Security for Decentralized Health Information Systems[‡]

Gerrit Bleumer

Institut für Informatik, Universität Hildesheim, Samelsonplatz 1, D-31141 Hildesheim, Germany

bleumer@informatik.uni-hildesheim.de

Running Title: Decentralized Information Systems

Keywords: Authentication, Confidentiality, Distributed System, Key Management

‡ This work was partly funded by the EC project SEISMED.

Summary

Health care information systems must reflect at least two basic characteristics of the health care community: The increasing mobility of patients and the personnal liability of everyone giving medical treatment. Open distributed information systems bear the potential to reflect these requirements. But the market for open information systems and operating systems hardly provides secure products today. This “missing link” is approached by the prototype SECURE Talk that provides secure transmission and archiving of files on top of an existing operating system. Its services may be utilized by existing medical applications.

SECURE Talk demonstrates secure communication utilizing only standard hardware. Its message is that cryptography (and in particular asymmetric cryptography) is practical for many medical applications even if implemented in software.

All mechanisms are software implemented in order to be executable on standard hardware. One can investigate more or less decentralized forms of public key management and the performance of many different cryptographic mechanisms. That of, e.g., hybrid encryption and decryption (RSA + DES–PCBC) is about 300 kbit/s. That of signing and verifying is approximately the same using RSA with a DES hash function. The internal speed, without disk accesses etc., is about 1.1 Mbit/s. (Apple Quadra 950 (MC 68040, 33 MHz, RAM: 20 MB, 80ns. Length of RSA modulus is 512 bit.)

0 Introduction

Health care is one of the most fundamental needs of society and, hence, it is deeply woven into modern societies. Many *subjects*, i.e., individuals and organisations take part in health care. Patients look for adequate treatment of their diseases and want their personal data to be protected. Physicians, general practitioners, and nurses provide the health care services. Insurances mostly do the financing. National and international organisations constantly watch the population's state of health and try to improve it. All the subjects together are called the *health community*[1] in the sequel. Obviously, these subjects have their specific interests, which might be conflicting [1].

Well-being of individuals depends upon *trustworthy* and *economically viable* health care *services*. This implies that, e.g., physicians are personally responsible for the treatment they prescribe[2] and patients may choose the physicians they trust[3]. Hence, one basic characteristic of the health community in contrast to, e.g., companies or the military is that its subjects are not and should not be ruled by one central authority. Otherwise the health community would soon face some kind of big health care brother.

Chapter 1 translates health community needs into requirements on health care information systems. Chapter 2 sketches how some requirements can be met by the use of cryptographic mechanisms. Chapter 3 sketches a prototype that demonstrates usability and performance of such mechanisms.

1 Requirements on Health Care Information Systems

Information is the vital link by which the subjects of the health community co-operate. Increasing mobility and transborder co-operation of these subjects have enforced a trend towards large scale integrated medical information systems. Facing the severe restrictions of centralized systems, medical information systems begin to make use of open distributed architectures, which achieve financial (lower cost of off-the-shelf computing and communication products), technical (e.g., interoperability, connectivity) and credibility enhancing (no need for one trusted central authority) advantages.

Let A denote the set of potential *subjects* interacting with an information system S. The term subject denotes any person who has access to the system (by means of some interface). Examples of subjects are conventional end users, system administrators, maintenance staff, as well as attackers who tap lines or inject viruses. An information system S may then be specified by a set I of interfaces i_a for each potential subject $a \in A$ and an *attacker model* $\mathcal{A}$. An interface i_a may be defined by a *functional specification* (which output at interface i_a should be produced by given inputs at any interfaces of I) and a *security specification* (which outputs at interfaces of I should not be produced by given input at interface i_a). The *attacker model* of a system describes for each subject $a \in A$ the worst case behaviour of all subjects $b \neq a$ under which the functional and security specifications of

---

1 The term "health community" is meant as a sociological rather than a technical term

2 E.g., physicians swear their hippocratic oath before they enter their profession. This oath stresses their personal responsibility for every treatment they prescribe.

3 This freedom of patients to choose their physicians is not common practice in all EC member states.

i_a still hold. From the viewpoint of a particular subject a, system S is the more trustworthy the “stronger”[4] its attacker model $\mathcal{A}$ is, i.e., the less a's interface specifications depend upon other subjects' behaviour (at interfaces i_b, $b \neq a$).

A *system S* is called *decentralized* if the attacker model for at least each of its end-users a comprises the behaviour of all other subjects $b \neq a$. “Other subjects” includes in particular those subjects having access to central parts (e.g., communication lines, switching centres, mainframes, etc.) of system S.

In health care, some of the characteristic security requirements at end-user interfaces are *long-term authentication*, *confidentiality*, and sometimes *anonymity* [2]. As these security requirements refer to individual subjects, they are reasonable requirements only on decentralized information systems. An integrated information system not committing to the above requirements would not be trusted by, e.g., many physicians and, thus, they would not use it or would refuse to disclose personal data to it. The system were neither trustworthy nor economically viable. Hence, decentralized information systems will play an important role in health care.

The above requirements can be achieved by means of cryptographic mechanisms. Obviously, there are other important requirements, e.g., to define which users are authorized to initiate which transactions upon which data (at which time, etc.), availability of services etc. These latter are not considered here.

1.1 Integrity and Authentication

Perhaps the most important security requirement on storing, processing and transmitting medical data is to ensure its *integrity*, i.e., to prevent undetected, unauthorized modification of the data. In general, this is achieved by appending some information to the data, which serves as a proof of *authentication* to the recipient if and only if it is received uncorrupted. Sometimes it is not only required that the recipient himself is convinced that some data is authentic but he should be able to prove this fact to third parties, too. This kind of authentication is called *non-repudiation*. Once, the author of some data has authenticated this data, his authorship will be provable to any recipient.

Physicians and nurses are personally accountable for the treatment they give to patients. Hence, health care information systems must support to authenticate documents about patients in order to archive them over long periods of time (usually 20 to 30 years). The need for authentication also applies to documents being transmitted. Future applications in telemedicine might highlight this need even more: e.g., medical observation of patients in their homes in order to shorten the periods patients stay in hospitals [2]. Various forms of electronic signatures are technical solution to this requirement.

---

4 The term “stronger” is quoted because it does not imply a total order on the set of all possible attacker models.

1.2 Confidentiality

Most medical data is highly personal and sensitive. Accordingly, it is to be protected from unauthorized disclosure during transmission as well as during storage [3]. The technical solution to achieve this in open systems is to use encipherment mechanisms.

1.3 Anonymity

Telemedicine might allow patients to access medical information systems and/or expert systems. In the past, information technology has brought more and more services directly to end users without moderation by experts (e.g., desktop publishing, home shopping, etc.) In the future, this might also apply to the medical field. E.g., patients might want to anonymously consult expert systems about mental health care, psychiatric and/or psychological advice, etc.

2 Using Cryptography in Medical Applications

If cryptographic mechanisms are used by medical application software they clearly have to be trustworthy and economically viable. Trustworthiness is achieved by using only published mechanisms that have resisted several years of detailed analysis by independent researchers. Furthermore, the implementation of these mechanisms and their management has to be publicly evaluated according to suitable security criteria. Economic viability can be achieved if software implementations of cryptographic mechanisms are used which are run on standard hardware platforms that are already in place in the health care environment. Within the EC's Advanced Informatics in Medicine (AIM) programme, SEISMED[5] explores the feasibility of this approach by developing SECURE Talk — a demonstrator for cryptographic mechanisms. Chapter 2.1 deals with the integration of cryptographic mechanisms into medical applications in general.

2.1 Integrating Cryptographic Mechanisms into Medical Applications

To put cryptographic mechanisms into every day practice, one has to integrate them smoothly into existing applications. Smoothly means almost transparent to the intended users. The user interface and the performance should not be affected, unless additional security justifies significant alterations.

Naturally, cryptographic mechanisms would be placed within the operating system and/or the network [4]. The commercial need for secure open systems increases and the market of commercial operating systems and computer networks is beginning to reflect this by utilizing cryptography. But so far, there are no commercial operating systems or networks available that (i) provide enhanced security by asymmetric cryptography and (ii) use only cryptographic mechanisms that are publicly evaluated. And even if such products were available, most health care environments were unable to afford a completely new operating system and/or network in the short run.

---

5 SEcure Information Systems in MEDicine (SEISMED) develops a framework of guidelines how to develop and maintain secure health information systems throughout Europe.

This lack motivated the development of a prototype that demonstrates the performance and usability of cryptographic mechanisms. The prototype allows to process files cryptographically and/or to transfer them. I.e., it can encipher, decipher, sign and verify files, or do combinations of these. The internal encryption and decryption rate achieved is 1.1 Mbit/s using a hybrid encryption mechanism. The signing and verifying rate is approximately the same using a DES hash function and RSA (at 512 bit modulus length.) This would allow, e.g., to support 16 ISDN D-channels simultaneously. The prototype is a standalone application collaborating with any existing medical application on a file by file basis.

3 A Prototype for Software Cryptography

The prototype SECURE Talk demonstrates secure communication utilizing only standard hardware. It shows, in particular, which mechanisms yield what performance. The most complex mechanisms are symmetric and asymmetric encryption, message authentication codes and digital signatures.

The message of this prototype is that cryptography (and in particular asymmetric cryptography) is practical for many medical applications even if implemented in software.

The recent years have shown that the computational power of hardware one can buy for one ECU increases by at least 40% each year. This means that software cryptography will fulfil the requirements of more and more ambitious applications at constant cost even if the algorithms are not improved. The prototype presents the operability of software implemented cryptographic services which are integrated into a simplified scenario.

This scenario is interactive, (transparent,) sequential multi-user, secure end-to-end file handling between the workstations[6] of a LAN.

It might, e.g., represent data transfer between the physicians (and/or patients) of different hospitals in possibly different regions or countries. It might, as well, represent the communication within one department of a hospital.

Interactive means that a command interpreter constantly offers a menu of communication and security services to the user, waits for a command, executes it and waits for the next one.

Transparent means that the **security management** is done nearly automatically. This optional feature releases the user from managing parameters and keys as much as possible. In an optimal case, one does not even notice that security services protect the communication.

Sequential multi-user means that multiple users are supported at the same workstation one after another[7]. The underlying operating system is not assumed to support a multi-user mode although this would be helpful. Users are requested to identify themselves before they gain access to the prototype. The basic version of the pro-

---

6 It is explicitly assumed that autonomous workstations are running in the network, not only terminals. These workstations may but need not be equipped with hard disks, CD-drives, smart card readers, etc.

7 This is a common requirement for many workstations of a hospital information system, e.g., ward PCs.

totype will support user identification by passwords, future versions might replace this method by more sophisticated techniques like smart cards, biometrics etc. A dependable identification mechanism will be the key to accountability, a necessary property of a system dealing with sensitive data.

Secure end-to-end means that the content of the communication is protected at the application layer [4] against repudiation of authorship (data authentication), undetected, unauthorized modification (integrity) and unauthorized disclosure (confidentiality). Other network layers are not affected by SECURE Talk.

File handling means that SECURE Talk supports the participants of the underlying LAN in loading, storing, and securely exchanging files created by arbitrary applications. (This includes text–, code–, picture–, video–, biosignal–, sound files, etc.) A generic way to exchange data between applications is by file. Hence, the smallest data unit protectable by SECURE Talk is a file. Many medical applications are supposed to be supportable by this interface, i.e., their communication can be directed into files, which can be transferred by the prototype. Of course, secure file handling in such a generic way does not cover every communication need of *every* medical application. At present, it appears unreasonable to adapt SECURE Talk to more specific data structures.

Beside exchanging other applications' data, SECURE Talk integrates editing and exchanging short text memos. This might be found comfortable not only by users who are used to e-mail.

The hardware assumptions of the prototype reflect the decentralized character of a typical health care environment. It is only assumed that there is some digital, bit transparent network (e.g., ISDN) connecting the workstations available.

Hard- and Software requirements: SECURE Talk 1.0 is implemented for workstations that run Apple operating system 7.0 or higher and are connected by Apple Talk (Ether Talk or Local Talk). On-line features require a set of at least 3 workstations. Off-line features can be demonstrated on at least one single workstation. Only the Apple operating system and the SECURE Talk software have to be installed on each machine. **No extra hardware, especially no crypto hardware is needed**.

Features: All symmetric and asymmetric cryptographic mechanisms are implemented and available as software modules. Characteristic parameters (security parameters, mode of operation, etc.) of each mechanism may be modified by a user as they are subject to the user configuration. This allows high flexibility and adaptability to future needs.

Among the available mechanisms are: Encipherment mechanisms like DES, G-DES [5], RSA encipherment [6][8], electronic signature mechanisms like RSA, ElGamal [7] and Damgård [8] signatures, DSS [9], the crypto-world's first provably secure[9] electronic signature mechanism GMR [10], etc., hash

8 To avoid active attacks, RSA encipherment is improved by a redundancy predicate.

9 Provably secure here means: provable under the assumption that factoring large integers is hard. No other unproven assumption is needed in contrast to many other electronic signature mechanisms like RSA, El Gamal, DSS, etc.

functions based on any blockcipher available and cryptographically collision free ones [8] and cryptographically strong pseudo-random number generators like the one presented by Blum, Blum, and Shub [11].

Acknowledgement

I would like to thank Birgit Pfitzmann, Joachim Biskup and Andreas Pfitzmann for fruitful discussions. Thilo Baldin did an excellent job on designing and implementing parts of the prototype.

Bibliography

[1] Joachim Biskup: Protection of Privacy and Confidentiality in Medical Information Systems: Problems and Guidelines; DATABASE SECURTIY, III : Status and Propects, IFIP 1990, pp. 13-23.

[2] Andreas Pfitzmann, Birgit Pfitzmann: Technical Aspects of Data Protection in Health Care Informatics; Advances in Medical Informatics, J. Noothoven van Goor and J. P. Christensen (Eds.), IOS Press, Amsterdam 1992, 368-386.

[3] Council of Europe (ed.): Convention for the protection of individuals with regard to automatic processing of personal data; European treaty series n^{o} 108; 1981.

[4] ISO: Information processing systems – Open Systems Interconnection – Basic Reference Model – Part 2: Security Architecture; INTERNATIONAL STANDARD ISO IS 7498-2; First edition 1989-02-15.

[5] Andreas Pfitzmann, Ralf Aßmann: Efficient Software Implementations of (Generalized) DES; SECURICOM 90, 8th Worldwide Congress on Computer and Communications Security and Protection, March 13-16, 1990, Paris, 139-158.

[6] R. L. Rivest, A. Shamir, L. Adleman: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems; Communications of the ACM 21/2 (1978) 120-126, reprinted: 26/1 (1983) 96-99.

[7] Taher ElGamal: A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms; IEEE Transactions on Information Theory 31/4 (1985) 469-472.

[8] Ivan Bjerre Damgård: Collision free hash functions and public key signature schemes; Eurocrypt '87, LNCS 304, Springer-Verlag, Berlin 1988, 203-216.

[9] CACM (some editing): The Digital Signature Standard Proposed by NIST; Communications of the ACM 35/7 (1992) 36-40.

[10] Shafi Goldwasser, Silvio Micali, Ronald L. Rivest: A Digital Signature Scheme Secure Against Adaptive Chosen-Message Attacks; SIAM J. Comput. 17/2 (1988) 281-308.

[11] L. Blum, M. Blum, M. Shub: A Simple Unpredictable Pseudo-Random Number Generator; SIAM J. Comput. 15/2 (1986) 364-383.