are numbers that will not change if the access control model change, and we can get the calculations we want without these parameters.

Table 7.1 contains the list of parameters which will be used in the calculations.

Number of patients	$\mathtt{P}$
Number of clinicians	$\mathtt{C}$
Total number of patient record queries	$\mathtt{Q}$
Number of accesses to blocked records performed	$\mathtt{B}$
Number of wards	$\mathtt{W}$
Time spent to check one acquiring of access to a blocked patient record	$\mathtt{T}_L$
Time spent on obtaining access to blocked patient information	$\mathtt{T}_B$

Table 7.1: Parameters which will be used in the calculations.

7.3 CALCULATING DIFFERENCES BASED ON THE PARAMETERS

To be able to extract useful estimates by using the parameters, relations between them are needed to form a foundation for the results. Table 7.2 describes the relations of primary interest. The one-letter abbreviations listed in the right hand column are the parameters found in table 7.1.

Average queries per patient	$\frac{Q}{P}$
Average acquirings of blocked patient records per clinician	$\frac{B}{C}$
Acquiring of blocked patient records per query	$\frac{B}{Q}$
Total time used on acquiring access to blocked records	$B \times T_B$
Time needed to read the total amount of log entries of blocked record acquirings	$T_L \times B$
Average number of access acquirings to blocked information per ward	$\frac{B}{W}$

Table 7.2: Defining relations using the parameters

The relations in table 7.2 are described in the following sections.

7.3.1 Average Queries Per Patient

Average queries per patient is needed in order to track how much time and money is spent per patient. We can also get an idea about how costs per patient develop when hospitals change size by examining these numbers on hospitals which differ in size.

7.3.2 Average Acquirings of Blocked EHRs Per Clinician

The time and cost spent on acquiring access to blocked patient records is a total waste of both time and money, so the acquiring of access to blocked records per clinician shows how much more effective they could become by removing this obstacle. How the use of access acquirings escalate when the number of clinicians increase can also be seen from this function.

7.3.3 Acquiring of Blocked EHRs Per Query

This expression estimates how many percent of all accesses are enforced accesses. This can again give a number on how much more efficient a patient's treatment can become by eliminating the frequent use of this feature.

7.3.4 Total Time Used on Acquiring Access to Blocked Records

The total time used on acquiring access to blocked information shows all the time that is wasted getting information one should have access to in the first place. This can be converted into how much money can be saved by using a more flexible system where such a feature is not used in everyday work.

7.3.5 Time Needed to Read the Total Amount of Log Entries of Blocked Record Acquirings

The total time needed to to do a complete check of the log files gives an indication of how much it costs to check the logs for all access violations or if it is even possible to do a complete audit. A check on time and cost to find a given percentage of the abuse can also be calculated from this function, if we say that checking a given percent of the logs will expose the same percent of abuse.

7.3.6 Average Number of Access Acquirings to Blocked Information Per Ward

The cost per ward related to the use of actualizations and emergency accesses can shown by using this parameter. If the relation of acquirings of blocked records grows more the more wards are added, this would be an important relation to establish. If this were to be established as an exponentially growing function, the result would be that a in large hospital the amount log entries would explode, adding to an already massive amount of entries unfeasible to audit.

CHAPTER 8
SIMULATION

A common methodology used for comparing access control models is simulation [49]. In this chapter there are two different scenarios shown in two different hospitals that differs in size and have different kinds of patient masses. The hospitals are partly fictional, but some of the numbers are based on information from the two Norwegian hospitals Rikshospitalet and Ullevål sykehus. The first scenario is purely fictional, while the complex one is based on a real event gathered from the iAccess [6] project. Within the two scenarios we show how the systems differ when the access control mechanism change. These numbers are not real, but they will give a good indication of how things change. Afterwards we indicate a percentage of how often each scenario occurs in each of the two hospitals.

8.1 SCENARIO 1 – SIMPLE PATIENT TREATMENT

The first described scenario is a quite simple one. A man comes to the hospitals casualty clinic with a cut in his arm. First he gets admitted by a secretary. After a few minutes a general practitioner looks at the patient, washes the wound, bandages him and refers the patient to a surgeon. After a while a surgeon takes a look at the patient, stitches his wound together and dismisses him.

Table 8.1 shows the course of events in a role based and a decision based system when scenario 1 happens. The first column shows the actions performed, the second one shows what operations are performed with RBAC, and the third column shows the operations when using DBAC. The W parameter counts the number of write operations performed, the R parameter counts the number of read operations and the B parameter shows the acquiring of blocked patient information. In the summary, the C parameter shows how many clinicians were involved and the Wa parameter shows the number of wards involved. The Q parameter shows number of total queries in the system.

8.2 SCENARIO 2 – COMPLEX PATIENT TREATMENT

The second scenario is a real event and is much more complex than the first one. A patient goes to the casualty clinic with blood in his feces. He first meets a secretary who admits him to the hospital. He then meets a general practitioner who gives a tentative diagnosis of possible causes. These are infection in the intestines, tumor or hemorrhoids. The patient is then transferred to the surgical ward. A doctor here orders a blood sample, an endoscopic

Action	RBAC	DBAC
Secretary creates a new admission.	1 W	1 W
General practitioner looks up the patient's record. General practitioner refers the patient to a surgeon.	1 R 1 W	1 R 1 W
Surgeon looks up the patient's record. Surgeon writes down his treatment and closes the case.	1 R 1 W	1 R 1 W
Summary:	3 C 2 R 3 W 0 B 1 Wa 8 Q	3 C 2 R 3 W 0 B 1 Wa 8 Q

Table 8.1: Course of events in Scenario 1

examination, a CT-scan, an MR-scan, ultrasound, and X-rays. When the results return, he concludes hemorrhoids.

However some secondary findings are discovered. The patient has glucose in his urine and unstable body movement. The doctor orders inspection from the neurology department to check his body movement and from the internal medicinal department to check the glucose. The results show the patient has diabetes and a possible tumor in the head.

The patient is then transferred to the neurology ward to check the tumor. They order a CT-scan, an MR-scan, ultrasound and X-rays of his head. When the results return, a conclusion of a removable tumor is made.

The patient is moved on to the neurosurgical ward and is set to be operated. Medical attention from internal medicine is needed for his newly discovered diabetes, and an anaesthetist is being sent for. The patient is operated with success and transferred to intensive care, where he is looked after until he is no longer in need of supervision. He then moves back to neurosurgical, where they order a physiotherapist, dismisses him and send him to an exercise facility. The exercise facility receives an epicrisis from the hospital but they keep their own record independent from the one used at the hospital.

Figure 8.1 shows the course of events in Scenario 2.

The two tables 8.2 and 8.3 show the course of events in a role based and a decision based system when scenario 2 happens. The first column shows what actions are performed, the second shows the operations performed with RBAC, and the third column shows the operations when using DBAC. The W parameter counts the number of write operations performed, the R parameter counts the number of read operations and the B parameter shows the use of access to blocked records. In the summary, the C parameter shows how many clinicians were involved and the Wa parameter shows the number of wards involved while the Q parameter shows number of total queries in the system.

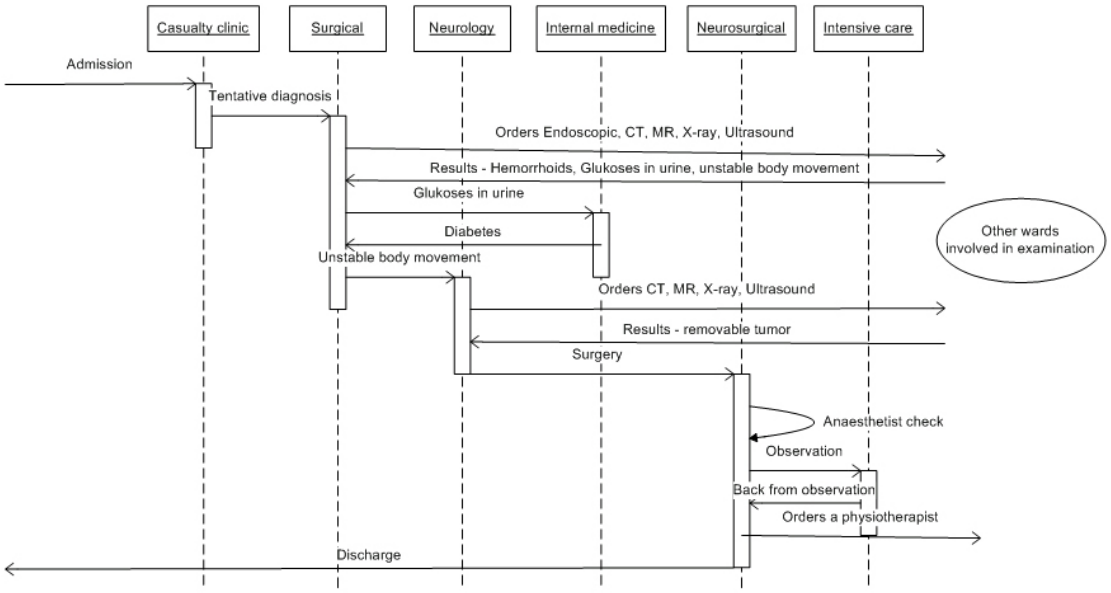

Figure 8.1: Sequence diagram showing the course of events related to Scenario 2.

8.3 SCENARIOS IN HOSPITAL 1

Hospital 1 is a fictional hospital, but it is based on the Norwegian hospital Rikshospitalet. Rikshospitalet has about 4000 employees, 210 000 consultations and hospitalizations during a year, and about 40 wards. In table 8.4 the numbers are mapped to the parameters and presented in a more structured manner. Since Rikshospitalet has mostly planned hospitalization with a more straight forward course of events, we make the assumption that Hospital 1 has a ratio of 70 percent simple scenarios and 30 percent complex scenarios. Since we have no way of exactly knowing the values of the parameters T_L and T_B, we have chosen the value of 1 minute in both. Although this is not exact numbers, we believe they are roughly right and give an estimate even if the numbers prove not to be exactly correct. Acquireing blocked access may involve a process of writing an explanation for why access is needed and this takes some time to complete. In other cases the clinician may need to find someone who is able to give away their credentials in order to get the access needed.

- Total number of Queries:
  $(49queries \times 210000consultations \times 30percent)+$
  $(8queries \times 210000consultations \times 70percent) = 4262000$
- Total number of access acquirings to blocked information using RBAC:
  $(17accessacquirings \times 210000consultations \times 30percent)+$
  $(0 \times 210000consultations \times 70percent) = 1071000$
- Total number of access acquirings to blocked information using DBAC:
  $(0acquirings \times 210000consultations \times 30percent)+$
  $(0 \times 210000consultations \times 70percent) = 0$

Action	RBAC	DBAC
Secretary creates a new admission.	1 W	1 W
General practitioner looks up the patient's record.	1 R	1 R
General practitioner transfer the patient to surgical ward.	1 W	1 W
Surgeon looks up the patient's record.	1 R	1 R
Surgeon tells nurse to order tests	1 B	1 W
Endoscopic examiner requires patient record	1 B	1 R
Endoscopic examiner writes to patient record	1 W	1 W
CT-operator requires patient record	1 B	1 R
CT-operator writes to patient record	1 W	1 W
MR-operator requires patient record	1 B	1 R
MR-operator writes to patient record	1 W	1 W
X-ray-operator requires patient record	1 B	1 R
X-ray-operator writes to patient record	1 W	1 W
Ultrasound-operator requires patient record	1 B	1 R
Ultrasound-operator writes to patient record	1 W	1 W
Nurse retrieves the patient results for surgeon.	1 B	1 R
Surgeon concludes hemorrhoids	1 W	1 W
Surgeon gets a nurse to order inspection from the neurology department	1 B	1 W
and an inspection from internal medicinal	1 B	1 W
Neurologist requires patient record	1 B	1 R
Neurologist writes to patient record	1 B	1 W
Internal medicine doctor requires patient record	1 B	1 R
Internal medicine doctor writes to patient record	1 B	1 W

Table 8.2: Course of events in Scenario 2, part 1

8.4 SCENARIOS IN HOSPITAL 2

Hospital 2 is also fictional, but it is based on the Norwegian hospital Ullevål sykehus. Ullevål sykehus has about 8200 employees, 355 000 consultations and hospitalizations, and about 75 wards. In table 8.6, the numbers are mapped to the parameters. Since Ullevål sykehus handles most of the emergency hospitalizations in the Oslo area, the amount of planned hospitalizations is estimated to be considerably lower than Rikshospitalet. Less straight forward courses of events are therefore probable to occur, so an assumption is made that Hospital 2 has a ratio of 50 percent simple scenarios and 50 percent complex scenarios.

- Total number of Queries:
  $(49queries \times 355000consultations \times 50percent)+$
  $(8queries \times 355000consultations \times 50percent) = 10117500$
- Total number of access acquirings to blocked information using RBAC:
  $(17accessacquirings \times 355000consultations \times 50percent)+$
  $(0accessacquirings \times 355000consultations \times 50percent) = 3017500$
- Total number of access acquirings to blocked information using DBAC:

Nurse gives surgeon the patient's results. Surgeon transfer the patient to neurology ward.	1 B 1 W	1 R 1 W
Neurologist requires patient record Neurologist orders tests	1 R 1 W	1 R 1 W
CT-operator requires patient record CT-operator writes to patient record MR-operator requires patient record MR-operator writes to patient record X-ray-operator requires patient record X-ray-operator writes to patient record Ultrasound-operator requires patient record Ultrasound-operator writes to patient record	1 R 1 W 1 R 1 W 1 R 1 W 1 R 1 W	1 R 1 W 1 R 1 W 1 R 1 W 1 R 1 W
Neurologist requires patient tests Neurologist transfers the patient to the neurosurgeon ward	1 R 1 W	1 R 1 W
Neurosurgeon looks up the patient's record. Internal medicine doctor looks up patient's record Anaesthetist looks up the patient's record Neurosurgeon writes to the patient's record Neurosurgeon transfers patient to intensive care	1 R 1 B 1 B 1 W 1 W	1 R 1 R 1 R 1 W 1 W
Intensive care looks up the patient's record. Intensive care writes to patient's record. Intensive care transfers the patient to neurosurgical.	1 R 1 W 1 W	1 R 1 W 1 W
Neurosurgeon looks up the patient's record. Neurosurgeon discharges the patient. Neurosurgeon orders a physiotherapist. Secretary prints out epicrisis.	1 R 1 W 1 W 1 B	1 R 1 W 1 W 1 R
Summary:	25 C 11 R 21 W 17 B 13 Wa 49 Q	25 C 23 R 26 W 0 B 13 Wa 49 Q

Table 8.3: Course of events in Scenario 2, part 2

$$(0accessacqurings \times 355000consultations \times 50percent) +$$
$$(0accessacqurings \times 355000consultations \times 50percent) = 0$$

Number of patients	P	210 000
Number of clinicians	C	4000
Total number of patient record queries	Q	4 262 000
Number of accesses to blocked records performed	B	1 071 000
Number of wards	W	40
Time spent to check one acquiring of access to a blocked patient record	T_L	1 minute
Time spent on obtaining access to blocked patient information	T_B	1 minute

Table 8.4: Parameters in Hospital 1 using RBAC

Average queries per patient	$\frac{Q}{P}$	20.3
Average acquirings of blocked patient records per clinician	$\frac{B}{C}$	268
Acquiring of blocked patient records per query	$\frac{B}{Q}$	25 percent
Total time used on acquiring access to blocked records	$B \times T_B$	17 850 hours
Time needed to read the total amount of log entries of blocked record acquirings	$T_L \times B$	17 850 hours
Average number of access acquirings to blocked information per ward	$\frac{B}{W}$	26775

Table 8.5: Relations in Hospital 1 using RBAC

8.5 VISUALIZING THE RESULTS

To be able to get a better understanding of some of the numbers we have estimated, graphical representations are presented by figures 8.2 and 8.3.

While figure 8.2 is showing the difference in percentage the number of accesses to blocked record information, figure 8.3 shows the relation between the number of employees and the total time spent accessing blocked records at the hospitals.

Number of patients	P	355 000
Number of clinicians	C	8200
Total number of patient record queries	Q	10 117 500
Number of accesses to blocked records performed	B	3 017 500
Number of wards	W	75
Time spent to check one acquiring of access to a blocked patient record	T_L	1 minute
Time spent on obtaining access to blocked patient information	T_B	1 minute

Table 8.6: Parameters in Hospital 2 using RBAC

Average queries per patient	$\frac{Q}{P}$	28.5
Average acquirings of blocked patient records per clinician	$\frac{B}{C}$	368
Acquiring of blocked patient records per query	$\frac{B}{Q}$	30 percent
Total time used on acquiring access to blocked records	$B \times T_B$	50292 hours
Time needed to read the total amount of log entries of blocked record acquirings	$T_L \times B$	50292 hours
Average number of access acquirings to blocked information per ward	$\frac{B}{W}$	40 233

Table 8.7: Relations in Hospital 2 using RBAC

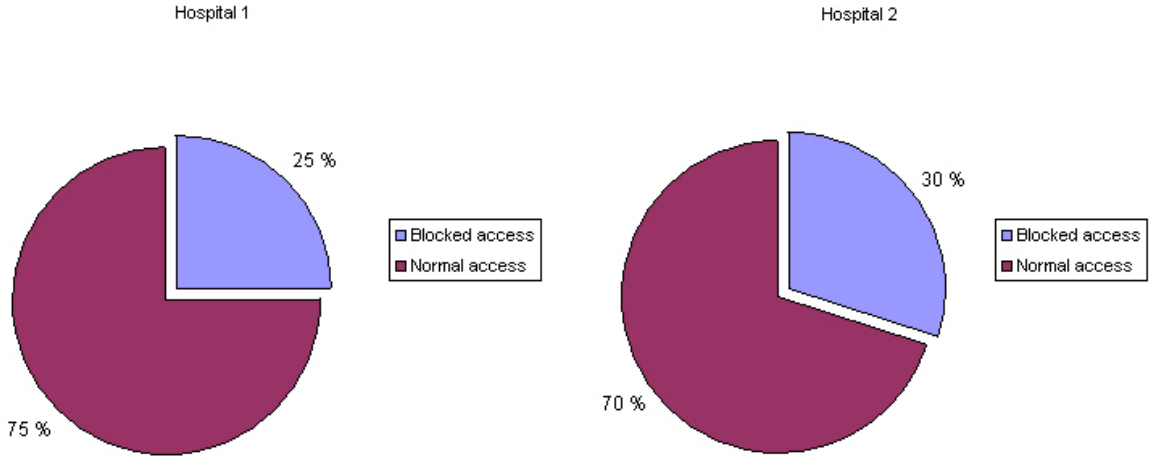

Figure 8.2: Pie chart representing the percentage of blocked accesses in hospitals 1 and 2.

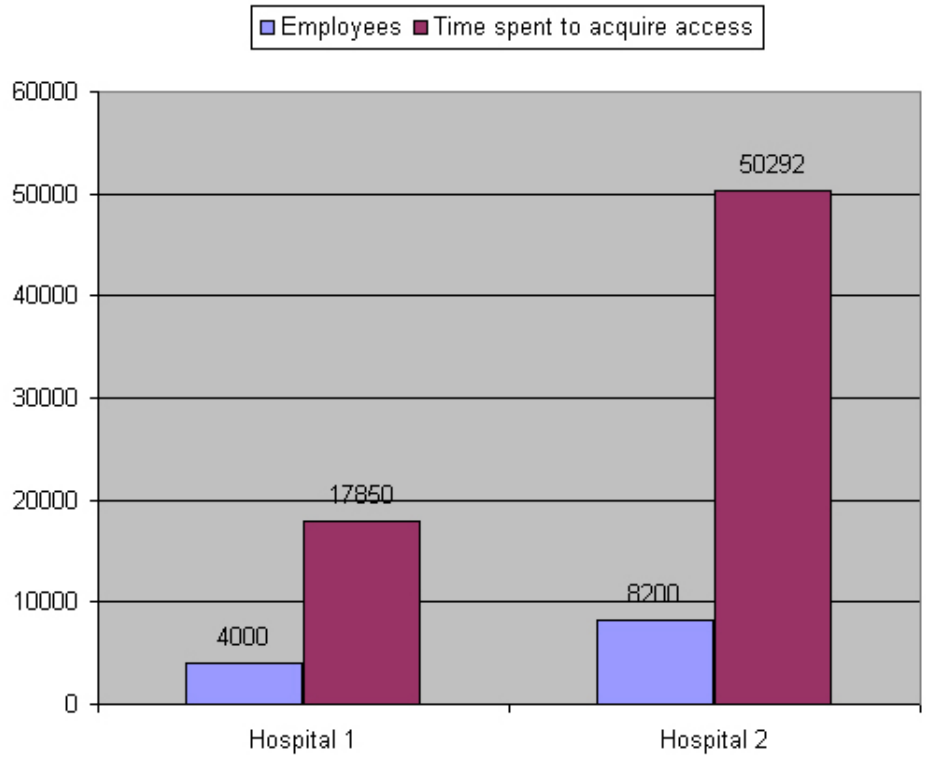

Figure 8.3: Histogram showing the relation between number of employees and time spend accessing blocked records in hospitals 1 and 2.

Part III

Discussion and Conclusion

Chapter 9
Discussion

When the need to secure computers and the information they contained emerged, the mechanism most commonly used was simple password protection. This solution would grant a user access to all or noting, giving little attention to the fact that it might be desirable to grant different users different levels of access. Access control mechanisms have been developed during the years to support the work flow of everyday work as the computers became more and more vital to the infrastructure in the industry.

It soon became clear that in systems holding a large number of users, not all of the information contained in the system where appropriate to share with all of the users. As a result of this, the principle of least privilege concept described in section 2.1.1 emerged. A user should only be able to access the information necessary to carry out their work and nothing more. The problem with the principle of least privilege is how to decide what is enough and what is to much. If one takes an example in a hospital, a nurse needs no access to a system while off duty, and different access is needed based on the assignments at work at any given day. However, having changed shifts with a coworker will require access beyond normal working hours. There may also be complications if a patient is transferred to another ward and the nurse has no access to the patient's medical data at this location. Problems like the described example makes the principle of least privilege a very complex problem, and makes it very hard to decide what is enough and what is too much access.

To be able to enforce the basic idea of the principle of least privilege has been the governing idea through further development of access control mechanisms. One step in differentiating access control levels was introduced by the group based access control scheme discussed in section 2.1.4. However, this model has some limitations, because it's groups are collections of people without the attributes and operations for various types of roles. This scheme evolved further into a role based access control mechanism which gave conformance to the different roles workers in an organization had. Today RBAC is in broad use to support the privilege of least principle. The ability to establish conformance between the organizational chart in a company and the access mechanisms in the system made it easy to adapt and manage on a high level.

Today RBAC is used in the health care domain as well. One of the main issues in the health care sector, is that the work flow in everyday work is complex to model and does not fit very well into the traditional role based access scheme. The result is that health care workers often are denied access to information they need to be able to do their jobs. Override mechanisms are implemented in the systems to be used in emergencies and other rare situations which are not supported by normal operations. However, the denial of legit information needed in everyday work makes these mechanisms frequently used. When these overriding mechanisms are used, more information is presented to the user than necessary as stated in section 1.2.

One of the biggest problems is therefore to enable selective information sharing without the risk of exposing additional information that needs to be protected. To solve this, a systematic approach to specify delegation and revocation policies using a set of rules is proposed in the model described in section 5.1.1.

The pursuit of an access control mechanism which both complies with the work flow in the hospital as well as the legal framework in Norway has started. By implementing a decision based access control scheme, the need to use the override mechanisms to obtain access to blocked information should be dramatically reduced. One of the things that escalates the use of the override mechanisms are the use of nurses and secretaries to register various results and examination data. This is a group that is not closely linked to any single ward in which they provide their services. This is also the case for specialists such as physiotherapists and nutritionists who help patients on many different wards every day. As with a traditional role based access mechanism restricting access to patients by the ward in which the health care worker is employed, a nurse or secretary may need to use the override mechanism every time a result is to be appended to a patient's EHR.

Implementations such as *open*EHR described in section 5.2.5 offers differentiation in the amount of information available as a result of who is making the request to look at the record. By using this approach, a more fine grained access scheme may be deployed. By embracing this way of protecting pieces of the health care records, the privilege of least privilege would be followed more closely. The "too many get to know too much too easily"-problem discussed in section 1.2 would be partially solved due to the restrictions the different entries in the record would have if a solution like this was to be adopted. To be able to implement this kind of differentiated access on this level, thorough process analysis are needed to identify main categories of purposes which health care workers need access to. Certain parts of a patient's record may be available to a larger number of clinicians than others. The process of establishing the different access levels and protected entries in the EHR may be a complicated process as both compliance to the legal framework and the work processes at hospitals must be preserved. However the idea of a multi leveled access hierarchy in health care records is probably a step in the right direction towards better compliance with the legal framework.

The results of the simulation in chapter 8 give an indication of how much time is spent on acquiring the correct amount of access, and how much time is needed to check for access violations. With the use of our numbers in Hospital 2, figure 8.3 shows that over 50 000 work hours are spent a year on acquiring the amount of access needed. This means that about 40 man-labour years can be saved every year by getting rid of the need to acquire enhanced access rights. These numbers will of course vary in different hospitals. Figure 8.3 also tells us that Hospital 1 only spends about 18 000 hours, a little more than a third of what Hospital 2 uses, even though it is half and not a third the size. The explanation is probably connected to the ways these hospitals operate. Since Hospital 2 has a much larger base of unpredicted patient treatments, the patients will also more often be transferred between wards, which creates a larger percentage of access acquirings as illustrated in figure 8.2.

Because hospitals are of different sizes and are operated in different ways, it is hard to give exact numbers representing gain in time and cost or a percentage which applies to all hospitals. In some hospitals, changing access schemes will probably not be favourable because of all the problems related to changing systems does not outweigh the expected outcome. In other hospitals, the advantages of introducing a new system will surpass the problems by far.

The average acquirings of blocked patient records per clinician is 268 in Hospital 1 (Table

8.5) and 368 in Hospital 2 (Table 8.7). These numbers will vary among different clinicians and different wards. Some doctors will almost never use this feature because they usually have the access needed, while some nurses and secretaries have to acquire extra access almost every time they write something into the records. Therefore, some users will say the existing systems work just fine, and other will say they work terrible while most users probably will be somewhere in the middle. The estimates we have produced are important, because they give an indication of how much overhead a user has to deal with when working with the systems. If users always feel that the system works against them, a bad work environment is created.

Our results in chapter 8 also show that in the hospitals we have used to simulate a working environment, the right amount of access is lacking 25 and 30 percent of the time as illustrated in figure 8.2. The need to use the override mechanisms is thereby increased. The idea of these features was originally to use them only in cases of emergency. Instead they are used on a daily basis in almost every third query in Hospital 2. This makes complete auditing of logs almost impossible. Over 50 000 hours and millions of NOK are needed to audit logs in Hospital 2 if one query is checked in one minute. To improve security, the hospitals will have to reduce the use of this feature.

The accuracy of the numbers used in the simulation lack the reliability to establish a quantifiable result. Obtaining the exact numbers for the parameters which form the foundation of the calculations would improve the trustworthiness of the computations. Nevertheless, if the parameters were to be adjusted properly according to the actual numbers, we believe that there would still be a considerable difference between the use of RBAC and DBAC in hospitals in regards of time clinicians spend accessing information and administrators spend auditing system logs.

The issues regarding the introduction of a robust DBAC system in the health care sector is at least a big organizational problem as it is a technical IT problem. There may be as many as hundreds of small heterogenous systems in use on a daily basis at the hospitals nationwide. To alter these systems in order to apply a new access control mechanism is both difficult and time consuming. To get the DBAC scheme to work, a good amount of work is needed in the phase of transition. In addition to health care workers, both IT-personnel and the staff must get a thorough introduction to ensure success in deployment.

There may be some change in the way young clinicians are working apposed to the ones who have not had computers around most of their lives. While the use of computers seem difficult for some, younger individuals tend to have a better understanding of computers in general and may therefore record patient data themselves instead of having someone else without the proper permissions to do so. If these speculations should hold to be true, the role based access control mechanisms seen in systems such as DocuLive described in section 5.2.2 may be adequate to handle access control. The number of access requests to blocked records would at least be reduced in the context of this speculation.

Chapter 10
Conclusion

This report focuses on the differences between role based access control and decision based access control in health care institutions in Norway. One of the most important things revealed by this study is that pretty much all security measures in the systems can be overridden by the use of a feature such as emergency access. This feature is used extensively in everyday work at the hospitals, and thereby creates a security risk. At the same time conformance with the legal framework is not maintained. The results in chapter 8 show that a complete audit of the logs containing access right enhancements is unfeasible at a large hospital, and even checking a few percent of the entries is also a very large job.

Users with too strict access rights without the possibility to enhance their own access also creates a great risk, since they tend to borrow accounts belonging to others in order to do their job. This creates a situation where there is little integrity connected the users identity. The result is that there may be difficult to hold someone responsible for actions carried out in the system, even if their credentials has been used.

There is definitely a need to find ways to make abuse of the systems harder, and a need for better ways to log and audit events. We believe a decision based access mechanism will do a much better job on solving the problems mentioned than the role based approach has done in the past. We can not claim that this is the ideal solution to be used in every hospital, and more testing has to be done in order to give such a conclusion.

Some economical advantages of decision based access control is also pointed out in this report. A lot of time, hence money, is spent by clinicians on acquiring access to blocked records and large resources are needed to be able to reveal violations. Tables 8.5 and 8.7 show that the total amount of time united spent to gain access at large hospitals in Norway is substantial, even though the time used to perform a single query is quite small.

How the hospitals are organized, their size, and how the percentage of complex versus simple patient treatment is distributed will determine how useful a change in access control mechanism may be. The economical savings will of course be weighted against the extra expenses in connection with developing, deploying and maintaining a new system. To find the real economical advantages and disadvantages in hospitals, there has to be internal explorations and surveys in each hospital in question.

To help find the need to change access model, part of our work was concentrated in identifying parameters by which to evaluate access systems. The ones we have identified as the most important ones are listed in table 7.1. These parameters are in turn used to create an outline for a survey which is presented in table 11.1. These results can be used further in order to get more detailed information about the cost of existing systems and uncover the possible need of a new one.

The ultimate goal of a hospital system which gives all users exactly the access they need without sacrificing usability or compliance to the laws may seem to lay sometime into the future, but with focus both from the media and the public, new systems and initiatives are established to try and solve the problems. One thing is building secure systems, another thing is creating systems which health care personnel feel assist them in their everyday work instead of making it more difficult and troublesome.

CHAPTER 11
FUTURE WORK

The purpose of this chapter is to describe how the research done in this report can be used in further research. We have divided this chapter in four sections. The first one explains the survey we have made and how it can be used to gather information from hospitals. The second section tells how the survey can be expanded to reveal better and more detailed results. The third and fourth section explain the need to estimate implementation costs and the need to try a DBAC system in a test environment.

11.1 SURVEY

In order to determine how much time and cost can be saved by changing access model, we have prepared a questionnaire which can be used to collect data about this subject at any hospital.

11.1.1 Recommended Questions

Based on the evaluation parameters purposed in chapter 7, we recommend the use of the questions listed in table 11.1 to obtain the necessary foundation of evaluation.

11.1.2 Distribution of the Questionnaire

To be able to collect the data needed to fill in the parameters identified i section 7 in an efficient manner, it is our recommendation that the questionnaire is being distributed using a web interface. This makes it less time consuming for the ones who are going to answer the questions, as well as it makes the job managing the returning answers less time consuming as well. One of many tools that can be used to do this is *IT's Learning* [7]. Figure 11.1 illustrates how a questionnaire is presented to the end user. Simple check boxes and mutual exclusive answering options help the results be less ambiguous and hopefully easier to interpret.

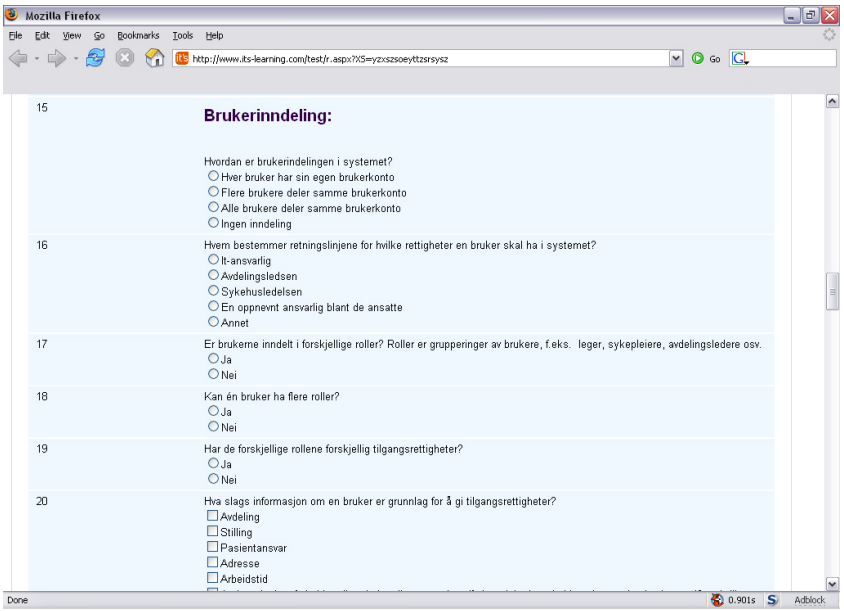

Figure 11.1: Data collection questionnaire

11.1.3 Processing the returning answers

IT's Learning also provides mechanisms to process the returning answers in an well arranged manner. An illustrative sketch of this is shown in figure 11.2.

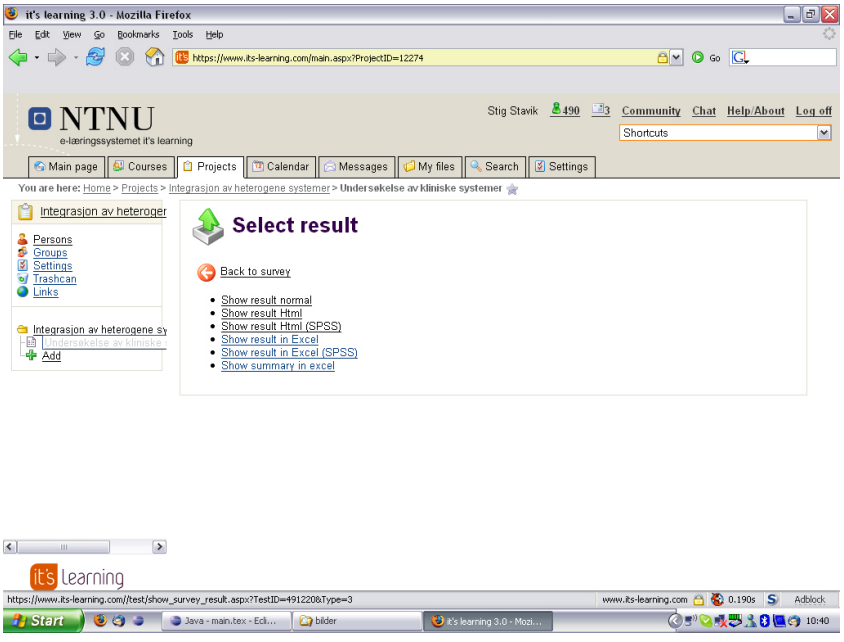

Figure 11.2: Data processing in IT's Learning

An important thing to emphasize is that the tool used to store the returning answers must be secure. If sensitive data is to be collected or a nondisclosure agreement is to be followed, it is important that nobody else is capable of viewing the data. If IT's Learning offers strong enough protection mechanisms must be discussed in the events of a survey taking place. The

lack of confidence in security may prohibit involved parties from participating.

11.2 Expanding the survey to reveal more detailed results

The survey proposed in section 11.1.1 does only cover the initial parameters of interest when an evaluation is to be made. To be able to uncover more fine grained details, a more specific survey has to be performed.

11.3 Get an estimate on implementation cost

To be able to get the full picture related to the cost of introducing a new access control system, the total amount of both time saved and savings of administration cost will have to be compared to the expected outcome with the new system. In addition the implementation cost will have to be taken into consideration as well. A large custom implementation requires both financial resources and manpower from the institution in which it is going to be deployed during the development.

11.4 Try a DBAC system in a test environment

Testing a DBAC system in a simulated environment would prove useful in order to point out things previously overlooked. Doing scenario simulation using real hospital's heterogenous environment is also recommended in order to uncover possible difficulties related to implementation and deployment.

Group	Key points	Parameter mapping
General	• How many patients are admitted during a year • How many clinicians are employed at the hospital • How large is the percentage of planned admittances opposed to emergency admittances? • What is the number of wards handling the EHRs at the hospital?	P,C,W
EHR inquiries	• How many percent of the record accessing is done by health care workers without the right amount of access? • What is the total number of daily EHR accesses in the hospital? • What is the total number of daily accesses to blocked EHR content done by either clinicians, nurses, secretaries or other personnel?	Q, B
Classification of users	• Do the users have their own user accounts on the system? • – Every user has one of their own – Multiple users share the same account – All users share the same account – No classification exists. • Are users divided into roles according to the organizational structure of the hospital? • Do the different roles have different levels of access?	
Overriding access	• Is it possible to access blocked health records and contents by using an override mechanism? • Does everyone handling EHRs have the power to override the blocking mechanism?	
Logging	• How thorough is the auditing process of the logs? • How are events related to access of blocked records logged? • – Together with other events – In a separate log – These events does not differ from other events • What does an entry dealing with access to a blocked record contain? – Subject - which user performed the action – Action - what was edited or looked at? – Object - the record affected by the action – Root cause - the reason the content had to be accessed – Time stamp - when did the event occur?	T_L, T_B

Table 11.1: Collecting data to map the parameters.

Bibliography

[1] Elektronisk tilgang til helseopplysninger - utfordringer og mulig tiltak. HØYKOM-rapport 506, Norges forskningsråd, Sep 2005.

[2] Doculive elektronisk pasientjournal, May 2006. http://www.medical.siemens.com/.

[3] *EPJ ved norske sykehus*. http://www.idi.ntnu.no/emner/tdt4210/2004/2004link/forelesningsfoiler/2004-11-03_NTNU_EMR_systems_in_Norway.ppt, May 2006.

[4] Health level 7, May 2006. http://www.hl7.org.

[5] Helse midt-norge, March 2006. http://www.hemit.no.

[6] The iaccess project, May 2006. http://iaccess.idi.ntnu.no.

[7] It's learning, May 2006. http://www.its-learning.com.

[8] National institute of science and technology, May 2006. http://www.nist.gov.

[9] Nist - role based access control, May 2006. http://csrc.nist.gov/rbac.

[10] Novell edirectory, May 2006. http://www.novell.com/products/edirectory.

[11] Object management group, May 2006. http://www.omg.org.

[12] openEHR, May 2006. http://www.openehr.org.

[13] The research council of norway, May 2006. http://www.forskningsradet.no/.

[14] Sintef, March 2006. http://www.sintef.no.

[15] Unique sampro, March 2006. http://www.sampro.no.

[16] Visma, March 2006. http://www.vismaunique.no.

[17] Martin Abadi, Michael Burrows, Butler Lampson, and Gordon Plotkin. A calculus for access control in distributed systems. *ACM Trans. Program. Lang. Syst.*, 15(4):706–734, 1993.

[18] Gail-Joon Ahn and Badrinath Mohan. Role-based authorization in decentralized health care environments. *ACM*, pages 251–256, 2003.

[19] Leif Egil Buen. Sikkerhetsarkitektur, klinisk portal. Technical report, 2005.

[20] Developed by Subcommittee: E31.20. *E1986-98(2005) Standard Guide for Information Access Privileges to Health Information*. American Society for Testing and Materials, 2005.

[21] Microsoft Corporation. Active directory ldap compliance. Technical report, October 2003.

[22] Information Technology Industri Council. *Role Based Access Control*. American National Standard, 2004.

[23] Marco Eichelberg, Thomas Aden, Jörg Riesmeier, Asuman Dogac, and Gokce B. Laleci. A survey and analysis of electronic healthcare record standards. *ACM Comput. Surv.*, 37(4):277–315, 2005.

[24] David F. Ferraiolo, Serban Gavrila, Vincent Hu, and D. Richard Kuhn. Composing and combining policies under the policy machine. June 2005.

[25] David F. Ferraiolo, Ravi Sandhu, Serban Gavrila, D. Richard Kuhn, and Ramaswamy Chandramouli. Proposed nist standard for role-based access control. *ACM Transactions on Information and System Security*, 4(3):224–274, 2001.

[26] Davik F. Ferraiolo, D.Richard Kuhn, and Ramaswamy Chandramouli. *Role-Based Access Control*. Artech House, first edition, 2003.

[27] Fisher-Hubner, Rannenberg, Yngstrom, and Lindskog. Security and privacy in dynamic environments. *IFIP International Federation for Information Processing*, 201(1):364–376, 2006.

[28] Norwegian Centre for Informatics in Health and Social Care. *EPJ Standard*. 2001.

[29] Jane Grimson, William Grimson, Damon Berry Gaye Stephens, Eoghan Felton, Dipak Kalra, Pieter Toussaint, and Onno W. Weier. A corba-based integration of distributed electronic healthcare records using the synapses approach. *IEEE Transactions on Information Technology in Biomedicine*, 2(3):124–138, 1998.

[30] Network Working Group. Lightweight directory access protocol. Technical report, dec 1997. http://www.ietf.org/rfc/rfc2251.txt.

[31] Thomas A. Limoncelli and Christine Hogan. *The Practice of System and Network Administration*. Addison Wesley, first edition, 2001.

[32] Gail-Joon Ahn Longhua Zhang and Bei-Tseng Chu. A role-based delegation framework for healthcare information systems. *ACM*, pages 125–134, 2002.

[33] J.J. Longstaff, M.A. Lockyer, and M.G. Thick. A model of accontability, confidentiality and override for healthcare and other applications. In *ACM Symposium on Access Control Models and Technologies. Proceedings of the fifth ACM workshop on Role-based access control*, pages 71–76, 2000.

[34] Per Håkon Meland, Lillian Røstad, and Inger Anne Tøndel. How to mediate between health information security and patient safety. In *Proceedings of the Eigh International Conference on Probabilistic Safety Assessment and Management (PSAM 8)*, 2006.

[35] Microsoft. Using access control lists. Technical report, Feb 2006. http://www.microsoft.com/technet/prodtechnol/sppt/sharepoint/reskit/part2/co8spprk.mspx.

[36] Jonathan D. Moffett and Emil Lupu. The uses of role hierarchies in access control. In *ACM Workshop on Role-Based Access Control*, pages 153–160, 1999.

[37] National Institute of Science and Technology. *New Draft RBAC Implementation Standard*, May 2006.

[38] Ministry of Health and Care Services. *Lov om sosiale tjenester m.v. (Sosialtjenesteloven)*. January 1993.

[39] Ministry of Health and Care Services. *Lov om pasientrettigheter (Pasientrettighetsloven)*. Jan 1999.

[40] Ministry of Health and Care Services. *Lov om helsepersonell m.v. (Helsepersonelloven)*. Jan 2001.

[41] Ministry of Health and Care Services. *Lov om helseregistre og behandling av helseopplysninger*. May 2001.

[42] Ravi S. Sandhu, Edward J. Coyne, Hal L. Feinstein, and Charles E. Youman. Role-based access control models. *IEEE Computer*, 29(2):38–47, 1996.

[43] Fred B. Schneider. Enforceable security policies. *ACM Trans. Inf. Syst. Secur.*, 3(1):30–50, 2000.

[44] Morten Solli. For mange får vite for mye for lett, May 2006. http://www.computerworld.no/index.cfm/fuseaction/artikkel/id/59823.

[45] William Stallings. *Operating Systems*. Prentice-Hall, Inc, fourth edition, 2001.

[46] William Stallings. *Network Security Essentials*. Prentice Hall, second edition, 2003.

[47] Andrew Tanenbaum, William Day, and Sandra Waller. *Computer Networks*. Prentice Hall, fourth edition, 2002.

[48] Jonathon E. Tidswell and John M. Potter. A graphical definition of authorization schema in the dtac model. In *SACMAT '01: Proceedings of the sixth ACM symposium on Access control models and technologies*, pages 109–120, New York, NY, USA, 2001. ACM Press.

[49] Mahesh V. Tripunitara and Ninghui Li. Comparing the expressive power of access control models. In *CCS '04: Proceedings of the 11th ACM conference on Computer and communications security*, pages 62–71, New York, NY, USA, 2004. ACM Press.

[50] Weigang Wang. Team-and-role-based organizational context and access control for cooperative hypermedia environments. In *HYPERTEXT '99: Proceedings of the tenth ACM Conference on Hypertext and hypermedia : returning to our diverse roots*, pages 37–46, New York, NY, USA, 1999. ACM Press.