AIM (Advanced Informatics in Medicine)
Secure Environment for Information Systems in MEDicine
SEISMED (A2033)

Document Reference	SEISMED(A2033) / SP08.08 / HILD / DEL / 08.03.1995		
Deliverable No.	29	Distribution	All parties
Deliverable Type	Deliverable	Status	Final
Activity			

Title

Guideline for cryptographic mechanisms
— Health care management —

Author

Gerrit Bleumer, University of Hildesheim,
Institute for Computer Science
Samelsonplatz 1, D-31141 Hildesheim, Germany,
bleumer@informatik.uni-hildesheim.de

Keywords: Secure IT-systems; Encipherment mechanism; Digital signature mechanisms

Collaborators: Erik Flikkenschild (AZL), John Fowler (RLT), John Davey (HEIM)

EXECUTIVE SUMMARY

The comprehensive objective of SEISMED (a Secure Environment for Information Systems in MEDicine) was to elaborate a consistent, harmonized framework for medical data protection throughout Europe. The specific technical proposals of SEISMED are thus accompanied by a high level security policy which presents the underlying principles. This approach is consistent with the forthcoming European ITSEC activity.

SEISMED proposes a suite of cryptographic mechanisms in order to provide sufficient flexibility to meet the characteristic challenges of health care data processing:

- A long tradition of decentralized processing of health care data with multilateral and legitimate interests.
- Ultra high sensitivity of personal medical data whose disclosure might not be repairable by, e.g. smart-money.
- Long periods of time (up to 30 years) over which health care data must be archived in its original state.

A 20 man-month workpackage evaluated the pertinent cryptographic literature, other relevant EC-projects (RACE Integrity Primitives Evaluation project RIPE), and renowned conferences (IACR Crypto, IACR Eurocrypt, ACM Symposium on Theory of Computing, Symposium on the Foundations of Computer Science, IEEE Symposium on Research in Security and Privacy, etc.). The result is a cryptographic guideline which is presented by separate documents to three different target audiences.

Cryptographic guideline of SEISMED

Audience	Document Title	Content
Health Care Management	Guideline for Cryptographic Mechanisms —Health Care Management—	Odds and ends of cryptography: The use for health care IT-systems
IT-system end-users	Guideline for Cryptographic Mechanisms —IT-system end-users—	Odds and ends of cryptography: The benefits for IT-system end-users
IT and security personnel	Technical Recommendations for Cryptographic Mechanisms —IT and security personnel—	Suite of proposed cryptographic mechanisms

Health Care Management

This part addresses the management of a health care environment. While a rapidly evolving information technology often leaves the management confused, the management is responsible for keeping its health care environment working efficiently. To this end, *integrated IT systems* appear to be the ideal solution. This report identifies their specific risks which should be considered when deciding about new systems or upgrades of existing ones. This is even more important since indeed the management decides about IT-system installation, but in many cases the medical end-users like physicians are accountable for breaches of security of these systems. Hence, a management will only succeed in installing integrated IT-systems if it succeeds in inspiring the confidence of the end-users into these systems. Severe limitations of conventional security measures like passwords are identified and it is shown how these limitation can be overcome by applying cryptographic mechanisms. General aspects of integrating cryptography into existing applications are discussed.

IT-system end-users

This part addresses IT-system end-users, like physicians, medical staff, etc. who deal with sensitive medical data. Normally, these end-users are *personally* responsible for the medical data they input and process. Complementarily, they are also responsible if such data is modified or misused by other users. Hence, system end-users are particularly anxious about the risks which stem from the use of IT-systems. A conclusive introduction to the fundamental benefits of cryptography is provided which outlines how the identified risks can be reduced or eliminated.

IT and security personnel

This part addresses software and hardware designers and implementors who are responsible for the security of an IT-system. A suite of cryptographic mechanisms is proposed to be used by health care IT-systems.

First, the identified security requirements are mapped to cryptographic building blocks. Second, a few alternative cryptographic mechanisms are proposed to implement each building block. This two-step approach was found useful to make the document more readable and adaptable to future results in cryptologic research. In order to support the selection of mechanisms that comply with a given security policy, this report analyses explicitly how strong an adversary the proposed mechanisms resist. Two key applications in health care data processing are digital networks and databases. Specific proposals outline how these key applications can make use of the proposed cryptographic mechanisms.

Demonstrator

In order to demonstrate the functionality and efficiency of the recommended mechanisms, a software prototype (SECURE Talk) was built that protects data transferred through (linked) Apple Talk networks from unauthorised disclosure and undetectable modification. The demonstrator also provides an automatic key management for all cryptographic mechanisms. All results are documented in the document “Technical Recommendations for Cryptographic Mechanisms —IT and security personnel—”. SECURE Talk is available as a software application for Apple Macintosh from the author.

CONTENTS

1 INTRODUCTION

Processing of health care data involves medical, social, administrational, and business aspects. The on-going increase of medical treatment forces the health care environments to rationalize their organization, medical treatment, communication, and documentation. This is the driving force to employ IT-systems in health care. Characteristic problems of processing medical data are:

1. Highly sensitive data (severe patient interest),
2. Potential misuse of Health care IT-systems (organized crime),
3. Long periods of archiving and authentication of data

However, IT-systems might offer efficient access to personal medical data not only to the intended end-users, but also to unauthorized users. But the increased efficiency must not be accompanied by increased risks.

2 WHY ARE PASSWORDS INSUFFICIENT?

2.1 From closed systems to open systems

Formerly, and sometimes even today, ”closed” IT-systems have been employed in health care environments, i.e., in hospitals. People who played a certain role (e.g., physicians, medical staff, etc.) were authorized by a system manager to access (specific parts of) the system. Authorizations were granted to persons as long as their respective role required it. Technically, an authorization was simply a pair of a user name and a password and probably the keys to the appropriate physical locks. The system manager authorized a person by establishing such a name-password pair in the system and probably by handing out the physical keys. Hence, at least for the system manager there has been a clear and understandable distinction between authorized and unauthorized users. All the authorized ones have had been authorized by him personally.

This strategy addressed two of the major security aspects: **user and data authentication** and **confidentiality**. The dilemma of passwords has always been and will always be that they cannot be short enough for users to remember, but cannot be long enough to be secure. Except exhaustive search there are many other attacks to figure out passwords [Neum_94]. Moreover, the system manager usually has access to all data processed by the system. This applies as well to the companies maintaining the system. It has been seen quite often that highly sensitive data has been released to maintaining companies because some backup device, hard disk, etc. had been exchanged. Obviously, there must also be a certain amount of trust into the manufacturer of the system. Hence, the authentication of users and the confidentiality of sensitive data relies on a significant portion of trust among the authorized users, the system manager, the manufacturer, and the maintenance companies of a system.

During the 1980s the limitations of closed systems became more and more apparent. Users like physicians, medical staff, laboratories, clinical administration, etc. required to integrate databases and communication services. Additionally, a strong need for systems arose which are easy to upgrade and which can be connected modularly. These requirements continued to result in local area networks of mini computers, micro computers, workstations, PCs, etc. The local area networks in their turn were themselves linked by different kinds of wide area networks like ISDN, Fax, and Internet.

2.2 High efficiency at high risk?

From the viewpoint of the management of a health care environment IT-systems can be of significant help for cooperation in general and for documentation, communication, image processing, information retrieval in particular. However, processing health care data is embedded into a legal framework which must be respected regardless of the technology applied. A crucial point of such legal framework is how the cooperations of end-users like internal and external health care professionals, administration staff, etc. is regulated. These regulations state, for example, who may or must create, update, or maintain which documents; who may or must read and consult which documents; who must not read which documents. Usually, these regulations only take the end-users into account, but not the manufacturers, operators, and maintainers of these systems. [Neum_95] provides an excellent overview and valuable insight into the risks related to such a vulnerable web of entities relying one or more distributed systems.

A distributed IT-system can be understood by a ”box analog”. Consider a set of users who store, retrieve, and communicate their data by means of some box-system, e.g., a system of post office boxes. This box-system can handle postcards only, not envelopped letters. Each user has one box associated. The front ends of the boxes serve as interfaces to the users and each user is provided with a key matching the lock of the front door of his own box. The back ends of the boxes are simply open. A transport service is provided which collects input postcards through the back of the boxes and drops them into the addressed boxes.

The boxes and keys correspond to accounts and passwords, the postcards correspond to or image files, etc. With the box-analog in mind, distributed systems obviously bear a variety of new problems and risks.

Breaches of user and data authentication: Often, for medical documents a proof of origin is required in order to provide accountability. Conventionally, such a proof is provided by a handwritten signature under a document. Even if documents would exclusively be handled by the above box-system signatures would by no means be superfluous. For example, if a doctor Alice finds a medical diagnosis in his box indicating that it was sent by doctor Bob, what worth is that diagnosis? Nearly nothing; doctor Bob is not provided with any *proof* neither that the data received is the one sent (the reliability of the transport service must not be presumed), nor that the defacto sender is indeed the one claimed (some doctor Charlie might have masqueraded as doctor Bob.).

Breaches of confidentiality: Often, medical documents are confidential. Conventionally, such a document would be enveloped before it is transported. Even if documents would exclusively be handled by the above box-system envelops would by no means be superfluous. The content of postcards could be inspected by the transport service, and hence, it would be uncertain who will get to know the transported data except the intended recipient. The transport service of the box-analog corresponds to public transmission lines, operators and maintenance personnel of transmission and storage devices, etc.

Unauthorized access: More and more health care IT-systems are being opened to worldwide communication networks and, hence, provide remote access. In the box-analog this means that there are some boxes whose front ends are unlocked. For users who gain access to them the locks of other boxes are no longer relevant. Conventionally, unauthorized access and misbehavior is tried to be detected by audit trails. Although necessary, they are not satisfactory. In the best case they can prove a suspicion but they do rarely *raise* it. For example, a security manager who has to scan hundreds of pages of an audit trail in order to detect any breaches of security is likely to overlook suspicious entries. Let alone that he gets bored and stops reading after only a few pages.

Thus in principle, it is desirable to install —whenever possible—

preventive countermeasures rather than **subsequent** ones and

interior countermeasures, which are implanted within the IT-systems rather than **exterior** countermeasures, which support the organizational environment into which an IT-system is embedded.

Cryptographic mechanisms are a suitable means to reduce or to eliminate the above mentioned risks and to enhance the security of open distributed systems.

User and data authentication can be achieved by so-called **digital signatures**. A digital signature can be *produced* and *verified* only by some electronic device. To produce a signature, this device has to ”know” the personal signing key of the respective signer. The digital signature itself is a string of at least say 700 bit and thus cannot comfortably be verified simply by looking at it. Hence, it is verified by a device which moreover has to ”know” the verifying key of the signer.

Digital signature mechanisms provide an even stronger authentication than handwritten signatures can because they are specific not only for the originating user, but also for the message signed. An originator produces a different digital signature for every message he signs. Thus, if a message is modified after it has been signed this modification will be detected by the verifier. It should be clear, that digital signatures are completely different from ”digitized signatures” which are simply digitally represented handwritten signatures.

Confidentiality can be achieved by so-called **encipherment mechanisms**. Data can be enciphered and deciphered by some electronic device; possibly the same which produces or verifies signatures. Enciphering corresponds to enveloping the postcards of the box-system above.

A strong encipherment mechanism can prevent users to read data which they are not authorized to read although they might be able to read the enciphered form of that data. This applies e.g. to wiretappers in digital networks or intruders of database systems.

3 IF WE WANT TO EMPLOY CRYPTOGRAPHY, WHICH TASKS ARISE?

In order to design, enhance, or purchase a distributed and networked IT-system the security needs have to be analyzed as thoroughly and completely as possible. Some experienced person should be designated to analyze the threats and risks relevant to the IT system in question, Possibly a micro risk analysis must be performed. Based on these results, a security manager in charge of the system in question has to make the following decisions:

3.1 Cryptographic host facilities

The host machines, e.g., PCs, workstations, mainframes, have to be equipped with cryptographic facilities. The **cryptographic host facilities** might be hardware devices (plug in cards) or software libraries. It might be tempting to look after cryptographic add-ons for digital networks, operating systems, or databases such that the applications and drivers currently applied can be reused after upgrading the IT-system.

Note for example, that there are several products in the marketplace to secure networks: (PC-Plug-In-Cards for Novell, ISDN, external network devices which are placed between a PC and the network, etc.) These devices provide data confidentiality at link level (**link-by-link encipherment**), i.e., during transmission between network links, but not at the links themselves. In many situation, however, two end-users want to be sure that no-one and no network link may listen into their communication. This can only be achieved by **end-to-end encipherment**.

Although applying digital signature or encipherment mechanisms can be done automatically (and thus transparently for the end-users) the cryptographic management for digital signature mechanisms and end-to-end enciphermentcan in principle not be completely transparent for the end-users (see cryptographic management below). For example, if someone is to validate a document by attaching his signature he should be *aware* that and when he is signing it. Thus, it is possible to exchange, for example, network drivers by cryptographically enhanced drivers, but the applications using them have to be enhanced too; namely, by supporting cryptographic key management [Sand1_94, Sand2_94, Sand3_94, PaKa1_94, PaKa2_94].

3.2 Personal, mobile devices

The users, e.g., physicians, nurses, and patients have to be equipped with cryptographic facilities, too. Every user must hold some kind of **personal, physical device** which is capable to hold his personal keys and to produce his digital signatures or to encipher his messages for him. Such personal devices can be smart-cards, advanced cards, handheld pen-computers, etc.

3.3 Concerted action for a health care directory

Some consistent **cryptographic management** for cryptographic mechanisms and cryptographic keys has to be ensured at least for the IT-system in question. If the IT-system is interconnected with exterior IT-systems the appropriate standards and formats have to be obeyed [PaKa1_94, PaKa2_94]. An appropriate key management which will most probably be on-line (via some network) to the largest extent and off-line to a minor extent, for example to establish initial keys by exchanging diskettes, smart-cards, etc. Some person must be designated responsible for the key management which is to be consulted in case of error, malfunction, etc.

On a larger scale (regional, national, European, international) the management of cryptographic keys requires the maintenance of publicly available "digital books" which provide the cryptographic keys of all available end-users. Such a "digital book" is called a **Directory** [Bleu 94, ISO9594]. Currently, there is no directory service available which could be utilized by local health care establishments or general practicioners. The technical establishment of a Health Care Directory (HCD) requires a concerted action of the health care community, the local authorities and govenments or, at the level of the European Union, the Commission. In the long run the patients will draw considerable advantage from an HCD if it is really used to achieve advanced security for health care information systems. However, patients lack the formal representatives which could start a concerted action for a European HCD. Hence, it is more probable that the medical professionals initiate it, if they discover the enormous risks of the evolving federated and integrated information systems and realize their dependability upon such IT-systems. It is even more probable that a, e.g., a consortium of a telecom company and a software vendor simply offer a directory service and a network software which makes use of that directory and provides end-to-end encipherment and digital signatures. (See Privacy Enhanced Mail on the Internet, etc.)

Rather than simply buying security off the shelf such products need further promotion.particularly by the health care community including the managements of local health care environments. A sufficient request should finally result in a suitable offer of directory services as well as of products employing them.

3.4 Training and awareness

Applying cryptography is a technical means which must be supported by **training and awareness program**. All parties involved must be informed about their benefits and must be motivated to use the new features appropriately. For example, social and legal impacts of digital signatures (HLSP_94) should be anticipated by the trainers and should be discussed by the IT-users.

4 HOW DO CRYPTOGRAPHIC MEASURES FIT INTO OUR LEGAL SITUATION?

The legal situation and patent situation with respect to cryptography in health care data processing is far from harmonious throughout Europe. Data confidentiality is considered a sensitive topic by either governments and by health care communities. For example, in Scandinavia health care data must be enciphered before transmission over public lines whereas in France and Italy this is prohibited. The necessity of digital signatures is much more agreed, but clear and consistent regulations about their legal validity are still lacking not only in Europe. On the one hand, the current and local legal situation must be explored before putting cryptographic mechanisms to every day's practice. On the other hand, the health care community should pioneer in applying cryptographic mechanisms since they reflect the interests of patients and of physicians in more and more complex IT-environments. This engagement implies to influence legal and technical development as well as further standardization.

BIBLIOGRAPHY

Bleu 94 AIM SEISMED: Bleumer G: Technical recommendations for cryptographic mechanisms —IT and Security Deliverable 29, SP08.10; ©Universität Hildesheim, Germany, 1994.

ISO9594 ISO/IEC: Information Technology–Open Systems Interconnection–The directory Part 1…8; ISO/IEC International Standard 9594, 1990.

KaGr 94 AIM SEISMED: Katsikas S: High level security policy for health care establishments, Deliverable 14, SP04.03; ©University of the Aegean, Greece, 1994.

Neum 94 Neumann P G: Risks of passwords; Communications of the ACM 37/4 (1994), 126

Neum 95 Neumann P G: Computer Related Risks; Addison Wesley - ACM Press, Reading Massachusetts 1995.

PaKa1 94 AIM SEISMED: Patel A: Guidelines of the possible implementation of the security mechanisms and protocols by the reference centres —Health Care Management—, Deliverable 27, SP09; ©University College Dublin, Ireland, 1994.

PaKa2 94 AIM SEISMED: Patel A: Guidelines of the possible implementation of the security mechanisms and protocols by the reference centres —IT and Security Personnel—, Deliverable 27, SP09; ©University College Dublin, Ireland, 1994.

Sand1 94 AIM SEISMED: Sanders P: Baseline security guidelines for existing systems —IT and Security Personnel—, Deliverable 26, SP07; ©University of Plymouth, England, 1994.

Sand2 94 AIM SEISMED: Patel A: Guidelines of the possible implementation of the security mechanisms and protocols by the reference centres —Health Care Management—, Deliverable 27, SP09; ©University College Dublin, Ireland, 1994.

Sand3 94 AIM SEISMED: Patel A: Guidelines of the possible implementation of the security mechanisms and protocols by the reference centres —IT and Security Personnel—, Deliverable 27, SP09; ©University College Dublin, Ireland, 1994.