A SECURE ONLINE MEDICAL INFORMATION SYSTEM IN DISTRIBUTED AND HETEROGENEOUS COMPUTING ENVIRONMENT

Muhammad Nabeel TAHIR

Abstract: The objective of this article is to analyze the importance and the role of Information Security in online medical information systems. Healthcare organizations have to protect private information pertaining to the individuals they serve. As more and more healthcare organizations implement computer-based ERPs, telemedicine, EDI, data warehouses and other network-based information systems, information security in healthcare gains importance more than ever before. Possible questions and issues related to information security requirements might be: "How do the healthcare professionals protect the information in their EPR systems?", "How can network data exchange and transfer over the Internet be accomplished without being tampered by hackers and other unauthorized individuals or groups?" To answer these questions, players in the healthcare chain (providers, physicians) are turning to computerized solutions. As one might recall, turning to computerized medical record systems was the solution for healthcare organizations some years ago. Now we are dealing with the problems that those computerized systems may bring.

Keywords: Medical Information Systems, Information Security, Distributed Computing.

Background

Information technology has become increasingly important in improving the quality and in lowering the costs in healthcare. Attempts to protect patient's privacy have to centre, therefore, on finding ways to protect the sensitive electronic healthcare information in a computerized environment rather than on opposing to the use of information technology in healthcare organizations.

As time progresses, ensuring information security in medical institutions becomes a burden for the Chief Information Officers (CIO) and other healthcare professionals. The technology evolves rapidly and keeping up with the technology is a tough task. For this and other not so important reasons priorities seem to be fluctuating. Health-

care information security professionals face a variety of issues at the forefront of information systems planning; however, it is a must for organizational success.

Problem Definition: Research Problems and Research Questions

Recent research has identified an increase in the awareness of the need of location-based services to support the application of secure E-cure.

Implementing security plans and technologies to protect electronic medical records systems is the paramount health data security issue today. This implication is backed up by the report of the National Research Council in 1997 entitled "Protecting Electronic Health Information." The conclusion of the report consists of seven items, which can be summarized as follows: healthcare organizations need to take a more aggressive approach to improving the security of health information systems to better protect electronic health information.

Healthcare organizations have been slow in adopting strong security practices, largely due to a lack of strong management and organizational incentives. No major breach of security has occurred that has catalyzed such efforts. Thus, the information technology vendor community has not found a market for providing security features in health information systems.

Patients have important roles to play in addressing privacy and security concerns. The greatest concerns regarding the privacy of health information derive from widespread sharing of patient information throughout healthcare industry and the inadequate federal and state regulatory framework for systematic protection of health information.

At the level of individual organizations, electronic health information is vulnerable to both authorized users who misuse their privileges to perform unauthorized actions (such as browsing through patient records) and outsiders who are not authorized to use the information systems, but break in with the intent of malicious and damaging action.

Adequate protection of healthcare information depends on both technology and organizational practices for privacy and security.

For IT professionals, the first real issue regarding integrity and security of electronic information came when the shift from mainframe to the client-server computing took place. In the mainframe model, no information was "leaking" to the outside world, the systems were of the single closed systems type. With the emergence of client-server architectures, distributed computing, heterogeneous computing environment and mostly with that of networking, information integrity and security became a serious concern as their use is not limited to desktop PCs but also to wireless technologies like mobiles, PDA's, laptops, etc.

In distributed computing systems (e.g. client-server systems or today's multi-tier systems) data is stored on many computers across an enterprise and even outside of the enterprise. The results of data being stored in and transmitted to numerous places (e.g. laptop, PDA, mobile phones) are massive and information system professionals recognized that data security would be an issue that had to be addressed with new solutions and new technologies.

When in the late 1980s the PC revolution took place and inevitably networking came on the scene, today's data security concerns started to appear. Before that, many healthcare information systems vendors and pioneering healthcare providers were installing IT products with the motto "Make it work first, then think about the security." But with the changes in the computer world and the health data security issues, securing systems is becoming a priority. Contrary to popular belief, security does not simply involve protecting the confidentiality of information. There are three basic elements of data security, all of which should be considered. These are *confidentiality*, *integrity* and *availability*.

Data confidentiality is most commonly associated with security and is easy to understand. Healthcare organizations must protect all confidential data so that it does not get disclosed either accidentally or maliciously. There have been several instances when health information about a patient has been leaked. Such disclosure, whether of a celebrity's health data or a private citizen's health data, can ruin a person's career, insurability or even his life. Thus, using technology and policies to protect the confidentiality of electronic health care information is a must.

Data integrity is not always associated with security, particularly in the eyes of the general public. Protecting data integrity means ensuring stored information is correct and not in any way corrupted. In the late I980s, a hacker group in Milwaukee known as The 414 Gang broke into several organizations, including Memorial Sloan-Kettering Cancer Centre in New York. They got into the provider's computer systems and were fooling around, doing nothing really malicious though. But this example clearly shows how data integrity is a crucial part of data security efforts. And in healthcare, if you corrupt patient records, that could cause a lot of problems, perhaps even the death of a patient.

The third and last major aspect of data security is data and system *availability*. Computer systems and electronic data must be available to users whenever they need it.

One of the factors that have slowed progress toward greater health data security is a lack of understanding of all three primary aspects of the security issue. There long has been an understanding that the only thing security precautions are supposed to do is to protect data confidentiality. While that is the truth, it is not the whole truth.

The idea of, "Make it work first, then secure it," is a step towards organizational suicide. Experts agree on the point that it is a huge mistake to install security after the fact. Some observers say that healthcare professionals are beginning to think about security first. These experts say that security is starting to be viewed as an enabling technology rather than as an inhibiting addition.

People have never really thought about these other aspects of security because they want to believe in the common good. They think there are not companies out there tracking your every movement and sending you catalogue for components when they have found out that you have broken your leg. People do not want to believe this incredible networked environment exists.

The confidentiality aspect of security has been around since Hippocrates. But when it comes to aspects like integrity, a member of the public would not know the appropriate way to cross something out on a medical record. The people on the streets would not even think about things like that; the only thing they think about is the confidentiality of their medical information. They presume its integrity, which can be a fatal mistake.

In short, success of an individual, business, government agency and health organization increasingly depends on the ability to securely communicate around the world in real time. The advent of widespread connectivity via the Internet and an array of ubiquitous and powerful mobile devices have changed the face of computing and communications. With the vast benefits of increased connectivity, however, a multitude of new risks has emerged, risks on a scale which few in the industry have anticipated.

Conclusions

Many security professionals have worked hard to secure the patients' medical records but a lot of work is required to be done in this field to achieve a secure medical information system due to the use of wireless heterogeneous technology. The objective of the future research work in this area should be to identify the major security weaknesses in the currently available hospital/clinic management information systems built for both online and offline client-server distributed and heterogeneous computing environments. The future is for the secure information technology and the same applies to health information as well. A distributed, wireless and heterogeneous client-server medical information system is a necessity nowadays. Security is a major factor when we deal with client-server environments or distributed and heterogeneous computing and addressing these problems is a big issue.

References:

1. Ross J. Anderson, "A New Family of Authentication Protocols," <http://www.secinf.net/authentication_and_encryption/A_New_Family_of_Authentication_Protocols.html> (10 November 2004).
2. *A History of Hacking*, <http://www.sptimes.com/Hackers/history.hacking.html> (8 November 2004).
3. Haio Roeckle, Gerhard Schimpf, and Rupert Weidinger, "Process-Oriented Approach for Role-Finding to Implement Role-Based Security Administration in a Large Industrial Organization," in *Proceedings of the 5th ACM Workshop on Role-Based Access Control (RBAC'00)* (Berlin, Germany, 2000), 103-110.
4. Amit P. Sheth and James A. Larson, "Federated Database Systems for Managing Distributed, Heterogeneous, and Autonomous Databases," *ACM Computing Surveys* 22, no. 3 (September 1990): 183-236.
5. Konstantin Beznosov, "Requirements for Access Control: US Healthcare Domain," in *Proceedings of the 3rd ACM Workshop on Role-Based Access Control* (Fairfax, Virginia, USA, 22-23October 1998), 43.
6. D.J. Thomsen, Richard C. O'Brien, and C. Payne, "Napoleon: Network Application Policy Environment," in *Proceedings of the 4th ACM Workshop on Role-Based Access Control* (Fairfax, Virginia, USA, 28-29 October1999), 145-152.
7. Salem Benferhat, Rania El Baida, and Frédéric Cuppens, "A Stratification-Based Approach for Handling Conflicts in Access Control," in *Proceedings of the Eighth ACM symposium on Access Control Models and Technologies*, ACM 1-58113-681-1/03/0006 (Como, Italy, 2-3 June 2003), 189-195.
8. George W. Dinolt, Lee A. Benzinger, and Mark G. Yatabe, "Combining Components and Policies," in *Proceedings of the Computer Security Foundations Workshop VII*, ed. Joshua Guttman (Los Alamitos, CA: IEEE Computer Society Press, IEEE Computer Society, June 1994), 22-33.
9. Jonathan D. Moffett and Morris S. Sloman, "Policy Conflict Analysis in Distributed Systems Management," *Journal of Organizational Computing* 4, no. 1 (1994): 1-22.

MUHAMMAD NABEEL TAHIR works as a Lecturer in Multimedia University Melaka-Malaysia. He is pursuing his PhD from Multimedia University Malaysia and his area of interest is Object Oriented Software Analysis & Design, Information Security in Medical Information Systems. He holds a Master of Science Degree in Computer Science and teaches to Bachelors Degree in Computer Science students at Multimedia University. *Address for Correspondence:* Multimedia University, Ayer Keroh P.O. Box 75450, Melaka-Malaysia; *Phone:* 0060-126823495, 0060-6-2523422; *Fax:* 0060-6-2318840, *Email:* m_nabeeltahir@hotmail.com.