MEDINFO 98
B. Cesnik et al. (Eds)
Amsterdam: IOS Press

Results of European Projects Improving Security of Distributed Health Information Systems

Bernd Blobel and Peter Pharow

Otto-von-Guericke University Magdeburg, Faculty of Medicine,
Institute of Biometrics and Medical Informatics, Magdeburg, Germany

Abstract

The challenge for improvement of quality and efficiency of health care systems causes the development and promotion of „Shared Care" in all developed countries. Distribution, decentralisation, and specialisation of health care must be joint with an extended communication and co-operation between the different care providers. Fulfilling the shared care paradigm, care supporting health information systems has to be distributed, interoperable, and scaleable too. Communication and co-operation across organisational, regional, and even national boundaries is bearing high threats and risks regarding security and privacy of medical and personal information of both patients and health professionals. Involved in several security projects funded by the European Union, the Medical Informatics Department and the regional Clinical Cancer Registry at the University of Magdeburg are piloting a secure regional distributed medical record system for cancer diseases. Requirements, solutions, and experiences are presented and discussed.

Keywords

Security; Data protection; Reliability; Digital signature; Privacy; Confidentiality; Integrity; Availability; Accountability; Smart cards; TTP

Introduction

Currently, in all developed countries there is a reorganisation of health care systems to a shared care structure for more efficient and high quality health services, which have to be supported by distributed information systems (IS) communicating and co-operating across organisational and even regional or national borders. In health care such systems record, process, stores, and distributes sensitive medical and personal information of patients and users respectively. Therefore, shared care IS are highly vulnerable and need enhanced security and privacy measures. The EU Health Telematics Applications Programme promotes by some projects solutions for secure health IS regarding different security issues as

- organisational aspects and High Level Policy [1, 2],
- smart cards, the specification of a set of layered interfaces for modular security functions and Trusted Third Party (TTP) based tools and measures for security infrastructures in heterogeneous networks [3] including Intranet [4] as well as
- architectural approaches for interoperable IS and distributed medical records [5].

To provide an enhanced practical solution for a secure distributed medical record in oncology within the regional Clinical Cancer Registry Magdeburg / Saxony-Anhalt, we have combined results and security solutions of all the mentioned EC funded projects the authors are involved in. Due to the restriction in pages, the paper can only address the chosen and combined measures and therefore refers to extended original publications.

A Common Security Model

The basic legal issues about security of personal and medical information are ruled in the „European Directive on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data" [6] and in the „European Recommendation No. R (96) of the Committee of Ministers to Member States on the Protection of Medical Data (and Genetic Data)" [7].

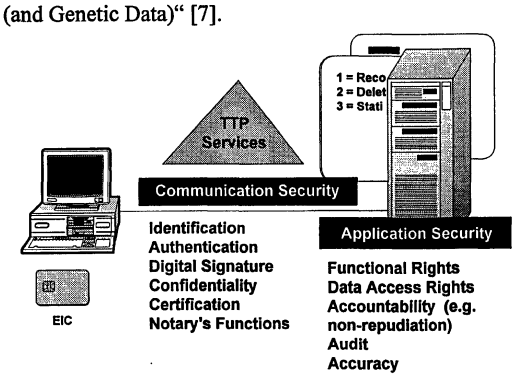

Figure 1 - Security types

Handling patient related information, the basic requirement is the provision of audited trust and non-reputable communication between authenticated partners and the audited non-reputable usage of applications in accordance with the 'need to know

principle'. The former requirement concerns the communication security; the latter concerns the application security [8], addressing the security dimensions integrity, confidentiality, availability, and accountability as shown in figure 1.

Each attack must be detected and any unauthorised access to communicated (communication security) or stored and processed (application security) information has to be denied. The relevant communication partners in the considered domain are usually health professionals and sometimes involved patients. The common principles for security provision in IS are based upon cryptographic algorithms. Especially public key algorithms (e.g. RSA) are used for identification and authentication, legal binding digital signature and session key exchange for confidentiality encryption using more efficient symmetric encoding algorithms. The digital signature facilitates integrity check and the proof of accountability of the user (non-repudiation functionalities). As a carrier for the keys and functionalities, the personal processor based smartcard format is an ideal one. Smartcards are supporting the user's logon procedures (single sign-on) for role-based access control and so allowing secure work from any user interface (PC). For health professionals, the Health Professional Card (HPC) as an example of a European electronic identity and profession card, including corresponding TTP services and interfaces, was specified and introduced within the TrustHealth 1 project framework [3]. In this context the need of an adequate electronic patient identity card is obvious.

Security Tools in Health Care Environment

Networks mediate communication and co-operation. Within health care and welfare, large organisations or regional structures use their own network structure as LAN, CHIN, MAN. In Germany, digital communication lines (ISDN) are wide spread. For that reason, the security mechanisms and the services mentioned in this chapter are based upon ISDN services or TCP/IP protocols.

On the other hand, the Internet or the Intranet related to domains has a growing importance in organisational and individual communications. So the chapter 4 will illuminate this aspect. Especially but not exclusively, general practitioners are interested in such opportunities for medical or general communication and information. The definition of security domains related to policy, legislation, duties, organisational issues, technologies etc. is used to specify an internal (more) secure area with restricted threats, risks, and attacks, which, e.g., is secured against external threats via firewalls. Our approach assumes in general an insecure world, specifying only secure micro-domains.

System Evaluation and Design

All systems including information communicating and processing ones are exposed several types of threats by human interaction or natural events. Risks in the context of information technology (IT) security define an aggregation of the likelihood of a threat actually occurring, the systems' vulnerability to that threat, and resultant consequence [9]. Real systems risks are especially determined on the one hand by social and economical circumstances and on the other hand by the security provided. The former factors are ruled by an adequate code of conduct and security policy. As an important project result, the SEISMED guidelines provide for these factors both definition/evaluation support and management tools [10], which will be updated and computerised by the SIDERO application within the ISHTAR project [2]. The latter risks-determining parameter requires corresponding organisational and technological countermeasures addressed in ISHTAR deliverables (e.g. [9]) and in a larger number of newly published books and papers.

Health Professional Card

Due to the sensitivity of the recorded, stored and processed personal medical data, in the Clinical Cancer Registry Magdeburg/Saxony-Anhalt as the first German health care IS a secure external communication has been introduced [11]. In the current phase, the system oriented security architecture will now be improved to a profession oriented solution based on HPC. Due to the situation on the market for the first implementation an available card was used, which will be replaced in Summer 1997 by the next generation of HPC then fulfilling the requirements of TrustHealth 1. The main functionalities of the actually used STARCOS PK version 1.0 card (implemented on a single-chip Philips 83C852) are e.g. the support of multiple applications, free definable control of processing, implementation of different file hierarchies (organisation of data), generation of digital signatures with the RSA algorithm, and differentiation of access controls (authentication, PIN). Due to the limited storage space the STARCOS PK 1.0 card contains only 2 private keys actually.

Our future HPC will hold at least 4 private keys: 1 for personal authentication, 1 for personal digital signature, 1 for personal decryption, and 1 private class key for group decryption. The latter is used in emergency cases. The use of 3 personal private keys facilitates the separated handling of decryption key availability on the application level (user working place, department) in the case of lost or destruction of that key, whereas the other keys are managed by more centralised TTP structures without any recovery functionalities.

Card Terminal

The smart card terminal, which is installed and used for calling the services and functionalities implemented, is named ICT 800. It is manufactured and exclusively designed for STARCOS smart card systems and STARCOS chip cards, and follows the Multifunctional Card Terminal Specification [12]. In addition to a normal chip card terminal, which is used for ID cards only, also two plug-in cards can be inserted at the bottom side of the terminal. The card terminal is equipped with a keypad according to ISO/IEC 9564, and a LC display fulfilling the T=1 specification. New terminal releases and versions related to new or extended standards will be handled by updating the internal software components.

Security Toolkit

For communication purposes between the card related part (smart card and card terminal) and the application itself a special security toolkit SecuDE (Security Development Environ-

ment) is used. It offers a library of security functions and an API written in C, which allows to implement security into virtually any application with functionalities as asymmetric cryptographic functions (e.g. RSA, DSA, DSS), symmetric cryptographic functions (e.g. DES, Triple DES, IDEA), and security functions for origin authentication, data integrity, non-repudiation of origin and data confidentiality purposes, as well as various hash functions (like MD2, MD4, MD5, SHA, Sqmodn). The software is able to handle X.509 public key certification functionalities, certification paths, cross certification, and certificate revocation. It provides utilities and library functions for the operation of certification authorities (CA) and interaction between a certifying CA and its certified users.

Trusted Third Party Services

To implement and to use the HPC within a secure infrastructure and within a secure network of services, several functionalities have to be installed which can be summarised as TTP services. Functionalities like naming, registration, certification, directory services, and key generation as well as card issuing are obvious. In that context, TTP employs X.509 V3 certificates and X.500 standard directories for distribution of certificates and revocation in the case of compromised or lost keys and cards respectively. These functionalities can be handled in a cross-certified as well as hierarchical manner. Regarding different security requirements depending on used services, mirrored (regularly updated) directories without any other TTP services could be provided on the application domain level, e.g. in the hospital. The discussion about a centralised or a decentralised key generation could be finished by the draft ISO 7816-8 proposing the key generation at the A6 secure environment of the smart card itself. Currently the decentralised key generation favoured for trust reasons is often rejected due to the insecure users' PC environment and the rest probability of doubled keys.

One of the most important aspects of designing and installing well-working TTP services is the trustworthiness of the involved organisations and institutions. That's why existing organisations in health care as e.g. the Physicians' Chambers of the federal states were asked to participate in developing, implementing, and evaluating real-working services for their members and users respectively. Within this paper, chapter 5 will reflect the situation.

Extensions to the Internet

Contrary to larger organisations mentioned in chapter 3, most of smaller institutions and GPs are not able (and sometimes also not willing) to implement additional functionalities which are necessary for realising the TTP functionalities mentioned above. But normally there is available another „port" into the electronic world - a port into the Internet and Intranet respectively. So this aspect results in a strong need to provide similar services also for Internet and Intranet based communications.

An application that has grown to be most popular on the Internet in the past few years is the World Wide Web (WWW). The WWW includes a body of software, a protocol suite and conventions that allow Internet users to access data through the use of a friendly user environment. Several efforts have been undertaken to address security in Web technology. In that context, the primary focus has been at the application level. The efforts have primarily addressed the issue of protecting the privacy, accuracy and authenticity of transactions conducted over the Internet.

The use of WWW in telemedical applications raises many threats to all dimensions of security. Since personal highly sensitive data are involved in a medical environment, particular measures guaranteeing data protection and data security have to be realised. As the number of telemedical applications using the WWW grows, security becomes an indispensable service for exploiting and utilising these applications in real (medical) environments.

The EC funded project „EUROMED-ETS" („ETS" in this case stands for a pan-European TTP Services network) deals with Internet based functionalities. The main objective of EUROMED-ETS is to exploit all aspects (operational, technical, regulatory, legal) of TTPs for telemedical applications on the WWW and to focus on implementing TTP functionalities using WWW means like Web servers and browsers for communication purposes. The project utilises standard Web tools such as Netscape and Mosaic, the authors' languages HTML (Hypertext Mark up Language) and VRML (Virtual Reality Modelling Language). Another objective is using the experts' experiences and findings to identify, define and verify operational, technical, regulatory and legal aspects of the TTPs especially for telemedical applications over the WWW. EUROMED-ETS concentrates on the establishment of TTPs for ensuring that all health actors are able to communicate in a secure way.

Secure Medical Record System in Oncology

Therefore, the Physicians' Chamber of the German federal state of Saxony-Anhalt was established as the (cancer caring) physicians' TTP of the catched region. The cancer centre implements the same functions for the non-physician staff. Regarding the real circumstances, all types of networks and protocols have to be served, including LAN, ISDN, and Internet etc. Therefore, TTP services based on LAN as well as Internet means have been implemented and tested to achieve cross-border TTP activities within Europe.

In the following an overview of the used software packages and the interfaces between them is introduced [13]. Cancer care is a typical example for shared care in the current health practice. Because different providers are involved in the same case of cancer care concerning the same patient, also the requirement for data communication and information access only in the context of the case and the defined purpose are fulfilled. Within the programme for nation-wide high quality cancer care in Germany, cancer centres and related clinical cancer registries have been established. As the first German (electronically) distributed regional cancer registry, the regional Clinical Cancer Registry Magdeburg / Saxony-Anhalt is nowadays covering a catchment area of 1.2 million inhabitants. Providing medical, caring, and organisational support, the register with its sensitive personal medical data has to guarantee adequate security on the

basis of advanced results of international research and development projects funded by the EC. Introducing the HPC, a TTP service structure has been developed regarding the structure of health care systems, cancer care, and physicians' organisatios.

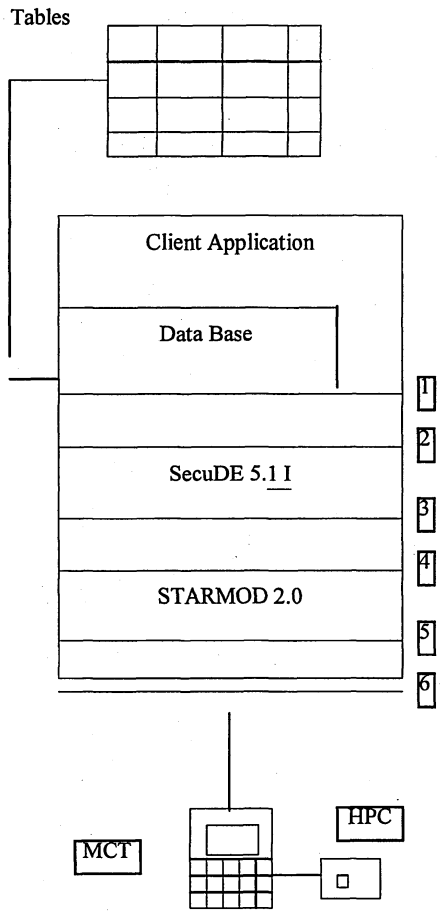

Figure 2 - Overview of software and interfaces (1-6)

Interface	Description
1	GSS - API, PKCS#7 - API
2	AF - API
3	Sec - API
4	STM - API
5	PCCTI
6	CT - API

Figure 3 - Interface Description

Middleware-Based Solutions for Distributed Interoperable Health Information Systems

Currently, distributed co-operating IS as distributed interoperable medical records are based upon middleware concepts as CORBA (Common Object Request Broker Architecture) of the OMG (Object Management Group), the European DHE (Distributed Health care Environment) approach, or HL7 (Health Industry Level 7 Information Standard) [14]. In such architectures, communication security but also application security related to functions provided by the middleware system has to be guaranteed. Additionally, the middleware must be able to promote the negotiation of security policy as well as of used protocols and algorithms, the optimisation of countermeasures as well as the access rights management transfer between applications. All security functionalities have to be transparent to the user, scaleable, independent on environments and platforms, using underlying services of operating systems, networks or DCEs. Such behaviour can be provided using credentials and security attributes as proposed in the OMG Security White Paper [15]. Using the CORBA specification to facilitate security, a generic security model was developed to introduce security measures into middleware based health IS [16]. The resulting security concepts, which joins the application and the middleware security services, has been introduced into the security architecture discussed in chapter 3 and is currently under development in our distributed cancer registry.

Discussion and Conclusions

Fulfilling the shared care paradigm, health IS have to support open systems' connectivity and -extending the mobility of both patients and health care providers throughout Europe - pan-European interoperability. In that context also the reliability and liability of business procedures have to be guaranteed. Therefore there is a need for trusted collaboration in the sense of communication and co-operation. Regarding the security requirements of the procedures and processes as well as the privacy requirements of users, all dimensions of data security as integrity, confidentiality, accountability and availability must be mentioned and taken into account. Beside of all others, in the future the latter both will get increasing importance considering common developments like distributed interoperable and multimedia medical record systems and the shared care provided by different legal and organisational types of health care institutions. Organisational and technical means for provision of availability are well known and are not to be discussed in this paper.

Providing strong authentication, legal binding and accountability by digital signature as well as confidentiality encryption, smart cards for health professionals (HPC) are the appropriate choice. (Supporting the patient's consent, electronic patient identity cards should be added.) Additionally a security infrastructure of a hierarchical system of TTP has to be provided, which should be organised regionally or nationally with international cross reference services. Security is depending on awareness and education of users and responsible staff. For that reason clear policy and appropriate continuous training for the different involved groups is required. To reduce the misuse of HPC, biometric methods to verify the identity of the card user as the card holder next year will replace the personal identifying number (PIN) with its known weakness. Security solutions

should be widely transparent to the users, mentioning all platforms and protocols as e.g. token in place by LAN-based and Internet-based TTPs. The openness of solutions can be facilitated by middleware approaches providing security.

Within the framework of the Cancer Centre Magdeburg / Saxony-Anhalt a secure distributed health IS pilot (an electronic medical record in oncology) was developed using the combined results of several EC funded Health Telematics Applications Programme projects on security in health IS. Based on systems' security evaluation and development (definition of a High Level Policy, performing a risk analysis) [1, 2], as the result of the TrustHealth 1 project [3] smart cards as well as an enhanced security infrastructure (TTP services) have been implemented. The security concept is based on minimal pre-assumptions and can be used in different environments under different conditions including networks as Internet and Intranet.

Acknowledgement

The authors are indebted to the European Commission, to the partners of the projects mentioned in the paper, and to the Ministry of Education and Science of the German Federal State Saxony-Anhalt for funding their research.

References

[1] Barber B, Treacher A, and Louwerse K. *Towards Security in Medical Telematics*. Amsterdam: IOS Press, 1996.

[2] ISHTAR Consortium. *Implementation of Secure Health Telematics Applications in Europe.* Project of the Fourth EU Health Telematics Applications Programme. http://www.ehto.be/projects/ishtar/

[3] TrustHealth Consortium. *Trustworthy Health Telematics 1.* Project of the Fourth EU Health Telematics Applications Programme. http://www.ehto.be/projects/trusthealth/

[4] ETS Consortium. *EUROMED - European Trust Structure.* Information Society Standardisation Programme. http://euromed.iccs.ntua.gr/

[5] HANSA Consortium. *Healthcare Advanced Networked Systems Architecture.* EU Health Telematics Applications Programme. http://www.ehto.be/projects/hansa/

[6] Council of Europe. *Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data.* Strasbourg, 1995.

[7] Committee of Ministers. *European Recommendation (Draft) No. R(96) of the Committee of Ministers to Member States on the Protection of Medical Data (and Genetic Data).* Strasbourg, 1997

[8] Blobel B. Threats and Solutions for Data Protection and Data Security in Health Care information Systems. Toward an Electronic Patient Record, Volume 5, Issue 8, March 1997, pp 1-16.

[9] Blobel B, Bleumer G, Müller A, Flikkenschild E, and Ottes F. Current Security Issues Faced by Health Care Establishments. *Deliverable of the HC1028 Telematics Project ISHTAR*, October 1996.

[10] The SEISMED Consortium, eds. Data Security for Health Care. Volume I-III. Studies in Health Technology and Informatics, Vol. 31-33. Amsterdam: IOS Press, 1996.

[11] Blobel B. Clinical Record Systems in Oncology. Experiences and Development on Cancer Registers in Eastern Germany. In: Anderson R, ed. *Personal Medical Information.* Berlin: Springer, 1997; pp. 39-56.

[12] Struif B, ed. *Specification for Multifunctional Card Terminal.* http://www.darmstadt.gmd.de/TKT/

[13] TrustHealth Consortium. Report on TTP development projects - German Site. *Deliverable D4.4 of the HC1051 Telematics Project TrustHealth 1*, July 1997.

[14] Blobel B, and Holena M. Advanced Healthcare System Architecture Using Middleware Concepts - A Comparative Study. *Deliverable of the HC 1019 Telematics Project HANSA*, July 1996.

[15] OMG. The CORBA Security Specification. Framingham: Object Management Group, Inc., December 1995.

[16] Blobel B. Security requirements and solutions in distributed Electronic Health Records. In: Yngström L, and Carlsen J, eds. *Information Security in Research and Business.* London: Chapman & Hall, 1997, pp. 377-390.

Address for correspondence

Dr. Bernd Blobel
Otto-von-Guericke University Magdeburg,
Faculty of Medicine,
Institute of Biometrics and Medical Informatics,
Medical Informatics Department
Leipziger Str. 44,
D-39120 Magdeburg,
Germany
Phone: +49-391-67-13542,
Fax: +49-391-67-13536
E-mail: bernd.blobel@mrz.uni-magdeburg.de