Cryptographic Protection of Health Information: Cost And Benefit

Joachim Biskup, Gerrit Bleumer
Institut für Informatik,
Universität Hildesheim,
Samelsonplatz 1,
D-31141 Hildesheim, Germany
{biskup, bleumer}@informatik.uni-hildesheim.de

Running Title: Protection of Health Information

Keywords: QUALITY OF HEALTH CARE (N4.761),
MEDICAL INFORMATICS (L1.700),
COMPUTER SECURITY (L1.209)
CONFIDENTIALITY (I1.880.604.583.80),
LIABILITY (I1.880.604.583.490),
COSTS AND COST ANALYSIS (N3.219.151).

SUMMARY

Medical, legal, and economic reasons inevitably force health care establishments to apply more and more open distributed IT systems rather than the less flexible and more expensive mainframes. Managing, for example, electronic patient records by various users at different locations by means of large scale client-server systems requires new security provisions for storing, archiving and communicating those data. Using an analogy, data processing is being changed from railroads to highways. Formerly, only one engine-driver was responsible for the security of a whole train, whereas now the car-drivers themselves are responsible each for its own car. Unless the cars are equipped with suitable security mechanisms like breaks and safety belts this change endangers individuals within and outside the cars. Cryptography provides many of the relevant security mechanisms for open distributed health care IT systems. Indeed, suitable cost effective cryptographic products are available but are rarely found in health care IT systems. The reason is more political than economic: Diverging national security interests in the EU have prevented strong security in public telecommunication infrastructures arguing that, e.g., criminals would profit, too. The resulting uncertainty of investments delays the development, standardization and installation of cryptographic solutions.

1. INTRODUCTION

Cryptology has become a subject of open research since the early 70's. Despite its fascinating potentials, it is rarely used by the best selling hardware and software products except its very trivial mechanisms like password protection. However, commercial companies and customers begin to realize their need for cryptographic security. Recently, three leading international industry organizations (EUROBIT, ITI, JEIDA) submitted a policy statement to the G-7 Global Information Society Summit in Brussels saying that "...without pervasive cryptographic technology there can be no basis for privacy or trust, and the main benefits of the new industrial revolution cannot be realized...".

2. IT IN HEALTH CARE: A NECESSARY RISK

The goals of public health care systems in Western democracies are to provide (1) high quality medical care for everybody, (2) at limited cost in terms of political economics and (3) to comply to human rights of patients including self-determination and equity of care. Information technology (IT) contributes to each of these goals but also introduces alarming risks. (Also see [1].)

Potentials of Health Care IT	Goals	Medical Concerns	IT Security Requirements
Harmonized medical nomenclature, language, procedures	(1, 3)	• Restricted expressiveness • Negligible use • Bureaucracy	—
Wide area, long time access On-line databases Off-line patient held databases	(1, 2) (1) (3)	• Useless flood of data • Insufficient for emergencies • "Invisible" modification, addition, deletion	• Availability • Authentication • Non-repudiation • Confidentiality
"Cradle to grave" patient records		• Sources of data untrusted	
Interoperable equipment for measuring and data processing	(1)	• Diffusion of responsibility • Privacy breaches	
Reuse for secondary purposes:	(1, 2)		
a) Medical research, data mining	(1)	• Privacy breaches	• Confidentiality • Anonymity
b) Enhanced medical education	(1)	• Privacy breaches	
c) Quality assurance, audit	(1, 2)	• Privacy breaches	• Anonymity • Non-repudiation • Separation of duty
d) Resource controlling	(1)	• Surveillance of staff	
e) Financial controlling	(1)	• Diffusion of liability	

Table 1 Potentials of IT in Health Care, Medical Concerns and Security Requirements

Big potentials are i) *harmonized medical nomenclature, language and procedures* which increase the quality of care and patient self-determination by supporting independent understanding of diagnoses, ii) *wide area and long time access* to medical data and iii) interlinking medical diagnoses up to "*cradle to grave*" patient records; the two latter being the logical consequence of the former. Access can be provided by on-line databases and by off-line patient held devices. Hence, iii) increases the quality of care and the patients' self-control of their data. As a further potential, iv) *interoperable equipment for measuring and processing* medical data and laboratory results would increase efficiency and cost effectiveness of health care. Finally, v) *primary health care data could be reused for several secondary purposes*. Clearly there are medical concerns about the benefits of these potentials which have to be discussed prior to any technical implementation. In addition, Table 1 identifies the resulting security requirements for health care IT.

Obviously, the goals of public health care systems conflict with each other. The progress in health care is driven by the first goal whereas the cost effectiveness and patient self-determination are necessary conditions under which health care can smoothly progress (Fig. 1). Applying IT in a public health care system has two inevitable consequences. Firstly, more and more personal patient data will be acquired and linked for medical, economic and legal reasons [2]: More accurate diagnoses can be provided, the local health care establishment gets more competitive, and the medical professionals can collect legal evidence in case they should be sued for malpractice later on. Secondly, the overall budget of the health care system claimed by the health care establishments (HCE) increases: Independent from the cost to install IT, the number of positive diagnoses increases simply because measurements become more sensitive and more frequent. At the same time the average price per treatment increases too since the information technology must amortize. The goal to be cost-effective counters the latter by restricting medical treatment, by putting some cost on the patients' excess or by capping the prices of the health care establishments. This is the subject of periodically emerging "health care reforms". In case a reform succeeds, the overall cost of the public health care system is reduced which implies that innovations are delayed and the quality of health care decreases. Hence, negative feedback to the first goal is established.

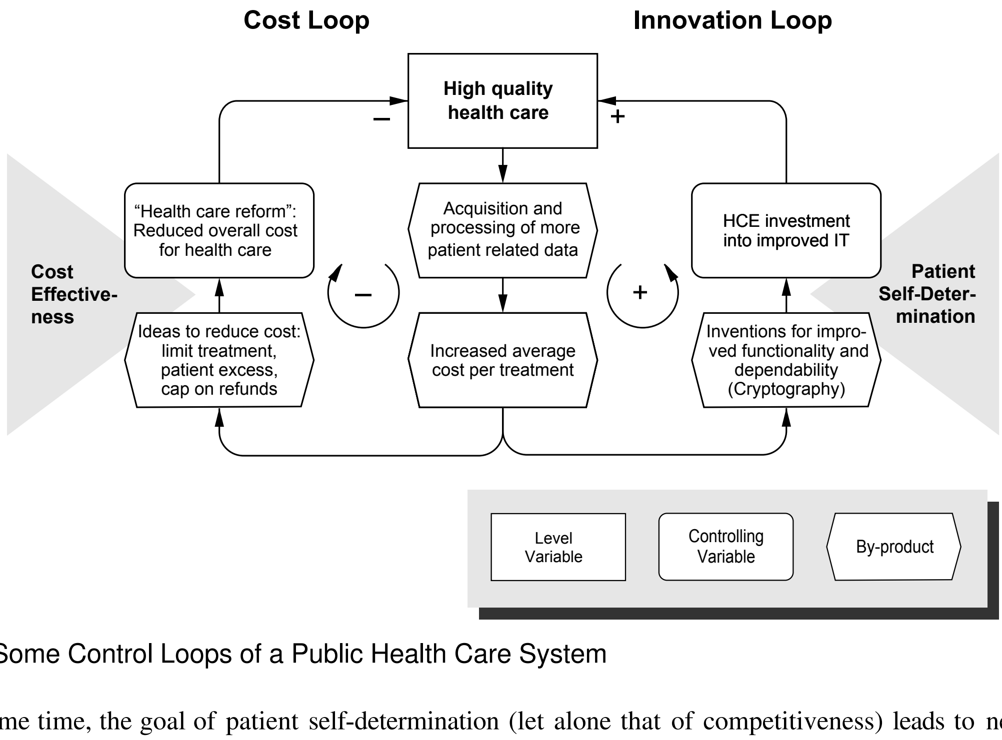

Fig. 1 Some Control Loops of a Public Health Care System

At the same time, the goal of patient self-determination (let alone that of competitiveness) leads to new inventions for improved functionality and dependability of IT. Although common practice, it is certainly not enough to rely on so-called "trusted" system kernels and cleared administrators. Rather patients could turn from passive usees into active users controlling their medical records. Here, cryptography is a necessary tool since it allows to enforce one's own vital security needs although using globally interlinked information systems and networks. As soon as products evolve from these ideas health care establishments tend to install them for the medical, commercial, and legal reasons mentioned above. Even more underhand is that improved diagnoses and therapies push forward the evolution of pathogens. Hence, positive feedback to the first goal is established.

3. CRYPTOGRAPHY IN HEALTH CARE IT: A NECESSARY TOOL

In order to design secure health care IT, particularly the goal of patient self-determination (3) must be translated into data objects, operations on data objects, rights and obligations for operations, etc. This has lead to various security models [3, 4] some of which have been applied to health care establishments [5, 6]. However, a convincing formal security model for at least some relevant applications in health care is still missing. A promising paradigm for the translation was suggested by [7], an approach to formalization in general is found in [8]. Enforcing self-determination ultimately requires some technical means for the self-control of personal data. This is the realm of cryptography.

Confidentiality can be achieved by encipherment mechanisms. *Authentication* can be achieved by message authentication codes or by digital signatures, depending on whether the receiver trusts in the sender of a message or not. Authentication against distrusted senders is also called *non-repudiation*. Authenticating documents guarantees for detecting any kind of subsequent modification. Authenticating binary executables is a perfect means to protect from viruses, worms, etc. [9]. If an entity, e.g., a user, performs an action indistinguishably the entity is said to be *anonymous* with respect to that action. For example, patients might require anonymity for remote mental health consulting. If several actions of the same entity cannot be detected as originating from one same entity, let alone by which, that entity is said to be *unlinkably anonymous* [10]. This is, e.g., required if individual behavior must not get profiled. Sometimes the right to sign or to encrypt must be controlled by sharing it among different individuals (*separation of duty*). This can be achieved by threshold cryptography [11].

We will briefly outline digital signatures and public key ciphers: Every participant holds a personal secret, her secret key, and derives from it a corresponding public key, her cryptographic address. (This can later be generalized to several secrets per participant, e.g., for signatures and ciphers.) The cryptographic addresses of all participants are listed in a public directory and it is impossible to reconstruct the secret of any individual from its corresponding cryptographic address in the public directory. A participant can now sign a message by using her own secret and every recipient can verify that message's signature by using the sender's cryptographic address which he simply looks up in the directory. Similarly, a participant enciphers a message by using the cryptographic address of the intended recipient and the recipient deciphers the ciphertext by using her own secret. Note, that each participant uses completely different secrets for signing and for deciphering.

Loosely speaking, digital signing and enciphering is generating secrets and addresses, distributing addresses and cryptographic coding. *Cryptographic coding* is similar to conventional coding, except that it depends on the sender (e.g., producing and verifying signatures) or on the recipient (e.g., enciphering and deciphering). This introduces the problem of *key distribution*. The distribution of cryptographic addresses is similar to the distribution of conventional network addresses, e.g., e-mail. There might be public directories to look up cryptographic addresses. However, unlike conventional addresses, keys must be authentic, i.e., provably correct. For example, if one looks up a wrong address under the right recipient's name, the message will probably not reach the intended recipient. But if one looks up a wrong key, the message might be revealed to some intruder. The latter is definitely unintended whereas the former is usually regarded as an unspecified error. Eventually, the security of digital signatures and ciphers relies on properly *generating the secrets*. Users who have their secrets generated by other instances, e.g. trust centers, do no longer control their own information.

If long files are transmitted or stored, the speed for enciphering, deciphering, signing and verifying converges to roughly the same speed, since fast pre-processing becomes the dominating factor. Off-the-shelf cryptographic processors (for e.g., DES, IDEA) achieve about 3 Mbyte/s and software operating on standard hardware allows for 250 Kbyte/s [12]. One conference [13] already reported software implementations of the latest and less crypt-analyzed mechanisms to perform at up to 5 Mbyte/s using standard hardware.

4. COSTS AND OTHER HURDLES

Although cryptography can be a profit center in itself it is rarely found in health care IT. Pointedly, the reason is more political than economic. We put 5 statements and a reminder highlighting the case for cryptography:

STATEMENT 1

Either patients are being appointed to effectively control their medical records by means of properly managed cryptographic mechanisms (delegation included) or the public acceptance of health care IT will be undermined to such an extent that modern health care itself is jeopardized.

In the near future, the health care information systems of regions, countries and continents will be closely interconnected such that this system federation will be highly security critical but far from secure. At the same time, patient records get more sensitive than they have been ever before (e.g., genetic analysis, hereditary diseases). Software based systems are estimated to be orders of magnitude less dependable than 10^{-9}/h, 10^{-5} /demand [14], which is usually held to be acceptable. Even more sobering is that these defects pay to the software manufacturers [15]. Besides, countless viruses sabotage the development and operation of IT systems. Fortunately, cryptographic integrity shells could eliminate this problem and are less costly than constantly updating virus scanners and monitors [16].

STATEMENT 2

In near future cryptographically equipped operating systems, network systems, database systems, etc. will be the rule rather than an exception. Cryptography in standard applications will be available at no additional cost.

Microsoft, IBM, Apple, Lotus and Novell will provide cryptographic mechanisms in their forthcoming products at the operating system, network system, and information system level. Today, standard active ISDN cards for PCs provide hardware encryption and authentication at the network layer for about 28% extra charge. Since the same hardware design is used, the extra charge is for the cryptographic customization only and will rapidly decrease if the demand increases. The next generations of products aim at security concepts applicable to several system layers, including the application layer (OSF-DCE [17], OMG-CORBA [18]). Even where cryptographic mechanisms are subject to patent claims, licenses are usually granted for nominal prices.

STATEMENT 3

The specific security requirements of HCEs call for integrating cryptographic mechanisms into medical applications, too. This will be at some additional cost but saves much money which is otherwise paid for countless security patches (firewalls) and overtime caused by system collapses.

What is really specific to health care *and* to security and what is thereby costly is to integrate a proper key generation and key management (chapter 3) into the medical applications like health care telematics, nursing systems, image and signal processing, etc. The evolving cost can be reduced the more the earlier such security requirements are taken into account during the specification process. Standardized cryptographic application programming interfaces [19] are a promising means for cryptographically open systems.

STATEMENT 4

Publication and retrieval of public keys will be just another standard service of public networks just as the well known X.400 address service is a standard on the internet today.

The commercial sector increasingly calls for national and international infrastructures to manage and distribute public keys [20]. The extra cost involved for health care will be negligible compared to the extra cost resulting from the expected amount of data transmitted in multi-media telemedicine.

STATEMENT 5

The reason why today's health care IT systems make no use of cryptography is not its cost, it is the lack of an agreed political strategy for IT security and cryptography that takes into account the legitimate individual, commercial and national security requirements.

Dependability of interlinked information systems ultimately requires security standards and independent evaluation of products [21]. Today, the contrary is true in most of the world: Specific security criteria for health care do not exist, and governments come up with diverse and incompatible national regulations. Even worse, these ad-hoc regulations put additional cost on organizations who have already invested into security [22], e.g., the FBI initiative which forces US telecommunication providers to assist in the Law Enforcement Act, or the analogous German legislation which is expected to cost each D-Netz provider about 20 MECU.

REMINDER

Considering that health care IT is becoming a big business, it is up to the HCEs to formulate their vital security needs mentioned above and to create the corresponding demand in this business sector.

The evolution of secure open systems including cryptographic compatibility, is always at danger by manufacturers that long for proprietary products and by legislation aiming at national security at the cost of individual security. HCEs could counter these tendencies by a strict quality control prior to purchasing, joining industry consortia, and co-operating in advisory boards on national security legislation.

ACKNOWLEDGMENT

We thank Ab Bakker, Birgit Pfitzmann and Matthias Schunter for their constructive criticism and helpful comments on an earlier draft of this paper.

BIBLIOGRAPHY

1 O'Connor K: Confidentiality, Privacy and Security Concerns in the Modern Healthcare Environment; *The Australian Computer Journal* 26/3 (1994), 70-77.

2 Jonas H: Towards a Philosophy of Technology; *The Hastings Center Report* 9/1, 1979.

3 Biskup J, Brüggemann HH: The Personal Model of Data; *Computers & Security* 7/6 (1988), 575-597.

4 Castano S, Fugini M G, Martella G, Samarati P: *Database Security*; Addison Wesley - ACM Press, 1995.

5 Henkind SJ, Orlowski JM, Skarulis PC: Application of a Multilevel Access Model in the Development of a Security Infrastructure for a Clinical Information System; American Medical Informatics Association: *Symposium on Computer Applications in Medical Care* 17/10 (1993), MacGraw Hill, 1994, 64-68.

6 Pangalos G: Security Guidelines for Database Systems Development; *Database Security XIII*: Status and Prospects, IFIP Transactions A-60, Elsevier, Amsterdam 1994, 353-370.

7 Kluge E-HW: Health information, privacy, confidentiality and ethics; *International Journal of Biomedical Computing* 35/1 (1994), 23-27.

8 Biskup J, Bleumer G: Reflections on Security of Database and Datatransfer Systems in Health Care; in: *Proc. IFIP 13th World Computer Congress 94*, Volume II, Elsevier, Amsterdam 1994, 549-556.

9 Davida GI, Desmedt YG, Matt BJ: Defending Systems Against Viruses through Cryptographic Authentication; *IEEE Symposium on Security and Privacy*, IEEE Press, Washington 1989, 312-318.

10 Chaum D: Security without Identification: Transaction Systems to make Big Brother Obsolete; *Communications of the ACM* 28/10 (1985), 1030-1044.

11 Desmedt YG: Threshold Cryptography; *European Transactions on Telecommunications* 5/4 (1994), 449-457.

12 Bleumer G: Security for Decentralized Health Information Systems; *International Journal of Biomedical Computing* 35/1 (1994), 139-145.

13 Anderson R (ed.): *Fast Software Encryption*; LNCS 809, Springer, Berlin 1994.

14 Laprie JC: How Much is Safety Worth? in: Technology and Foundations; *Proc. IFIP 13th World Computer Congress 94*, Volume III, Elsevier, Amsterdam 1994, 251-253.

15 Wirth N: A Plea for Lean Software; *IEEE Computer* 28/2 (1995), 64-68.

16 Cohen F: A cost analysis of typical computer viruses and defenses; *Computers & Security* 10/3 (1991), 239-250.

17 Rosenberry W, Kenney D; Fisher G: *Understanding DCE*; O'Reilly & Associates, Sebastopol 1992.

18 OMG Security Working Group: OMG White Paper on Security; OMG TC Document 94-4-16, Issue: 1.0, available from: Framingham Corporate Center, 492 Old Connecticut Path, Framingham, MA 01701-4568.

19 Linn J: Generic interface to security services; *Computer Comunication* 17/7 (1994),483-491.

20 Chokhani S: Toward a National Public Key Infrastructure; *IEEE Communications Magazine* 32/9 (1994), 70-74.

21 European Communities - Commission: ITSEC: Information Technology Security Evaluation Criteria (Vers. 1.2, 28/06/1991); Office for Official Publications of the European Communities, Luxembourg 1991.

22 London W: EC Information Security Legislation: Where Now?; *Computer Law and Security Report* 10/5 (1994), 226-233.