IDENTIFICATION AND EVALUATION OF
THE SECURITY REQUIREMENTS IN
MEDICAL APPLICATIONS

Deborah L. Hamilton
Hewlett-Packard Laboratories
Palo Alto, California 94304

Abstract

Computerized medical systems are emerging to help health care professionals cope with
the difficult problems of patient data explosion and increasingly complex diagnostic in-
formation. The security of these medical information systems is extremely important
- one catastrophe could hamper their chance of success. The state-of-the-art security
mechanisms can not appropriately address the needs of these systems without interfer-
ing with the system's effectiveness and current research efforts are not aimed at the
unique needs of the medical industry. This paper summarizes the security aspects of
today's medical information systems and evaluates the software security requirements
necessary for the computerized systems of tomorrow. The second part of this paper
discusses how these concerns are addressed by today's technology.

Objectives

The objective of this paper is twofold. The first objective is to initiate discussions on the security
concerns of medical information systems. The second is to emphasize the importance of security
to the medical community and to discuss the security gaps in today's technology.

Introduction

Current and future health care systems require large amounts of information to be collected, stored,
processed and managed. A computerized system can speed processing and reduce paperwork
creating more time for health care workers to spend with patients. They can provide an easier
method for health care members to share information with specialists, compare patient data with
diagnostic information, link patient data with family health history, and access the most recent
research information. The government and some major insurance companies have already proposed
a national database for patient health data to improve health care and cut costs. The secretary
of health and human services has suggested that patients carry a "smart card" which will allow
centralized database access and insurance billing. Computerized medical systems are emerging and
have a promising future, however, progress could be hampered or killed due to lawsuits and legal
regulations if the systems provide inadequate security. Legal regulations will probably become
more stringent due to the general public's increasing sensitivity to the disclosure of information.
In spite of the importance, little research effort is directed towards the area of medical system's
security or even general commercial application security.
As computerized medical systems become more sophisticated and systems allow wider access of information and increased ability to share data, the need for security will increase. Security breaches of computerized systems will be more tempting and more devastating than in today’s system due to the perceived anonymity, and the perceived ease of access to massive amounts of patient information. The complications increase when considering the implications of networks.

Security in medical applications is necessary for three main reasons: to protect the integrity and confidentiality of health care data; to ensure availability of resources; and to provide accountability records for malpractice cases. Incorrect patient data could lead to incorrect decisions and bad medical care. Leakage of highly subjective or very sensitive data such as a patient’s HIV status, for example, could prevent someone from getting insurance or employment. This problem will only get worse as more information becomes available. For example, physicians may soon use chromosome analysis to determine whether a patient is highly susceptible to alcoholism, colon cancer, Alzheimer’s or diabetes. This information can be very useful in the right hands but can be very dangerous in the wrong hands.

Background

This paper is based on information from a variety of sources such as interviews with several nurses, doctors and other staff in hospitals and clinics; documents on the legal regulations of patient data; government studies [3]; research in academic institutions [10]; and industry [8, 7].

Scope

The number of security issues associated with security for medical applications is vast. The scope of this paper is limited to application level concerns such as data integrity, accountability, confidentiality, authentication, auditing, and access control. Some very important issues are not discussed here but the intent is not to deemphasize them. These issues include fault tolerance, recovery mechanisms, secure operating systems, secure networking, secure databases, security policies, politics, reluctance to using or trusting computers, password generation, training, ease of use, system maintenance and administration, viruses, worms, secure backups, secure data storage, secure hardware, human entry mistakes and quality assurance.

Premises

Current regulations on patient records and medical applications are conflicting and ambiguous. Different states have conflicting regulations making it impossible to develop systems that conform to all regulations. Furthermore, there are laws in some states that prohibit the use of computers for many tasks. For example, one state requires that patient records be handwritten and another requires that orders for medications be handwritten in ink [3]. We must assume that these regulations will change when it is shown that computer applications and systems are able to provide the security and integrity necessary. The laws mandating hand-written records are not discussed in this paper. Instead, the actual reasons behind these restrictions are addressed.

Security Concerns

There are many complex security constraints for a computerized medical system most of which stress the current technology and present interesting and challenging problems for those working in this field. There are a variety of types of medical applications - this paper focuses on applications which require wide access such as medical information systems since these applications have the most challenging security requirements. However, many of the same concerns apply to other types of medical applications as well.
Current regulations dictate that medical records be accurate, accessible, authenticated, organized, confidential, secure, current, legible, and complete [4]. Each county, state and possibly hospital has unique regulations and policies so security mechanisms must be easily and dynamically configurable. The security concerns associated with meeting these requirements are discussed below.

**Court Admissibility**

Medical records must be admissible in court should a lawsuit arise. This means records must be up-to-date and contain the name, time and date of any changes or additions to the records. Deletions must be logged as well. The records must remain easy to modify and the most up-to-date information should be easily identifiable. Properly used paper records provide some sort of a logging mechanism to record changes. It is not as easy to provide a mechanism to keep track of modifications to patient information in computerized systems. A logging mechanism should audit who entered the information and where and how the data originated if it was electronically transferred. For example, if test results are transferred directly to a patient's record, the instrument on which the test occurred should be noted. If the instrument is found defective, this information can then be tracked and invalidated. If information is transferred in from another medical center, that should be noted to allow tracking down the source. The information or source be deemed questionable later.

**Accurate And Authenticated Information**

Data integrity is of the utmost importance in a medical system. One mistake, intentional or unintentional, could prevent someone from having the proper information in a life-threatening situation. This will become more important as tasks are computerized since humans become more removed from the collection, processing and management of data making it less likely that mistakes will be caught and corrected before damage is done.

Data integrity is very important, however, the trade off on performance should be considered carefully. Different applications require integrity to varying degrees. Insuring data integrity requires CPU time and a slow system will deter and hinder users. Thus the level of integrity should be configurable to the applications.

In today's systems, the physician's written signature is an effective method of verifying that they have entered information, ordered tests or agreed to information others have entered. Even if notes are dictated and entered by a staff member on a physician's behalf, a written signature can verify that the physician has read and agreed with the information. Signatures offer a mechanism for proving authenticity, indicating responsibility, and showing permission and understanding (e.g., permission by the physician to dispense medicine or to authorize a procedure, permission by the patient to allow a procedure). In order for a medical system involving signatures to be computerized, a mechanism must be available to provide identical functionality and with the same ease as written signatures. This mechanism must be reliable and verifiable; otherwise regulations will prohibit their use like some states currently do with signature stamps.

A secure authentication system is very important since it provides the basis for other security functionality such as confidentiality and data integrity. Currently, authentication is often done by visual recognition (i.e., looking at a person's badge, visually comparing signatures or sometimes just looking for a white coat). A computerized system will not have the benefit of this type of visual recognition any time in the near future.

Depending on the application, medical systems may need a mechanism to ensure that requests are submitted once and only once. For example, the following abuses may need to be defeated: a patient copying an order for a prescription and resending it at a later date to obtain refills without authorization; a pharmacist copying prescriptions to resubmit multiple times to make records account for missing drugs.
Confidentiality And Accessibility

There are many reasons to require confidentiality for patient data and health care information. Some information is especially important to secure, for example, HIV-antibody test results, records of drug and alcohol abuse, psychiatric records, and records of celebrity patients. In addition, private information may be given in confidence to the physician in order to aid patient care such as sexual preference or abortion history. In addition, protecting access to resources such as instruments and CPUs is very important.

Accessibility, however, is also very important. Information and computer resources must be available to those that need them, when they need them. Unfortunately, who needs them and when can not always be determined ahead of time - this is especially true in emergency situations. Current mechanisms of ensuring confidentiality and accessibility in the medical field rely upon physical control over paper records and access to computer systems. The method of controlling access must become much more sophisticated before information and resources become widely accessible across systems. To provide the proper amount of both confidentiality and accessibility in a computerized system is a challenging problem.

Access must be carefully controlled and monitored to prevent abuses and it must be restricted as much as possible but yet flexible. Authorized personnel should never be refused access and should not have a difficult time obtaining access. There should be a mechanism of allowing some users access from only certain locations while allowing others to use any location. A receptionist, for example, only needs access from the reception desk while a physician should be able to log on from any location especially in the event of an emergency.

When one gives permission today for someone to access their health record, it typically allows access to all of the data. For example, one usually gives complete right of inspection to our insurance carrier when they insure us. However, there are several things that provide a small amount of protection in current systems.

First, sensitive records are often physically separated from more commonly accessed information. Various pieces of information are stored in different forms and different locations (ie. billing and accounting information might be stored separate from patient data). Various departments will often store some information locally such as information that is sensitive or relevant to current treatments. Records are stored locally either because the records are sensitive or because they can take a long time to retrieve from the main storage and are often misplaced. For example, many of the very sensitive records containing information on drug abuse or psychiatric care are stored separately and out of reach from the insurance companies or employers. If this kind of information is stored on a computer system, access is quick and all patient data can be linked together, however, physical location no longer provides a barrier to access.

A second example of how the current system provides some protection involves human intervention. When patient information is passed on for research, comparison, or consultation, a human must intervene to pass the information on. This person can act as a filter and forward only the information that is relevant and required thus providing an informal control of access. This person can also detect any requests needing additional checking because they are unusual or relate to sensitive information. For example, if someone requests information on a celebrity patient, access will be granted more cautiously than usual. If information is shared electronically with insurance agencies and billing groups for example, access will have to be carefully monitored and intelligently controlled at a much finer level than it is now. The challenge will be to allow wide access and electronic sharing of some information while still tightly regulating other information.

Many health care workers must be able to access and enter information into a patient’s records. A computerized system that did not allow the same access as currently available would be a hindrance. One could simply open up all records to all health care members, however unlike humans, a
computerized system is not able to determine when abuses are occurring using intelligence and visual cues. Access must be closely controlled and/or securely and reliably audited.

If access is allowed based on the patient record level, auditing should record who accessed what pieces of information and what changes were made in order to abide by regulations. This auditing information must be collected and intelligently analyzed in order to detect abuses and mistakes. However, attempting to securely monitor and analyze all actions on a patient record is difficult and time consuming.

A second alternative is to control access based on smaller and more independent pieces of information. This method creates a more complicated access control system for two reasons: job duties vary greatly with health care providers and individuals, and there is no simple method of modeling who needs access to what pieces of information (ie. there is significant overlap in the access, modification and confidentiality requirements between users). For example, the clerical staff may need access to the patient's address but should not be able to change the patient's health history. Technicians need information on tests to be performed on a patient and should be able to enter the results into the patient's record but should not be able to modify the patient diagnosis or physician's notes. Computer administrators need to have complete power over the computer's functions in order to properly administer the system but should not be able to access patient information. Researchers should be able to gather clinical information for studies but not be able to access the patient's names or modify their medical records. Social workers should be able to flag patients who may be suicidal or physically abused but not access nor modify other patient information.

It would be very cumbersome if one could not assign rights to a group of people based on the role they play on the health care team. To allow easier granting of access rights, one should be able to grant and modify rights by title (eg. physician, security officer), relationship to patient (eg. primary care taker), area of specialization (eg. intensive care), patient status (eg. inpatient, under-treatment) or just by the individual.

In addition to the relationships discussed above, there should be a special method for a physician or nurse to obtain access to any information in the event of an emergency without spending time looking for someone who can grant them permission. However, these emergency override situations would need to be monitored carefully to prevent abuse.

The scope of access for patient information is variable. Certain information should be available on a fairly large scale (e.g. information on what precautions should be used in handling bodily fluids of particular patients). Other information should only be available to a select group of the primary care providers and possibly others in emergency situations (e.g. a patient's history of abortions or suicide attempts).

Deletion, replication and queries must be tightly controlled. Regulations prohibit deletion of some patient information, however, there should be a mechanism to remove this information from view. Reproductions of records must be trustworthy. This means that creating, accessing and storing records must be tightly controlled. Duplicated information should bear the same access rights as the original information to prevent intentional and unintentional abuses of confidentiality. It is also critical that massive copying, searching and modifying of patient records be very tightly controlled.

In today's systems, there is usually a person in charge of patient-record storage who keeps track of what records are checked out and by whom. This information is used for both tracking down lost records and for keeping track of who has had access to patient data. When patient data can be stored and transferred electronically this auditing capability will have to be duplicated. In addition, information must be stored in order to track down inaccurate data. For example, if a lab test result is entered incorrectly and later corrected, there should be a mechanism to determine where the incorrect data was used and who must be notified of the correction. Otherwise, future treatment
may be based on incorrect information.

**Accessibility From Outside Connections**

Medical care is improved when medical information can conveniently be shared outside of the department, hospital or clinic. Physicians are able to consult with specialists and share patient data. Research groups benefit greatly from anonymous patient information. Physicians need access to networks for on-line databases with medical information and news groups to keep in touch with the many new medical developments. Time and energy can be saved if records are shared electronically among medical groups, insurance agencies and billing agencies. Physicians can benefit from remote access to medical information. One medical application's development team noted that physicians welcomed their computer application especially since they could now access information from home [9]. Security, however, was not mentioned. Remote access of medical systems provides great benefits but also significantly increases the complexity of securing the system. Not only must one know which people to trust but it must also be able to determine which machines it can trust.

**Data Storage**

Patient data storage is regulated by state and federal agencies. Regulations stipulate that various portions of the medical records must be kept from 7 to 75 years depending on the information and state. Some states require that medical records be retained in the hospital so they are always accessible. This means that administration of a computer system handling patient data cannot be done off-site by a third party - administration must be simple enough for the on-site personnel to handle.

**Comparison With Current Technology**

Many of the security requirements discussed in the previous section are either not possible with today's technology or exist with limitations. This section discusses important gaps and limitations that should be taken into consideration when designing systems. The prevailing attitude is to delete functionality in order to provide a secure system. It would be unfortunate, however, to create a secure system by limiting functionality which would have helped to lower costs or improve the quality of health care.

A high percentage of the current work in security is funded by the government and is geared towards the Department of Defense (DOD) work, an industry with security concerns and priorities very different from that of the medical industry. One of the major differences in the DOD sector is the emphasis of confidentiality over all else. Medical applications require confidentiality but not at the expense of obtaining access during emergency situations. In addition, the need to keep records which are admissible in court and adhere to regulations is not of concern to the DOD work.

**Areas That Present Obstacles**

Sharing resources and information efficiently requires open and/or distributed systems. The underlying components for a secure open or distributed system are not well developed. In addition, there are no good mechanisms to allow authentication of users, applications and systems over the network. The current mechanism requires preselected passwords shared between every two parties that may need to trust each other. This creates key storage, management and distribution problems.

One major requirement of a medical system is a very secure auditing mechanism. Technology has not progressed much on this front especially when considering distributed systems. Detecting
abuses on distributed systems requires collaboration between the systems. For example, a physician accessing data over the network may not create concern, however, that information tied to a user switching user IDs and accessing many different patient records through various physician’s names should create a warning. The systems must have a method of trusting each other to some degree and they must be able to share data so that it can be correlated and interpreted to determine when abuses occur. In addition, auditing mechanisms need to be able to tell when humans are able to infer information they should not have. For example, if the results of some tests are marked confidential only when particular results are found, it is not difficult to infer what the results indicate. Technology has not produced sufficiently smart auditing systems that are able to collect information as well as analyze that data effectively and intelligently in order to prevent abuses and minimize inferencing. The solution today is to have humans analyze the audit logs, however, this is tedious and error-prone.

There should be a standard method of evaluating software systems to ensure they meet the necessary security requirements. There are currently two standards available. One evaluation process is controlled by the U.S. government and is very complicated and time consuming. The other is a European standard which is not fully developed or tested. Furthermore, these standards do not address the needs of the medical community. They were developed mostly with military systems in mind. They emphasize confidentiality over all else. For example, these standards require that all information access be prohibited if a failure occurs in the auditing mechanism. This is clearly unacceptable in the medical industry. In addition, these standards do not address the security needs of open distributed information systems and are not integrated with cryptographic mechanisms to provide data integrity and signature mechanisms. The government and commercial industries are attempting to address these issues; however, it will take a while.

Current systems require that you determine ahead of time who should have access to information or resources. If someone requires emergency access, they must find an authorized user. This would encourage administrators to grant general access and keep sensitive data and resources off of the system. A medical system would benefit from a system that allowed emergency access in a carefully monitored mode to prevent abuse. There would have to be some motivation not to stay in this mode longer than necessary thus creating massive audit logs and weakening the security of the system. A system like this is not yet available.

Areas That Present Some Challenges

Many security functions depend upon the authentication mechanism. Therefore it is extremely important that this mechanism be very secure and robust. Passwords and smart cards are the major technology available today. Passwords are usually either easy to figure out or difficult for users to remember forcing them to write them down. Smart cards provide better security but create problems if they are lost or stolen. Biometric authentication mechanisms are better suited for the medical community, however, they are expensive and will sometimes deny access to authorized users. There is much research occurring in biometric mechanisms because many industries would benefit from such a system, however, there are not currently any inexpensive yet very secure mechanisms suitable for the medical industry.

It would be handy if there were a system that required permission from two parties before a major modification was granted or sensitive information accessed. This would make it more difficult to abuse the system. There are very crude and awkward forms of this present today but no elegant mechanisms.

Current systems are not dynamically configurable in the manner needed for the medical industry. Applications should be able to determine what kind of tradeoff should be made between security and performance. Access control should be dynamic since staffing situations are constantly changing. Work is progressing slowly in these areas.
There is currently a scheme that allows only one person to write something but every one to read it. This can be used for creating a signature mechanism. There is a fair amount of work going on in this area, however, the current schemes need to be evaluated with court admissibility in mind.

The access control needed for medical information systems is difficult to model with the current access control technology. The administration of control and power of the DOD applications can be structured in an hierarchical fashion (eg. the person at the top should have access to everything and control over all tasks). However, medical systems should not be modeled hierarchically. The group that has control over the system administration should not have control over the records and vice versa. Furthermore, if there is a person with complete control over all functionality, records from the system could not be admissible in court since one can not be sure whether a physician's signature is authentic and untouched. There must be a method of proving that only one person could have created the signature.

Current security systems were not created with the idea of one person entering information on another person's behalf or for one person to delegate a task to another (eg. a nurse or clerical worker often enters notes on behalf of the physician). In addition, there isn't a good mechanism available which allows a patient to give permission to access their record to the health care providers without allowing the patient to have access themselves. This is a requirement somewhat unique to the medical community and is not receiving much attention from the security field.

Areas With Limitations

Encryption is an area where much research effort is concentrated because many industries view it as a high priority. However, the restrictions that are currently placed by the government on exporting the most widely used encryption mechanism may hinder vendors who are developing systems for use outside the U.S. Performance of the current encryption mechanisms could also present a limitation if large amounts of data are sent across networks.

Auto-logout is important since health care members are frequently interrupted and not always thinking about logging out once they give up physical control of the terminal especially in emergency situations. Without auto-logout, it would be easy for users to intentionally or unintentionally share sessions thus weakening the authentication of the system. It is especially important that login be quick and easy or users will find a way to intercept the auto-logout process. One current solution to this problem involves the users wearing badges which emit a unique signal. When the user strays a certain distance from the terminal, they can be automatically logged out. However, there are ethical questions of enabling a mechanism which can constantly monitor the location of individuals.

Summary And Conclusions

A medical information system must have a reliable mechanism for verifying who has entered, agreed to, or ordered what. Data integrity must be guaranteed. There must be a reliable authentication mechanism. Information from the medical system must stand up in court should a lawsuit arise. Many parts of the medical team must be able to enter information into the patient record and various members need different levels of access. Access should be restricted as much as possible but patient data should always be accessible in an emergency situation. Access should be configurable based on any of the following: person, job, relationship to patient, area of specialization, or patient status. Physicians should be able to consult with specialists, share patient data for research and compare symptoms with on-line databases without infringing on the rights of the patients. There must be a means to correct data as well as track down the propagation of the inaccuracies before it results in incorrect actions. Information should never be deleted, only removed from view. There should be a mechanism available to ensure that a request is submitted once and only once.
Designers of medical applications need to be aware of the lack of security and need to be careful to secure systems before damage is done. The current technology in security is primitive and research efforts are not addressing all of the needs of the medical community. Precautions are especially important if medical information systems run on distributed systems or are accessible remotely.

References


