Exchange of Patient Records – Prototype Implementation of a Security Attributes Service in X.500

Marjan Jurečič
Albert-Ludwigs Universität Freiburg
Institut für Informatik und Gesellschaft
Friedrichstr. 50
D-79098 Freiburg

Herbert Bunz
IBM
European Networking Center
Vangerowstraße 18
D-69115 Heidelberg

1 ABSTRACT

In Europe, the use of computers in health care industry has increased rapidly in recent years. This increase, however, has been accomplished with research efforts in the area of privacy and confidentiality of personal data. In the German legislation, protection of personal data is guaranteed by the constitution, granting a general right to privacy. This constitutional right has been amended by the German Central Court (Bundesverfassungsgericht). It says that each individual has the right to decide to whom and where he wants to give personal information.

In the US, similar problems of granting privacy and confidentiality of sensitive medical data will emerge. The Clinton administration's health plan has led to a discussion on privacy and data protection in the US. If that health plan is realised, it will lead to an exchange of personal medical data over data-highways.

In this paper, we will describe a prototype implementation of a secure hospital environment offering the basic functionality that is necessary for secure medical information storage and exchange inside a hospital computer network and the secure exchange of medical information over publicly accessible networks between different security domains. The functionality and security requirements have been derived in cooperation with a large university hospital in Germany, the University Hospital Freiburg. The relevant technical solution has been developed jointly by the IBM European Networking Center in Heidelberg and the Institute for Computing and Society University Freiburg. This paper will focus on the technical solutions to provide the needed functionality.

The main topics of this paper will be the security services granted, especially the role–based Access Control as well as the storage and retrieval of the Privilege Attributes (ECMA-138) for the various users. We shall describe how the Directory Service (X.500) is used for storage, retrieval and management of organisational structure information as well as for the dynamic handling of user roles and Privilege Attributes Certificates according to the suggestions of ECMA-138.

As a result, it can be shown that the security services and architectures currently under standardization are capable of providing sufficient security mechanisms. They also provide the flexibility necessary for the adoption to environments that deal with highly sensitive data even in a distributed applications environment.

2 INTRODUCTION

It is commonly agreed that properly designed clinical computer systems can increase the health care productivity and reduce medical costs. Moreover, patient treatment can be improved, too. These benefits can even be increased if there is an electronic exchange of medical information between different hospitals or between doctors. Such an electronic health data network is currently discussed in the Clinton administration's health plan [14]. The benefits a health information network offers are manifold. Information about

CCS '94- 11/94 Fairfax Va., USA
© 1994 ACM 0-89791-732-4/94/0011..$3.50

patients could rapidly be retrieved by doctors from anywhere in the country. This would speed health claims e.g. due to the avoidance of redundant medical tests.

Yet, all these benefits can turn into disadvantages. If there are no sufficient protection mechanisms, the patient information can easily be abused. It is evident that medical records include very sensitive private data. They may give information about genetic testing, sexual orientation, sexually transmitted diseases and other personal details. A more detailed discussion of the legal and social aspects of patient data exchange is beyond the scope of this paper and can be found elsewhere [12].

In a close collaboration with the University Hospital of Freiburg we have been able to elaborate the requirements end-users of a clinical information system have. These requirements are not only restricted to problems like ease of use or good performance of the system but they also include security questions, demands for safety and confidentiality and the trustworthiness of the system, especially concerning privacy enhancements.

Hospitals employ staff in several functions - ancillary staff, support staff (e.g. pharmacists and medical physicists), administration (e.g. medical records and medical secretaries) and direct care (e.g. consultants, nurses and radiographers). Most departments are computerized granting more or less security. But in most cases, no integrated solution exists for the whole hospital yet. Hospital computer and network equipment is often highly heterogeneous and there is almost no possibility for inter-department computer-communication. In the administrative sector of the University Hospital Freiburg we find the most computerized department, which is typical of most clinical centers. Here, the management of material, technical equipment, the personnel costs etc. is computer-based. But this is only an isolated solution within the clinical center, as are the computer environments in other departments of the hospital. Each computer environment is highly adapted to the needs of the specific department or lab e.g. the Picture Archiving and Communication System of the department of radiology. Thus there is no interoperability between the various systems.

Obviously, the need for an interconnection of these different environments comes up and thus the need for a hospital information system occurs. The system architecture for a communication environment should fulfill the following requirements:

- communication-protocols according to open standards namely OSI standards
- a uniquely structured communication-network with a high band-width
  (to support exchange of multi-media documents)
- a system security management covering all subsystems
- effective management of the whole system
- assurance of obedience to data protection laws in all proceeding steps
- standardized application e.g. for distributed application
- user-interfaces which are easy to use, especially an intuitive obedience to the security policy

Some important security requirements that can be derived are:

- the creator of a medical document or file has the responsibility for the obedience to all data-protection laws
- access rights to a document may change dynamically, depending on the context
- all steps in the treatment of a patient must be documented
- access rights should depend on the accessor's role/function (e.g. doctor, nurse, secretary ..) and on the "document"-type, too
- it should be possible to delegate access rights and responsibilities
- recovery of the data about the delegation of rights and responsibilities must be possible
- there must be a possibility to bypass security checks in case of emergency, but only with special audit activity

The demands for additional teleworking applications can be summarized as follows:

Clinical information relevant to the medical care of a patient is distributed over many locations within a hospital. The acquisition of patient data is supported more and more by computer based systems. Distributed data processing systems have to be connected via an Open Communication System in order to form a hospital information system. The success of doing this depends on the possibility to use standards for the communication of medical data.

Medical information consists of different data types from various sources, such as documents containing the patient history, laboratory results, classical X-Ray images or computer based data e.g from CT and NMR. The content of the documents may consist of text, graphics, images (bitmap) and audio. Thus, a document containing all relevant patient data is a multimedia document. There is a need for multimedia mailing and desktop conferencing. Physicians communicate diagnostic reports to exchange desired information. The main goal of this paper is to show that the security architectures and services that are under standardization are capable of forming a technical solution that grants the desired applications and services for storing, retrieval and exchange of medical data without compromising the needs for data security and confidentiality. The prototype implementation serves as a proof of this concept. The System Security Architecture implemented enables the enforcement of a large variety of security policies even such a complicated one as in a hospital environment. By means of a security firewall there is the possibility for inter-domain communication between different security domains, e.g. between a secure hospital network and a doctor's surgery. In the first chapter the global System Security Architecture will be explained in a more detailed way. The following chapters will discuss the single components of the architecture, mainly focusing on the implemented Privilege Server.

3 DETERMINATION OF THE SECURITY POLICY

In order to determine the appropriate security policy for a specific organization, the structure of the organization and the interdependencies between the different parts and members have to be investigated carefully. As a prerequisite for an organisational security policy there must be a well-defined **Organisational Model**. The enforcement of a specific security policy requires a set of rules that are used to determine the access rights of a given subject to a specific object. Thus the Organisational Model should at least contain

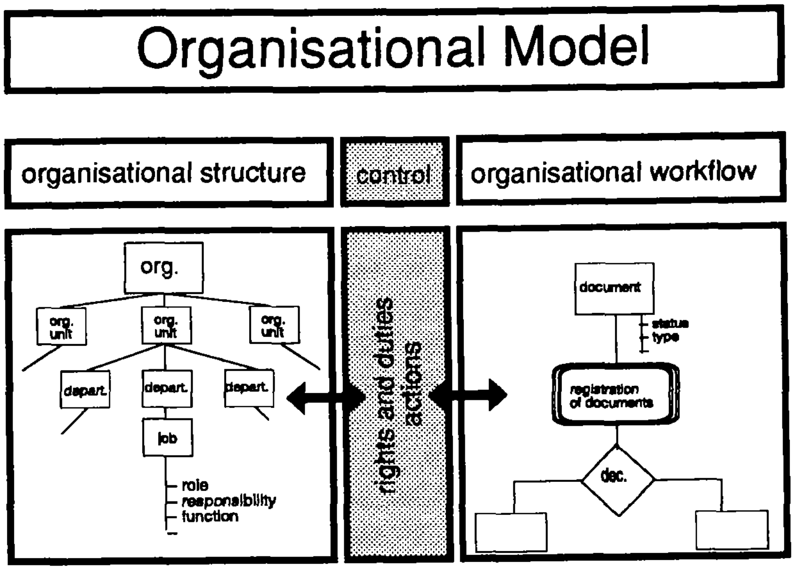

Figure 1: The Organisational Model

a definition of the various subjects or **principals** and the different objects that might be used or proceeded. Principals may be real persons, applications running on behalf of a real person, applications running on behalf of another application, etc.. Objects may be hardware, such as printers, application programs, the data that is proceeded, etc.. The organisational environment can be divided into three logical parts (see figure 1): One part contains the information about the structure of the organization, thus describing the hierarchy and dependencies between the different organisational units, departments and subdepartments of the specific organization. This part also contains the information about the different roles and/or tasks that can be identified. The second part holds all the information about the information proceeded including the flow of information and the usage of resources. The third part describes the rights, duties and possible (permitted) actions.

We have chosen the X.500 Directory [6] as the right place to map the organisational model on. However, extensions have been built into the X.500 service to form an **Organisational Directory**.

The **Organisational Directory** provides access to security related information especially

- public key certificates to verify digital signatures,
- Privilege Attribute Certificates, representing the actual rights of users,
- responsibilities,
- the classification of organisational units and connected responsibilities,
- and classification information about principals.

Therefore, the Organisational Directory contains all information related to the structure of the organization, the persons working in the organizations and their responsibilities. In order to model a complex hierarchical structure of an organization and the security information for the principals the following features of the Organisational Directory have been realized:

- freely definable directory schemes and object classes that allow for organization specific
  - modelling of the organisational structure
  - modelling of interdependencies
  - security privilege attributes for all principals
- Certification Authority
  - Public key certificates for each principal entry
- PAC Authority provides the
  - Privilege Attribute Certificates per principal entry
- security features to protect the stored data against misuse (X.509 [3], access control)

It is beyond the scope of this paper to discuss all these features of X.500 in general. Therefore we will only give a more detailed description of the PAC-Authority in section 6.

4 THE SYSTEM ARCHITECTURE

A clinical computer system has to serve at least three fundamental needs. There must be a comprehensive electronical medical record database, a friendly and easy to use computer interface for the medical professionals and a set of system interfaces to permit data exchange with other existing computerized systems. In addition, a workflow support for routine jobs is also very helpful. The picture (see figure 2) shows an overview of the implemented system architecture. The services and applications provided are:

Archive: A major requirement of physicians is to access and share clinical patient information electronically. As mentioned above, an electronic patient chart contains data of a multimedia type. For the purpose of storing and retrieving of multimedia data we have chosen to use an implementation of the DFR-Standard [8] which handles the stored data in a

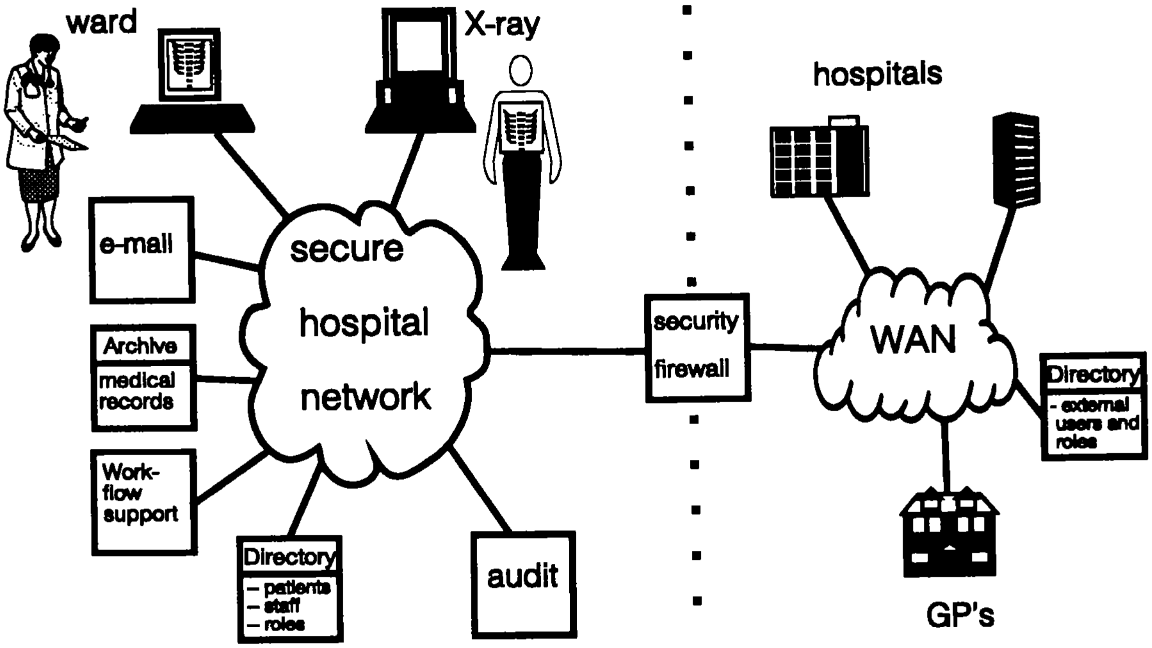

Figure 2: The system architecture

transparent way. DFR is an object oriented service for the storage of a large collection of documents in a distributed client server environment.

Electronic Mail: Electronic mail is a convenient way to exchange ideas and information. It can also simplify referral and consulting procedures. Mail interfaces used are SMTP and MIME.

Audit: From the point of view of controls as well as of legality, it is necessary to maintain records of the activities performed by each system user. Audit mechanisms also detect unusual events and bring them to the attention of the management. This commonly occurs through violation reporting or via an immediate warning to the computer system operator. The type of alarm generated depends on the seriousness of the event. In the current implementation these events are mainly of the type SecurityAlarmInfo [10], AlarmInfo [10] and SecurityAuditInfo [7].

Workflow support: A workflow application would ease the work with everyday tasks such as pharmacy orders or prescriptions. The workflow application uses and analyses the audit information and starts an appropriate action on the occurrence of a predefined audit information. The information to react on and the action to react with are freely configurable. In our prototype the workflow support is realised by a notification service. On specific actions in the hospital network e.g. admittance of a new patient the responsible person is notified via e-mail. But there is also the possibility of connecting the workflow application to an existing workflow-system.

Directory: There is a need to store and retrieve information about the hospital organization, including the employees and hierarchical organization data, too. This service is offered by the Directory application (X.500 [6]) which provides a repository for information about named objects. In addition to this informative aspect, the Directory is mainly used for security features e.g. for the secure mapping of users and their public keys.

User interface: The hospital application is of course easy to use. An acceptable application should not increase the workload of the user or constrain him to a specific workflow. But it has to assure the obedience to the security policy. In order to prevent the system from insider attacks a secure desktop with a graphic user interface has been built. The user interface is object-oriented and supports a wide spread of application programs such as e.g. text editors, image viewers and tools for medical image manipulation.

External communication: There is a gateway that supports communication with external partners on different (public) networks. Such a gateway is necessary e.g. for the physician wanting to communicate via e-mail with a specialist from another hospital.

In fact, this gateway is a security firewall that separates the trusted LAN of the hospital from the untrusted public network. This approach also minimizes the need to encrypt the data transmitted inside the trusted LAN.

The implementation on AIX is mainly based on ISODE 8.0. ISODE [15] is an openly available code for OSI services on UNIX platforms and has been adapted and extended to include the required security services.

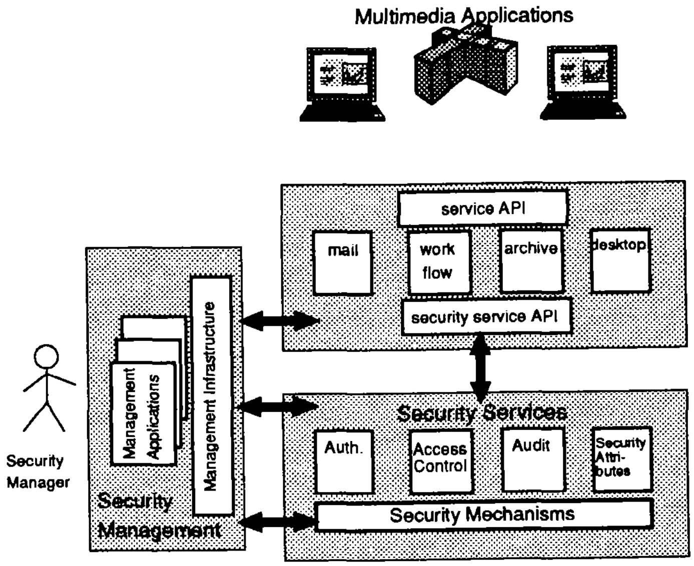

Figure 3: The security system architecture

The use of all these services must be under the control of a clearly defined Security Policy to avoid abuse of the sensitive data collected and transmitted.

Thus the system consists of a secure hospital network with different applications that are under control of a specific security policy. In terms of the DOD [1] a security policy is "the set of laws, rules and practices that regulate how an organization manages, protects and distributes sensitive information." A **security domain** can be viewed as a set of users who share the same security policy. The system architecture that has been implemented thus builds a security domain for all users in the hospital.

5 THE SECURITY ARCHITECTURE

The enforcement of the appropriate security policy for a security-sensitive hospital application requires a properly designed security architecture. Our goal has been to use existing open standards to the largest possible extent. The approach taken has been the combination of the OSI communication security standard with ECMA-138.

ECMA 138 [2] addresses security in distributed systems mainly focusing on Authentication and Access Control Services. ECMA 138 SECURITY IN OPEN SYSTEMS - DATA ELEMENTS AND SERVICE DEFINITIONS describes an approach to security in the context of completely open systems, rather than just communications. This standard adapts an object orientated client-server model of security interactions.

The standard that is generally accepted in security for open systems is ISO 7498-2-1988 SECURITY ARCHITECTURE [4], Part 2 of ISO 7498 OPEN SYSTEMS INTERCONNECTION - BASIC REFERENCE MODEL. ISO 7498 provides a reference model for communications between open systems (the well-known OSI Reference Model) and ISO 7498-2 which covers communications security for OSI protocols. But this standard does not cover the problems of security in distributed systems (processing and storage of data, etc.).

The picture (see figure 3) shows the major components of our prototype. The security architecture is composed of four major components. The Multimedia Applications as the interface to the user access the underlying distributed services over a specific service API. In our prototype these services are mailing, archiving, workflow support and a secure, personal desktop. The distributed services themselves are under control of a security policy which is enforced by the underlying security services like Authentication, Access Control, Audit and Cryptographic services. The third component consists of the Security Management. Security management affects the control, administration and review of a system security policy. In addition, it is concerned with the management of the security services and mechanisms.

5.1 THE ORGANISATIONAL DIRECTORY: PROVIDING SECURITY INFORMATION

The Organisational Directory provides access to security related information especially to public key certificates and Privilege Attribute Certificates. Therefore, the Organisational Directory contains all information related to the structure of the organization, the persons working in the organizations and their current responsibilities. For example the information about the doctor on duty of a ward can be found in the organisational directory. Due to the security policy, this role is connected with special access rights to all patient data of this ward. During a change of shifts the Organisational Directory has to be updated and the privileges connected with this role will be delegated to the new responsible medical doctor.

5.2 AUTHENTICATION SERVICE

The base of every Security Policy is a reliable identification of system users or, more general, of principals. The identity of the principal is established by using a Trusted Authentication Service which checks the credentials provided by the principal against an authentication database.

The Authentication service used is implemented in accordance with X.509 THE DIRECTORY: AUTHENTICATION FRAMEWORK [3]. The implementation used offers the cryptographic techniques needed for asymmetric encipherment and decipherment and for strong authentication. It is based on the OSI Security Package OSISEC [13] as provided e.g in CEC sponsored PODA-SAX, PASSWORD project. OSISEC provides the following functionality:

- systems for asymmetric key generation and providing of public key certificates
- establishing of "Certification Authorities" as defined in X.509 [3]
- mechanisms for distributing certificates
- mechanisms for integrity protection of information
- digital signature capability
- asymmetric key algorithms

The choice of cryptographic algorithms is unimportant, as long as they are consistently used over the network.

5.3 LABELING SERVICE

Labeled objects, as defined in ECMA 138 [2], use encryption and digital signatures to protect an object against modifications and misuse. Any object may be included in the certificate, and security labels are attached. Labeled objects provide a flexible way to secure migrating objects, e.g. security over insecure mail network as well as local security for objects. An object oriented interface for working with labeled objects has been implemented. This interface allows for the invocation of appropriate security mechanisms, according to the classification (label) of the object and the security policy.

5.4 ACCESS CONTROL

Access control policies in the hospital environment are quite complex and depend on the identity of the person, the current role, the document type as well as the current status. In addition, the environment is very dynamic - e.g. changes of shift or patients may be transferred to another department. In spite of the common use of ACLs (**A**ccess **C**ontrol **L**ists) for access control purpose this approach is not sufficient for the enforcement of a hospital security policy. ACLs cannot reflect the requested granularity and flexibility of access control for the great number of different documents that have to be accessed by various users. In an environment with a lot of different users and roles and a great number of objects the management of the Security Policy becomes impossible if the Access Control is based on ACLs only. Just imagine a change in the Security Policy of a large hospital, saying nurses are no more allowed to read the medical result of a patient. In the University Hospital under consideration this would lead to the change of the ACLs of the specific documents contained in more than 100,000 patient records. The consequence of this dynamic behavior in a model using only identity based ACLs would be an unacceptable administrative workload and would open potential risks - every change in the responsibility of an individual would cause changes to be done to the ACLs of all the objects the person has been and is responsible for. Therefore the access control service has been implemented in conformity with the suggestions of ECMA-138 [2] and X.741 [11] ISO/IEC DIS 10164-9: INFORMATION TECHNOLOGY – OPEN SYSTEMS INTERCONNECTION – SYSTEMS MANAGEMENT: OBJECTS AND ATTRIBUTES FOR ACCESS CONTROL. Furthermore, this approach offers the advantage of direct, high-level specifications of access control policy rules for the hospital organization and assures the enforcement of the security policy in all processing steps.

ECMA-138 defines a set of Security Attributes that can be attached to objects and subjects. These attributes can be used to label the objects (classification) with security information. Security Attributes attached to an object are named **Control Attributes**, attached to a subject or principal, they are referred to as **Privilege Attributes**.

In our current implementation we use the following **Control Attributes**:

- Security-confidentiality-class: is used for the classification of data to control read-access. Confidentiality classes are patient-record, medical-result, medical-report, administrational, etc.
- Security-integrity-class: is used for the classification of data to control write-access. Integrity classes are, care-documentation, medical-finding, etc.

The **Privilege Attributes** used are:

- Security-group: security groups may be secretaries, administration-staff, doctors, medical-staff, etc.
- Security-role: these roles may be assistant-doctor, chief-doctor, doctor-on-duty, etc.
- Security-capability-type-1: this attribute may be used to grant an explicit access right to a specific document for a specific user.

In addition to these ECMA-defined attributes hospital-specific Security Attributes have been defined, for example the LIST-OF-PATIENTS attribute. It contains information about the patients the user is responsible for at the moment.

5.5 SECURE DESKTOP

The secure desktop enforces the assurance of the security policy for all documents stored locally on a workstation. Integrity and confidentiality are provided through encryption of selectable document classes as well as the assurance of access control policies between different services, e.g. restricted distribution of an archived patient record via electronic mail. For example the hospital security policy might require that medical documents which are classified with the SECURITY-CONFIDENTIALITY-CLASS set to medical-result must be at least confidentiality-protected before they are stored to the local disk. This organisational algorithm would avoid insider attacks.

5.6 AUDIT

Audit is a necessary component within any secure environment. It has a complementary action to all other security services and allows to monitor the proper usage of the system and allows to detect security failures and potential breaches of the system security. However, audit is a pervasive service - it has to be implemented and consistently used by all applications, security services and network resources.

All created events have to be processed and distributed over the network to the according management applications without loss or duplication of events. However, management applications may temporarily be not available over the network - introducing dependencies of all applications to the properly working audit system. In addition, it is not acceptable that the performance of an application is heavily affected due to the auditing of events.

The local gathering of audit events has been realized in compliance with X.721 [10], X.740 [9], the remote audit management in compliance with X.700 [5].

5.7 SECURITY GATEWAY

The security gateway is the only point of connection between the hospital network and the external network. In order to avoid break-in attempts the following features are supported:

- protocol mapping (internal protocol not supported over WAN)
- verifying user identity and mapping of privileges
- confidentiality of the patient records over the public network
- separate audit of all external communication

The gateway currently allows external access to the patient archive, to selected information contained in the organisational directory and the workflow support.

5.8 SECURITY ATTRIBUTE SERVICE

As described in ECMA 138 ([2]), a Security Attribute Service provides attributes for entities on presentation of the authenticated identity of the entity . Security Attributes associated with an active entity in the distributed system are known as Privilege Attributes. For use in a distributed system, these Privilege Attributes have to be transferred via communication protocols and thus have to be protected against several attacks. ECMA-138 defines a Privilege Attribute Certificate (**PAC**), a form that can be transmitted in many security protocols and which is protected against a variety of possible security attacks. This protection is necessary because PACs are frequently under control of software entities which cannot be trusted. Thus the standard envisages protection against

- undetected modification,
- use by the wrong initiator with or without the collusion of the intended initiator,
- use for the wrong target,
- use outside stated constraints (in particular after the privileges have expired)
- and protection against use by the right initiator for the wrong purpose.

In every security domain there must be a reliable Security Attribute Service that provides attributes for the entities. In the next chapter we will describe how the Directory service can be extended to include the Security Attribute Service for the security subjects of a security domain, too, thus offering all the functionality of a PAC-Authority.

6 THE PAC-AUTHORITY

This section will describe how a Security Attribute Service has been implemented in the Directory service and how it serves for the access control in a prototype implementation of a security domain that represents a hospital environment.

Our extension to the Directory service goes far beyond an implementation of a simple repository for static PAC's. Indeed in our implementation the PAC is built dynamically on a user's request to actually reflect dynamic changes in the environment. Our experience has shown that it is not sufficient to offer Privilege Attributes depending only on the principal's authenticated identity. Moreover, the Privilege Attributes depend upon the principal's identity **and** his role. The same requirements, of course, arise in organizations, companies or hospitals. Physicians in a university hospital must be able to act in different roles, e.g. as doctors on duty or just as scientists – of course a different role then implies different responsibilities and rights. The figure (see figure 4) gives an idea of how the PAC-Authority works. On a user's request for a PAC, the PAC-Authority proceeds in the following way:

1. The initiator sends a PAC-request to the PAC-Authority together with its digital signature.
2. The identity of the initiator is proved by verification of his digital signature.
3. The initiator's entry in the Directory – containing his role attribute – is read.
4. The role entry that corresponds to the initiator's role attribute is read.
5. If the initiator does not appear in this entry as a role member, then his request for a PAC is denied. If necessary, additional mechanisms may be invoked to check the initiator's authorization for the requested role.
6. Otherwise the relevant Security Attributes – according to the security policy – are collected to form the set of Privilege Attributes for the initiator.
7. The role entry may contain additional attributes that point to another entry in the Directory. Depending on the security policy in force, these entries may also be evaluated so that their Security Attributes can be included in the PAC.
8. Now, after all the relevant Security Attributes have been collected the PAC is built – including all the necessary protection information.

This kind of procedure offers many advantages and support to the dynamic changes of responsibilities and duties that might appear in

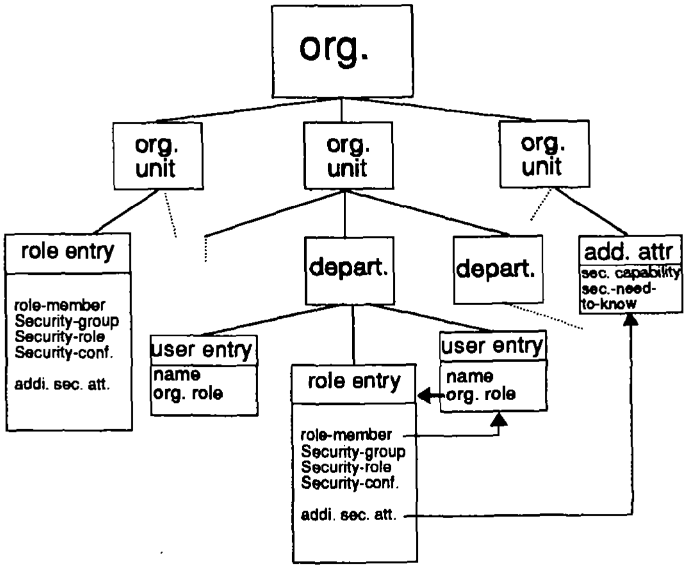

Figure 4: The PAC-Authority: Dynamic collection of Privilege Attributes

a real hospital environment. The most important advantage is the ease of use of security management actions as are:

- Security Policy Management
- Security Attributes Management

A change of shift e.g. is just managed by changing the ROLE-MEMBER attribute in the desired role entry to point at the user's entry of the new role occupant.

Management of Security Attributes and Security Policy is eased by sharing Security Attributes that different roles have in common. For example, in a specific organization all managers of a department have the same SECURITY-NEED-TO-KNOW attribute in common. Thus this attribute is held in a specific Directory entry that the ADDITIONAL-SECURITY-ATTRIBUTES attribute in each role entry of a department's manager points to. In the hospital scenario these entries are used to hold the information about the patients that are under treatment of a specific hospital-ward, their names or identification numbers are stored in a Directory entry that is shared by e.g. all the role-entries that are relevant for this hospital-ward.

Another example might be the use of the SECURITY-CAPABILITY-TYPE-1 attribute (see ECMA-138 [2]) which grants specific access to specific objects. This attribute can also be placed in a Security Attribute entry that is shared by different role entries. Let's assume that all managers of a department within a given organization share one specific Security Attribute entry, containing a SECURITY-CAPABILITY-TYPE-1 attribute. If the manager of this organization has the right to change the value of the SECURITY-CAPABILITY-TYPE-1 attribute, he has e.g. the possibility to give these managers temporary access to a document that is under his control. This is necessary if he e.g. wants to get some comments on an important contract he is just working on.

Due to the configurability of the implemented PAC-Server, changes in the Security Policy can be managed easily, too. There is an entry in the Directory containing configuration attributes for the PAC-Authority. These attributes give information about

- the Security Attributes that are permitted to be included into a principal's PAC,
- all the paths to additional security attributes entries that are permitted to be resolved
- and PAC protection information.

If a change in the security policy of an organization says that the use of the Security-need-to-know attribute is not allowed any more, the only security management action necessary is to change the appropriate configuration attribute in the configuration entry of the PAC-Authority.

Of course, these examples are not exhaustive, but they will give quite a good impression of the high adaptability to specific organisational requirements this implementation of a PAC-Authority offers.

6.1 SECURITY WITHIN THE PAC-AUTHORITY

The implemented PAC-Authority is only trustworthy if the Security Attributes stored in the Directory are sufficiently secure. This implementation of the Directory service has sufficient protection schemes to prevent unauthorized modification of attributes. Thus it is ensured that only the responsible security administrator is allowed to change e.g. the configuration attributes for the PAC-Authority.

7 CONCLUSION

The evaluation of the real requirements emerging from the computer users in a hospital environment leads to the conclusion that it is crucially important to keep apart the Application Standards and the Security Services. The Application Standards, however, should include consistent link-up points for the connection with extended Security Services. The security services and mechanisms should not be tied into Application Standards because of the resulting lack of flexibility.

Existing standards mainly deal with communication security. Nevertheless implementations are missing. Building distributed client-server applications requires more than communication security alone. There is a need for the definition of application-layer end-to-end security services.

Within the hospital environment end-to-end security can be achieved by the use of a trusted network that is strictly separated from other networks by means of a security firewall. The use of cryptographic mechanisms for intra-hospital communication is not practicable at the moment because of a reduction in performance. For external communication, however, they are suitable enough to ensure integrity and confidentiality protection of the information exchanged.

8 ACKNOWLEDGMENT

The described prototype implementation is a team effort and the authors are very grateful to all members, especially A. Bertsch for his technical contributions and the suggestions to this article.

References

[1] Department of Defense. *Department of Defense Trusted Computer System Evaluation Criteria*, December 1985.

[2] European Computer Manufacturers Association, Geneva. *ECMA-138, Security in Open Systems Data Elements and Service Definitions*, 1989.

[3] International Standards Organization, Geneva. *Information Technology - Open Systems Interconnection - The Directory - Part 8: Authentication Framework.*

[4] International Standards Organization, Geneva. *ISO 7498-2-1988(E), International Standard Security Architecture*, 1988.

[5] International Standards Organization. *ISO/IEC 7498-4: Information Processing Systems- Open Systems Interconnection - OSI Management Framework*, 1989.

[6] International Standards Organization. *ISO/IEC 9594-1: Information Technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models, and Services*, 1989.

[7] International Standards Organization. *ISO/IEC DIS 10164-8: Information Technology - Open Systems Interconnection - Systems Management: Security Audit Trail Function*, 1991.

[8] International Standards Organization. *ISO/IEC DIS 10166: Information Technology - Text and office systems: Document Filing and Retrieval (DFR)*, 1991.

[9] International Standards Organization. *ISO/IEC 10165-1: Information Technology - Open Systems Interconnection - Structure of Management Information: Management Information Model*, 1992.

[10] International Standards Organization. *ISO/IEC 10165-2: Information Technology - Open Systems Interconnection - Structure of Management Information: Definition of Management Information*, 1992.

[11] International Standards Organization. *ISO/IEC DIS 10164-9: Information Technology - Open Systems Interconnection - Systems Management: Objects and attributes for access control*, 1993.

[12] Marjan Jurečič, Ulrich Kohl and Ernst Pelikan. Safercom – ein prototyp für datenschutz in verteilten klinikanwendungen. *Datenschutz und Datensicherung*, 3:146–152, March 1994.

[13] Michael Roe, Steve Hardcastle-Kille, Peter Williams and Peter Kirstein. *The OSI Security Package: OSISEC User's Manual.* University College London.

[14] Gary Stix. Dr. big brother. *Scientific American*, February 1994.

[15] X-Tel Service Ltd. *The ISO Development Environment: User's Manual*, 1991.