SECURING A WEB-BASED EPR
An approach to secure a centralized EPR within a hospital

Ferreira A, Correia R, Costa-Pereira A
Department of Biostatistics and Medical Informatics, Faculty of Medicine, University of Porto
Al. Prof. Hernâni Monteiro 4200-319 Porto, Portugal

Keywords: Electronic Patient Record; Information Security; Standards & Internet Technology;

Abstract: The introduction of new technologies such as the EPR stresses the importance of healthcare information security. The Biostatistics and Medical Informatics Department of Porto's Faculty of Medicine is developing a centralized Electronic Patient Record at Hospital S. João, in Portugal, the *HSJ.ICU*. The main objective is to electronically integrate heterogeneous departmental information in a secure way, using Internet technology. The methodology used takes into consideration user-driven security issues in terms of confidentiality, integrity and availability of information. This was achieved using CEN/TC251 prestandards, Internet security protocols (e.g. TLS) and digital signature protocols. Having in mind the CIA (Confidentiality, Integrity and Availability) structure helps organizing and in a way, separating concepts that can be assessed in a more direct and efficient way. Security issues are already rooted and constitute a good basis for any enhancements that will be made in the future.

1 INTRODUCTION

The Electronic Patient Record (EPR) is a fundamental information system for healthcare organizations, enabling a single point of entry and access to patient-related, administrative and research information (Shortliffe, 1999). It provides for easier and faster access to patient information. Further, it helps for the creation of a more complete and better quality record (Hassey, 2001)(Stausberg, 2003).

The introduction of new technologies such is the EPR also stresses for the importance of healthcare information security. New challenges (to face old problems) need to be dealt with new measures, and these must be evaluated for its effectiveness.

Several pressures during the development of IT solutions often imply that security is an afterthought. It is quite often overlooked so that the system can be easier to work with (Godoy, 2002). This and other factors make the integration of the EPR into medical processes within large environments, such as hospitals, very difficult (Benson, 2002).

The Biostatistics and Medical Informatics Department of Porto's Faculty of Medicine has started to develop and implement the *HSJ.ICU* project, a centralized Electronic Patient Record (EPR) at Hospital S. João, the second biggest hospital in Portugal with about 1.350 beds. The main objective is to electronically integrate heterogeneous departmental information in a secure way, using Internet technology. Many people and services, as well as a complex infrastructure, are involved in this process (Kurtz, 2003). There is the need to provide for confidentiality (avoiding unauthorized access (Salazar-Kish, 2000)), integrity (information needs to be accurate, valid and complete (Bemmel, 1997)) and availability (Bemmel, 1997) of patient's information. That is why learning from previous experiences, specifically in Portugal and in the same hospital, can be very important and rewarding whilst saving time and avoiding the most common mistakes (Ferreira, 2002). In summary, information security is fundamental for the success of the EPR.

This paper describes the methodology to assess system infrastructure, healthcare professionals' attitudes and patient's information workflow affecting information security. It also presents some results, analysis and procedures to be implemented so that this project is successful.

2 METHODS

Prior to any action, it is important to assess the infrastructure where the system *HSJ.ICU* is going to

A F., R C. and A C. (2004).
SECURING A WEB-BASED EPR - An approach to secure a centralized EPR within a hospital.
In *Proceedings of the Sixth International Conference on Enterprise Information Systems*, pages 54-59
DOI: 10.5220/0002655000540059

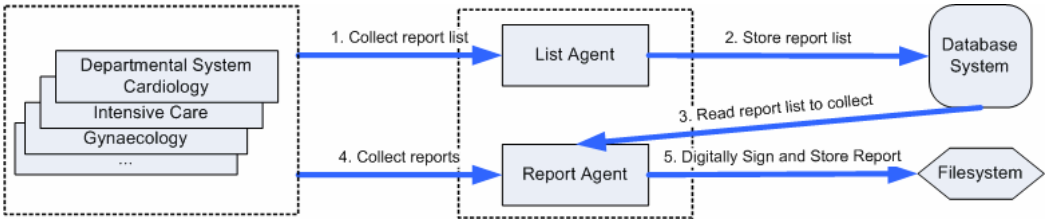

Figure 1: *HSJ.ICU* Generic Infrastructure

be integrated. Figure 1 presents a generic architecture of the EPR system to be implemented. It shows the heterogeneity of the infrastructure that supports the healthcare information flow within the hospital. The departmental systems presented above have different infrastructures and types of workflow. In some of these departments, patient records are still paper-based while others have a mixture of procedures and technology that make the integration of a common platform not straightforward.

Another important step is to assess what are the main concerns of the healthcare professionals involved. This is done with several meetings with each department's staff. Other contacts made afterwards during the development of the project are also taken into consideration.

In summary, security services will be implemented so that information security (mainly user-driven) can be effectively achieved whilst still allowing for the proper use of the system. It follows the description of the security services and problems that need to be taken into consideration whilst developing this project.

2.1 Confidentiality

In terms of user-driven security issues, confidentiality can be provided by controlling access to the system and make sure that only authorized users access information. When this rule is breached, unauthorized users' actions along with their identification should be recorded for further responsibility and subsequent legal actions.

Also, this project involves the integration of several physical places making it crucial that all communication channels are protected. This will provide for the secure information flow. Any breach that may occur (e.g. eavesdropping) should not allow for unauthorized access to sensitive information.

The following two sections will explain the methodology used for both these issues (access control and secure communications) in more detail.

2.1.1 Access Control

Controlling the access to sensitive information is fundamental; moreover when that information relates to healthcare patient sensitive information. The heterogeneous environment, such is the healthcare environment where different people and services are required to interact, make it more difficult to control and provide for its proper use. Nevertheless, there are ways to provide for proper access control.

The main step is to make sure every user can be uniquely identified so that his actions can be easily traced. Usually, every healthcare professional within the hospital has his reference number, which is unique.

In order to provide for an efficient way for identification and authentication, the development of access control tools is based on a European prestandard, ENV 12251 (CEN/TC251, 2000). This allowed for a better understanding and definition of some basic, standard rules pertaining to the use of login and password.

For this purpose, the standard protocol LDAP (IETF, 2003) was introduced. In this specific case, due to institutional policy demands, the chosen tool to provide for that protocol is the Microsoft Active Directory (MSDN, 2003). Some results from this implementation are described in section 3.

2.1.2 Secure Communications

The same issue about heterogeneity applies to this section (Figure 1). Each departmental system is positioned in a different physical location within the hospital while the database server and file system are placed somewhere else. It becomes very difficult to both protect and monitor every part that comprises the system. Internet technology is the most appropriate in this case because several platforms and processes need to be integrated (Correia, 2001). This technology is cost-effective, easy to implement and has standards that a wide number of people nowadays is used to interact with.

However, it is very hard to protect this infrastructure against eavesdropping, tampering or message forgery, when all the wiring and equipment is spread all over a big hospital. Means to prevent (or

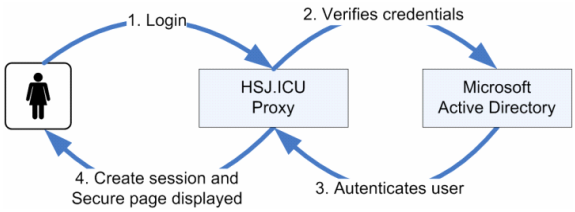

Figure 2: User Authentication to the *HSJ.ICU*

at least minimize) malicious and/or accidental actions were implemented.

2.2 Integrity

One of the main security issues that healthcare professionals specified (and is implicit) is the trust or confidence put into the information withheld by the patient's reports they need to access. The alteration or corruption of these reports needs to be avoided. The healthcare environment, probably more than any other environment, requires that information is valid, correct and complete (e.g. provide for integrity).

In order to achieve this, the reports that are automatically generated from the departmental systems (Figure 1) are all digitally signed and encrypted before being stored in the file system server. More details about how this is done and some performance tests are presented in section 3.

2.3 Availability

As was already mentioned, availability is a fundamental part of information security but often overlooked. Having user-driven security measures in mind, availability issues need to focus on means to provide for the continuous information availability for authorized users of the *HSJ.ICU*.

It is then important to provide for equipment redundancy, with the use of action-specific machines and other redundant power equipment; the recording of the most important actions and errors that may occur during system's usage (so that the system can be always updated and corrected); and finally, there is the need for backups so that information resources can easily be replaced if anything damages them.

3 RESULTS

Each departmental system can generate several reports daily (some up to 30 reports per minute). These reports are collected by the EPR *HSJ.ICU* and stored within a file system. Further information about their location, date and time, exceptions, errors and so on, are stored in a database system. This will enhance and speed their retrieval.

Most healthcare professionals' concerns assessed by the project's team relate with secure auditing for further notification and responsibility of unauthorized users' access; the integrity and reliability of the generated reports; and the provision for the confidentiality of the sensitive information involved within the whole process. These issues map very well with what the project's team assessed as user-driven security problems. Also, apart from the concerns mentioned above, there is also a main issue not to be overlooked: availability (Barrows, 1996). Some implementation tools, technologies and performance tests will be now presented.

3.1 Confidentiality

3.1.1 Access Control

Figure 2 shows how the user authenticates to the Microsoft Active Directory by presenting a login and a password (Figure 3 presents the web page where the user gives his credentials for authentication.). These credentials are verified in the Active Directory server to allow (or not) the access to the *HSJ.ICU*.

The main advantage for the use of Microsoft Active Directory (Microsoft implementation for the LDAP protocol) is the separation between access control and access to the requested information stored in the database. Using technologies dedicated to specific services that can easily integrate among each other improves performance and establishes separation of concerns. Further, the Microsoft Active Directory contains other tools that allow configuring security policies in accordance to the ones specified within the prestandard ENV 12251.

Table 1 (AD=Active Directory) shows the requirements that were implemented from the prestandard. Only two of the requirements are still being implemented. It is also important to refer that

Figure 3: Form for user authentication to the *HSJ.ICU*

all these tasks are quite transparent to the user when he tries to authenticate himself to the system.

Other issues such as maintaining the identity of active users, is achieved by creating and managing sessions with PHP (PHP, 2003). This registers a unique and temporary session for each user that logs-on allowing the control of user's activity. Also, whenever each user logs to the system, a flag in the Active Directory (e.g. isLoggedIn) is set to TRUE, and the opposite when he logs out. Information about date, time and user's identity is also recorded in the Oracle Database for future actions, if needed.

Table 1: Prestandard ENV 12251 requirements

Requirement		Tools
Unique identification & authentication (user reference number)	Y	AD
Identification and Authentication prior to all other interactions	Y	AD Oracle PHP
Associating unique identity with users (ref. no)	Y	AD
Maintaining the identity of active users (flag *isloggedin* in AD)	Y	AD PHP
Log-on message (Figure 3 – top left corner)	Y	HTML
Number of log-on trials (3 times)	Y	AD
Incorrectly performed log-on procedure	Y	AD
Display of log-on statistics	Y	AD
Password sharing	Y	AD
Password storage (one-way encryption tools)	Y	AD
Logging of passwords	N	
Password display suppression	Y	HTML
User-changeability of passwords	Y	AD
Default passwords	N/a	N/a
Initialised passwords	Y	AD
Temporary passwords	Y	AD
Password expiration (2 months)	Y	AD
Password expiration notification (before expires)	Y	AD
Password reuse	N	
Password Complexity	Y	AD

The only part of the process that breaches the access control rules explained before is when an authorized user (already logged-on to the system) wants to access some resources he is not authorized to. In a case like this (e.g. break the glass), he has the option to proceed or not whilst all his actions are properly recorded for future notification.

In summary, the access control is a security service that was thought from the beginning and simple rules were applied so that no extra effort would be asked to the user. Still, its transparency does not allow for security relaxation. There are a series of procedures that provide and support for the monitoring, notification and prevention of unauthorized access and usage of the system.

3.1.2 Secure Communications

Encryption is a security mechanism that allows for the transformation of plaintext information to a sequence of non-understandable characters.

In order to provide for the encryption of all information whilst in transit the system uses the TLS authentication protocol (IETF, 1999). This protocol is a standard and is widely used for client/server secure transactions among the most common browsers, using internet technology. It has a selection of encryption algorithms to be chosen according to the type of authentication (e.g. mutual/unilateral) required.

3.2 Integrity

The process of digitally signing, along with signature verification of the generated reports by the departmental systems can be seen in Figure 4.

A digital signature, allied to a digital timestamp (particularly helpful in enhancing the integrity of a digital signature system) is applied before the reports are stored. This means that if someone or something tries to tamper with the report, that signature will not be valid any more.

Without getting in too much detail, the technology used for this process is the GnuPG (GnuPG, 2003), an open source that is based on the PGP standard email encryption software. It uses

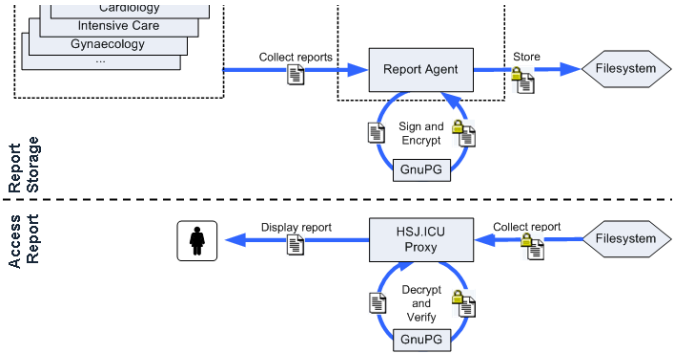

Figure 4: Report's Digital Signature and Signature Verification process

public key DSA algorithm with key size 1024 bits, impossible to break with today's technology (Silverman, 2000). Table 2 presents some performance results to both apply and verify the digital signature. It is important to mention that different technologies are used for each of these processes.

Table 2: Performance tests for a report's digital signature

Process (Mean N=5)	Without DS	With DS
Store report	5 ms	33 ms
Access report	35 ms	48 ms

According to the results presented in Table 2, the process of signing reports is generally slower than the process of verifying their digital signatures. Nevertheless, the process of signing and storing a report is only done once, while the process of accessing reports will be done numerous times. Further, the digital signature and storage of the reports is an automatic process and does not require any user interaction. It is programmed to do it at the least workload time.

In conclusion, the time difference registered between both processes (signing and verification of the digital signature) is not that relevant and does not compromise system's usability.

3.3 Availability

According to what was already mentioned about availability, Figure 5 shows the generic hardware architecture of the *HSJ.ICU*.

The extra equipment such is the load balancer, allows for the balance of the work load to the available web servers (two in this case). This will enhance the availability of resources and will provide access redundancy whilst increasing speed retrieval of users' requests.

All connections started directly or indirectly by users are registered. Information about the user, date, time and a unique session identifier are also recorded. Apart from the usual file and database log mechanisms supplied, user actions are recorded into a file (at real time), ready to be inserted in a structured way in the database system.

Other unsuccessful actions or errors generated by the system are also registered because the *HSJ.ICU* is still in the development stage and there is the need to know what the weakest points are and what problems still need to be corrected. Further, this will allow following all important steps of the system's execution and guaranteeing that it does what is supposed to do (or not).

Even more important than redundant equipment is the need for data redundancy. Regular backups are being made with database structure, data and file system stored information so that it can be easily replaced if anything corrupts or damages the original information. This will allow minimizing the unavailability time, and if possible, preventing any outage of the system.

4 DISCUSSION

The development and implementation of the *HSJ.ICU* project has been a very good learning process for everyone involved in it. Although is still work in progress, very important results were already obtained.

One important conclusion is the fact that the introduction of security from beginning as part of the systems' features and capabilities is essential. It makes the process much simpler and transparent to the normal user. Furthermore, having always in mind the CIA (Confidentiality, Integrity and Availability) structure helps organizing and in a way, separate concepts that can be assessed in a more direct and efficient way.

However, this is not enough. People (specially future users) must be involved in the whole process. Healthcare professionals have a higher sense for providing for information security and patient privacy. However, there is the need to make sure security does not interfere with their work.

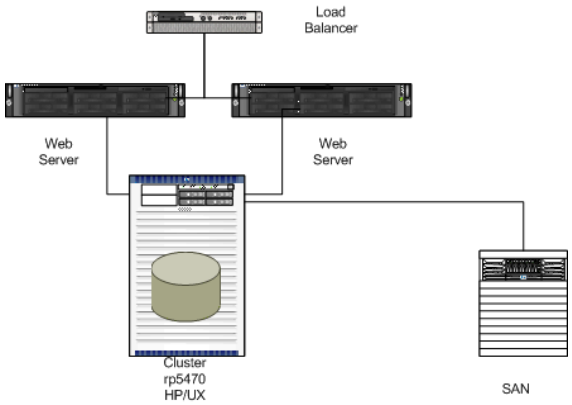

Figure 5: Generic *HSJ.ICU* hardware architecture

Another important consideration is the use of standards. This helps and speeds any project's implementation, whilst benefiting from the already thought, tested and implemented procedures.

Another relevant aspect of this project's implementation is the use of cost-effective tools, mainly web based, and the fact that it is still possible to build security that works and is usable.

Finally, this project needs to be tested and evaluated on a real environment. There is the need to analyze some more performance and usability issues that involve security. It is a project that will never be completed as management support and updates will be essential to apply. Nevertheless, security issues are already rooted and constitute a good basis for any enhancements that will be made in the future.

REFERENCES

Barrows, C., 1996. Barrows C, Clayton P. *Privacy, Confidentiality and electronic medical records*. JAMIA. 3:139-148.

Bemmel, V., 1997. *Handbook of Medical Informatics*. M. A. Musen Editors. Springer.

Benson, T., 2002. *Why general practitioners use computers and hospital doctors do not-Part2: scalability*. BMJ. 325:1090-1093.

CEN/TC251, 2000. ENV 12251: *Health Informatics - Secure user identification for health care management and security of authentication by passwords.*

Correia, R., 2001. *Acquisition, processing and storage of vital signals in an electronic patient record system*. Presented at Mednet 2001.

Ferreira, A., 2002. *Electronic Patient Record Security*. Msc in Information Security. Information Security Group. Royal Holloway, University of London.

GnuPG, 2003. *Gnu Privacy Guard, Open PGP*. Available at: http://www.gnupg.org.

Godoy, C., 2002. *A privacidade e o registro informatizado na Faculdade de Medicina de Marília*. Encontro Paulista de Pesquisa em Ética Médica 2002.

Hassey, A., 2001. *A survey of validity and utility of electronic patient records in a general practice*. BMJ. 322:1401-1405.

IETF, 1999. TLS – *Transport Layer Security*. RFC 2246. Internet Engineering Task Force - IETF. Available at: ftp://ftp.rfc-editor.org/in-notes/rfc2246.txt.

IETF, 2003. LDAP – *Lightweight Directory Access Protocol* . RFC 2251. Internet Engineering Task Force - IETF. Available at: http://www.ietf.org/internet-drafts/draft-ietf-ldapbis-protocol-18.txt.

Kurtz, G., 2003. *EMR confidentiality and information security.* Journal of Healthcare information management. 17(3):41-48.

MSDN, 2003. *Microsoft Active Directory*. Available at: http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netdir/ad/active_directory.asp.

PHP, 2003. *PHP Hypertext Preprocessor*. Available at: http://www.php.net.

Salazar-Kish, J., 2000. *Development of CPR Security Using Impact Analysis*. AMIA Annual Symposium.

Shortliffe, E., 1999. *The Evolution of Electronic Medical Records. Academic Medicine*;74(4):414-419.

Silverman, R., 2000. *A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths*. RSA Laboratories Bulletin, 13.

Stausberg, J., 2003. *Comparing paper-based with Electronic Patient Records: Lessons Learned during a Study on Diagnosis and Procedure Codes*. J Am Med Inform Assoc. 10:470-477.