Security for the Digital Information Age of Medicine: Issues, Applications, and Implementation

Michael A. Epstein, Michael S. Pasieka, William P. Lord, and Nicholas J. Mankovich

Privacy and integrity of medical records is expected by patients. This privacy and integrity is often mandated by regulations. Traditionally, the security of medical records has been based on physical lock and key. As the storage of patient record information shifts from paper to digital, we find new security concerns. Digital cryptographic methods provide solutions to many of these new concerns. In this paper we discuss the new security concerns, new legislation mandating secure medical records, and solutions providing this security. Copyright © 1997 by W.B. Saunders Company

KEY WORDS: security, medical records, cryptography, teleradiology, digital signatures, certificates, RSA, smartcards.

TECHNOLOGY CAN meet increasing demands for secure digital medical information arising from patients, policy makers, and others.^{1,2} Banking and the military already use security technologies. This article is an overview and survey of security as applied to medicine. It covers the changing needs for security, available technologies, and implementation considerations. From the perspective of a health care consumer, privacy of medical information can be very important.³ Insurance or job opportunities may be denied if news of a patient's medical condition is discovered. Public figures may get unwanted publicity should medical information be released. Patients with medical conditions having an associated social stigma will not want knowledge of their condition disseminated or they may wish anonymous access to disease-related information. Recognizing the demand for secure medical records and the increased potential for abuse with digital information, the US government recently has adopted legislation to meet these demands.

In pre-computer medical environments, the security of records relied on physical lock and key. Many computer-based systems have individual users interacting with specific information gathering or presentation applications. Security for these

systems also can rely on physical lock and key, but usually implement locks via passwords. With today's networking technology as an enabler, managed health care strives for efficiency and broader access to medical information. In this networked environment, a whole new paradigm for security must be implemented, as multi-facility health maintenance organizations (HMOs) and information-hungry community health information networks (CHINs) increasingly are relying on non-secure networks, like the Internet, to exchange what should be private, immutable, and verifiable medical information.

We begin this article by introducing the major issues that are of concern in providing a secure medical environment, with reference to the techniques used to provide such security. Next, we discuss the protocols used to ensure security. Finally, some of the legal requirements of health care institutions to provide security, and the legal restrictions on the use of security technology are presented.

ISSUES OF SECURITY

Security is a complex objective. To successfully achieve this objective, the issues and terms must first be defined:

- **Authentication:** Are users who they say they are?
- **Access Privileges:** What applications and information can a particular user read, write, or modify?
- **Privacy:** Can the information be understood by someone other than the intended recipient?
- **Immutability:** Can the information be modified without detection?
- **Accountability:** Did the person responsible for the information *really* sign it?
- **Traceability:** What is the change and review history of the information?

A *communications model* cryptographers use to analyze security concerns is shown in Fig 1. Each of the participants in an exchange have traditional names to refer to them:

- **Client:** An approved party wishing to obtain, modify, or add to information contained on a server. In the medical domain this would be a

From Philips Research, Briarcliff Manor, NY.

Address reprint requests to Michael A. Epstein, MS, EE, Philips Research, 345 Scarborough Road, Briarcliff Manor, NY 10510-2099.

*Copyright © 1997 by W.B. Saunders Company
0897-1889/97/1003-1040\$3.00/0*

Fig 1. A communications model.

medical professional, such as a doctor, nurse, or administrator.

- **Server:** A repository for needed information. In the medical domain this could be a hospital's central computer system.
- **Trent:** A trusted third party. A person or computer system that can be trusted by both the client and the server without reservation. In a secure system this party serves as the basis for trust over a network.
- **Eve:** An attacker that can eavesdrop on communication between the client and server. It is assumed that Eve can read all bits transmitted over the network. Eve also has the ability to store and analyze these bits.
- **Mallory:** An attacker that is more powerful than Eve. Like Eve, Mallory can see all the bits on the network, but also can delete, modify, or add bits in the transmission of any bits on the network.

The assumption of abstract powerful attackers aids in building secure systems. It is clear that if attackers such as Eve and Mallory can be defeated by the security of a system, then more realistic attacks also will fail.

CONCEPTS FOR SECURE SYSTEMS

To address the issues introduced in the previous section, a collection of methods are available. For clarity, these methods are discussed individually. How one uses these methods in various combinations and interactions with users and systems is called a *protocol*.

Encryption for Privacy

Encryption is the mathematical means used to disguise a message so as to hide its contents from unauthorized viewing. A significant early step in

any protocol used for the establishment of a secure connection is the agreement of the server and client on the type of encryption to use. Modern cryptographic systems rely only on the security of the key. It is assumed that an attacker will obtain knowledge of the cryptographic algorithm and the protocol. There are two major types of encryption currently in use: *symmetric key* and *public key*. Each has strengths and weaknesses. In practice, most protocols use a combination of both types, relying on the strengths of both.

The basic protocol used by both systems is straightforward. The message, also termed *plaintext*, is encrypted via a mathematical method into *ciphertext*. The ciphertext then is transmitted over a channel that is assumed not to be secure. The ciphertext then is decrypted via an inverse mathematical method back into the original plaintext message.

In a *symmetric key encryption* system, there is only one key used for both the encryption and decryption of a message. The strength of this method is the relatively fast speed of the encryption and decryption algorithms. This makes the use of symmetric key encryption attractive for bulk transfers of information.

The major drawback of a symmetric key scheme (like the one shown in Fig 2) is the problem of key distribution. If two parties desire to communicate securely, a single key must be generated in a secure manner in one location and then transported securely to a second location for use. This example of distribution also makes an assumption that there are only two parties who must communicate securely. In situations in which many parties each need independent secure communication with each other, key distribution is a major problem. For example, if there are 10 parties, each must have a separate key to communicate with the other nine. The total number of keys, which must be generated and

Fig 2. Symmetric key encryption.

correctly distributed, is $n(n-1)/2$ or, in this case, 45. Adding one more party to the group means generating 10 more keys and securely distributing one to each of the other 10 parties. In any large system, this problem rapidly grows out of control.

In a *public key encryption* system, there are two mathematically related keys. Encryption and decryption are asymmetric. That is, one cannot use one key to both encrypt a message and decrypt the resulting ciphertext back to plaintext. As shown in Fig 3, given a plaintext message, one key is used to encrypt to ciphertext and the other key is used to recover the plaintext. At the time of key generation, the two keys are interchangeable. One is selected to be the public key and the other to be the private key. The public key is published so that it can be known to anyone. The private key is kept secret in a secure manner. It must be very difficult to discover the private key from the public key. An inherently difficult mathematical problem is chosen as the basis for the algorithm. One method of keeping a private key secure is by the use of smartcards. Smartcards contain not only a private key, but also have a computer that can be used to perform all necessary computations that involve the private key. Therefore, the private key never leaves the card and remains secure.

The weakness of the symmetric key system, key distribution, is not a problem in the public key system. Here, one wants to publish the public key in such a way that those parties wishing to communicate securely will be guaranteed to have the correct public key and not the public key of some other party. One way of accomplishing this is by the use of certificates (see section on certificates and timestamps). Additionally, the number of keys (or in this case public/private key pairs) that must be generated is one per server and not one per independent connection. For the case of 10 users, there will be only 10 key pairs. The major weak-

Fig 3. Public key encryption.

Fig 4. A digital signature.

ness of the public key system is the relative slowness of the method when implemented in computer software or hardware. In comparison with symmetric key systems, public key systems are between 10 and 100 times slower.

Digital Signatures for Immutability and Accountability

One use of public key encryption is in creating *digital signatures*. Signatures found on physical documents have certain properties that must be carried over to digital signatures. The two primary properties that physical signatures have are *immutability* and *accountability*. These two properties can be further elaborated:

- Authenticity
- That the signature cannot be forged
- Non-reusability
- That the signed document cannot be altered without detection
- The the signature cannot be repudiated

To assist in ensuring the properties of non-reusability and that the signed document cannot be altered, the concept of a *hash* of a document is introduced. A straightforward analogy is that a hash of an electronic document is similar to a human fingerprint. A hash uses a mathematical function that has the following three properties:

1. It is impossible to take the hash value and recover the document
2. It is nearly impossible to find a second document that hashes to the same value
3. Changing one bit or character of the docu-

ment will change on average 50% of the bits of the hash value

Referring to Fig 4A, the process of creating a digital signature is as follows:

- Compute the hash value of the document
- Encrypt the hash value with the private key of the person signing the document

If both the hash and public key encryption methods used are secure then all of the objectives of a digital signature mentioned previously will hold.

Referring to Fig 4B, the process of verifying a digital signature is also straightforward, given that the individual has what he or she believes to be an exact copy of the original electronic document, knowledge of the hash method used, the digital signature, and the public key of the person who digitally signed the document:

- Compute the hash of the document
- Decrypt the signature
- Compare the computed hash with the decrypted signature

If there is an exact match, then it is proven that both the signature is verified and the copy of the document is identical to the original.

Certificates and Timestamps for authentication and traceability

When paper documents are signed for legal purposes a notary countersigns the document to guarantee that the signatures are valid. A *certificate* is a plaintext document that contains information that is signed digitally by a trusted third party, such as a notary. Normally, the information contained in a certificate must be verified unaltered before use. To make it possible for the client to verify the certificate, a standard set of information is included in the certificate. This set includes the name of the company that signed the certificate, method of hashing, method of encryption, and dates of validity of the certificate. The information put in a certificate is the public key of a server. The client connecting to the server wants to verify that the server responding is the correct one and not some other party trying to mimic the server and gain secret information from the client. Thus, the client needs to authenticate the server.

In the authentication protocol, there is a slight chicken-and-egg problem: The client must have the public key of the trusted third party that signed the certificate. In the case of World Wide Web (WWW) browsers, this is done by building into the software

the public keys of major companies selling certificates. The authentication is performed as follows:

- The client requests the certificate of the server from the server of interest
- The software looks up the public key of the certifying company named in the certificate
- The client verifies the signature of the certificate

A *timestamp* is a certificate that contains the time when a specific event occurred. This can be used in combination with a digital signature to specify when a document was signed. Specifically, once a document is signed digitally, the signature is timestamped. To verify a timestamp, one must go through the same process as verification of a certificate as a timestamp is a particular kind of certificate. A record of all timestamps issued by a particular trusted third party is kept to prove, if necessary, that the issuers integrity has not been compromised.

COMPLETE SYSTEMS

A complete system starts with authenticating a user, a server, and that user's access privileges on that server. Authentication is best done with smartcards, but is more often done via a password. Some of the common systems already in use are Pretty Good Privacy⁴ (PGP) for E-mail and Secure Sockets Layer⁵ (SSL) for use over the WWW. Both of these packages use combinations of public and symmetric key cryptography.

Whenever a cryptosystem is discussed, the issue of security under various forms of attack are mentioned. The security of an algorithm is defined by the length of time that it takes for an attacker to decrypt the ciphertext without knowledge of the key. The methods an attacker can use to decrypt a message are varied.

For the most secure methods of symmetric key encryption, the best known method of attack is by brute force. A brute force attack will succeed when the attacker has one block of ciphertext in which the corresponding plaintext is already known. This is a trivial requirement as most messages have a known header, for example word processing files, e-mail messages, and so on. The attacker then decrypts this block of ciphertext with all possible keys until the known plaintext appears. As of November 1995, if the key was 40 bits or fewer,

then a solution could on average be found in 2 seconds using \$100,000 of custom hardware.⁶ If a key length of 64 bits is used the average time to a solution is 37 days using \$1 million of custom hardware. For systems that must be absolutely secure, a key of 128 bits can be used, which would require 10^{11} years for a solution using \$10 trillion of custom hardware. For comparison purposes, note that the national debt of the United States is \$5 trillion, and that the estimated age of the universe is 10^{11} years. A secure algorithm with a 128-bit key can be considered absolutely secure for all purposes unless a method more efficient than brute force can be found and applied.

Knowledge of the mathematics, algorithms, and protocols for secure systems is not enough. On June 19, 1996, the *New York Times*⁷ published an article on the failure of a system thought to be secure. Mitsubishi Corporation (Tokyo, Japan) and Sumitomo Corporation (Tokyo, Japan) had formed subsidiaries to produce digital cash cards for a popular form of gambling in Japan called *pachinko*. The goal was to use an electronic cash system to ensure that taxes would be paid by this lucrative business. The losses due to flaws in the system totaled more than \$600 million. Clearly, the design and implementation of secure systems is a subtle art. No one should implement a secure system without the oversight of a competent person skilled in the art of cryptography.

STANDARDS AND THE LAW

The US government currently sponsors a number of initiatives to study and recommend appropriate policies for cryptography in general⁸ and for health care in specific. A report is due early 1997 from US Department of Health and Human Services (DHHS) Computer Sciences and Telecommunications Board (CSTB) of the National Research Council. The latter initiative has resulted in a comprehensive bibliography of publications that relate to the confidentiality of electronic health data.⁹ For an overview of the politics of cryptography in general see chapter 25 in the Schneier.¹⁰

Much of the current discussion of cryptography in medical records has been spurred by the US enactment of the Medical Records Confidentiality Act of 1995 (S1360). This law details the required mechanisms for handling health care information and the remedies for violations of this Act. It charges the US Secretary of the DHHS to establish

regulations that safeguard medical record confidentiality. Such regulations are expected to be derived from the findings of the CSTB.

The medical field also is standardizing its efforts. At the 1996 annual meeting of the Radiological Society of North America, there was a joint meeting of the security committees of Digital Imaging and Communications in Medicine (DICOM), Comité Européen de Normalization (CEN), and Japan Industries Association of Radiation Apparatus (JIRA). There was general agreement that only one security standard should be formed for all medical purposes. Initial proposals involve the use of the SSL protocol for the protection of privacy and public key-based digital signatures.

In practical terms, the application of cryptographic algorithms to medical records are subject to the laws and regulations in the country of use. The export of cryptographic algorithms likewise is regulated heavily in most countries. In the United States, the government can consider cryptography a munition and it is listed on the US Munitions List. An unofficial nontreaty international organization, Coordinating Committee for Multilateral Export Controls (CoCOM), was formed by NATO to coordinate national restrictions on various controlled technologies including cryptography. The regulations and restrictions go beyond the actual algorithms and include information required for the design, development, production, or repair of defense articles.¹¹

In summary, the lawmaking and regulatory agencies of most governments have not kept pace with the diffusion of information technology and the need for secure communication in commercial enterprise. Governments are wrestling with the issues surrounding cryptographic policy, and medicine is one of many commercial applications that seeks clarity. Health care information system providers therefore must work with a complex array of regulations on the development, sale, and export of cryptographic methods.

CONCLUSION

In this article we briefly explored some of the many facets of security with respect to medical information. Security, although a broad and complex field, cannot be ignored as legislation and regulations enforce its use. Also, the use of digital information in medicine continues to increase.

Many tested algorithms, protocols, and tools exist with which to build secure systems, but their use should be by people well trained in the art of cryptography. The potential loss from a failed

security implementation is high. The text by Schneier⁵ is an excellent book on security, and provides a good starting place to learn more about cryptography.

REFERENCES

1. Lafrance S, Krok S, Moore R, et al: Security vs. Access: A New Health Care Dilemma. Proceedings of the 1996 Annual HIMSS Conference 1:1–9, 1996
2. Wong S: A cryptologic based trust center for medical images. *JAMIA* 3:410–421, 1996
3. Cimino JJ, Socratous SA, Clayton PD: Internet as clinical information system: Application development using the World Wide Web. *JAMIA* 2(5) 1995
4. Zimmermann PR: *The Official PGP User's Guide*. Boston, MA, MIT Press, 1995
5. SSL 3.0 specification: Netscape, Mt. View, CA, <http://www.jp.netscape.com/eng/ssl3/>, March 1996
6. Schneier B: *Applied Cryptography*. (2nd ed). New York, NY, John Wiley & Sons, 1996, p 153
7. Pollack A: Counterfeiters of a new stripe give Japan one more worry: Fake cards thwart efforts to end pinball scams. *New York Times* 1996 June 20:1(col 2)
8. Dam K, Lin H: *Cryptography's Role in Securing the Information Society* (pre-publication copy). Washington, DC, National Academy Press, 1996, <http://www2.nas.edu/cstbweb/28e2.html>
9. Auston I: *Confidentiality of Electronic Health Data: Methods for Protecting Personally Identifiable Information* (bibliography). National Library of Medicine, US Department of Health and Human Services, (<http://www2.nas.edu/cstbweb/28e2.html>)
10. Schneier B: *Applied Cryptography*. (2nd ed). New York, NY, John Wiley & Sons, 1996, pp 597–618
11. Department of State: *International Traffic in Arms Regulations (ITAR)*, 22 CFR 120–130, Office of Munitions Control, 1989