Compliant Secured Specialized Electronic Patient Record Platform

Gouenou Coatrieux, John Puentes, Catherine Cheze-Le Rest, Christian Roux

Compliant Secured Specialized Electronic Patient Record Platform

G. Coatrieux, J. Puentes, L. Lecornu, C. Cheze Le Rest and C. Roux

Abstract— **Distributed medical information systems are prone to security flaws at three main different levels: storage, processing and transmission. Among implemented security mechanisms, few concern intrinsic patient records multimedia content protection. This article presents a Secured Specialized Electronic Patient Record (SSEPR) based on a JPEG2000-XML structure designed to provide interaction with the Medical Information System (MIS) security mechanisms and policies. Such SSEPR is an Electronic Patient Record (EPR) elementary resource, containing data and information generated by daily practice in a technical medical unit, grouping information that belongs to one patient examination (images, examination data, medical report). Devoted to be handled and shared, it integrates different security attributes that are used to certify information reliability (information integrity and authenticity), while controlling information access in a compliant MIS. Aiming to be as generic as possible, the presented SSEPR and its platform prototype have been developed in the framework of a nuclear medicine service. Properly defined, EPR security layer can be used to improve security in handling and sharing medical information.**

Key Words— **Specialized Electronic Patient Record, Security, Reliability, Watermarking, Cryptography.**

I. Introduction

ELECTRONIC Patient Record (EPR) handling in a networked Medical Information System (MIS) significantly improves daily medical practice, introducing however, new risks for medical information.

Ensuring EPR security guarantees that an authorized user will have information access (*confidentiality* & *availability*). At the same time, the user must have a confirmation that the accessed information is reliable (*reliability*), by means of a certification that the information has not been modified in a non-authorized manner (*integrity*), and that it belongs to the right patient, being issued from the correct source (*authentication*) [1]. Hence, an EPR will be reliable, only if each one of its elements is certified as reliable. Defined as such, security acts like an EPR quality factor. Furthermore, when medical information is shared, reliability becomes a critical feature for healthcare professionals activity, as well as in the responsibilities chain.

Usually, handling EPR security means dealing with the security of the MIS that handles the information. MIS security design may be covered in three main steps [2]. First, an analysis leads to the identification and evaluation of risks that can damage the system, its functionalities, and especially the handled medical information considering the sensitiveness of data integrity, confidentiality and availability. In the second step, security objectives are simultaneously defined and implemented (security policies and procedures design, security tools integration). The third step consists on testing and verifying that the security objectives are satisfied.

Information access control is a good illustration of these concerns. An access control policy can be deployed using the Role Base Access Control model (RBAC) [3] and different security tools like the two-factor authentication (combining: password, biometrics, smartcard [4],…), firewalls, virtual private network, etc.

We consider that several security layers have to be distinguished: EPR itself, MIS (storage and processing), and transmission, inherently linking each layer to the others. Because EPR security layer is integrated to the previous ones, the EPR structure has to provide security facilities and attributes to be handled in a secure environment. DICOM (medical.nema.org) integrates this concept, only for medical images providing security mechanisms to be used in a secure environment for storage, transmission and image anonymity.

In this context, we propose a Secured Specialized Electronic Patient Record (SSEPR) model, showing the example application of a nuclear medicine service. Such a SSEPR is an EPR elementary resource containing data and information, belonging to one specific patient exam (images, examination data, and medical report) in a technical medical unit. One patient EPR may contain therefore several SSEPRs.

SSEPR security attributes have been designed taking into account MIS interactions based on access control, cryptographic and watermarking mechanisms. Cryptography and watermarking are complementary algorithmic approaches used in this context to certify information reliability. Watermarking, originally proposed for copyright protection of multimedia documents [1], is starting to be considered in healthcare. Applied to images, it allows embedding data directly within the host media, by modifying its pixel grey level values, preserving the image file format. In that way, watermarking facilitates different kinds of information to be put together as a unique entity: a watermarked image. In our scheme, watermarking is used for medical image protection and to inherently link images with the SSEPR medical report. SSEPR design, based on XML (eXtensible Markup Language) and JPEG 2000, is discussed

G. Coatrieux, J. Puentes, L. Lecornu, and C. Roux are with the LatIM, INSERM U650, GET ENST Bretagne, Brest, France (phone: +33(0)229001508; fax: +33(0)229001098; e-mail: gouenou.coatrieux@enst-bretagne.fr).

C. Cheze Le Rest is with the nuclear medicine service of CHU Morvan, Brest, France.

in section II, according to medical use considerations. Thereafter, SSEPR security attributes, are presented in section III. Before concluding, we describe in section IV the SSEPR platform prototype that has been developed.

II. Specialized Electronic Patient Record (SEPR)

The proposed SSEPR has been designed to satisfy a given daily medical practice user requirements, according to the workflow of the Nuclear Medicine Service (NMS) at the CHU Morvan, in Brest, France. Nevertheless, the proposed methodology and SEPR model can be adapted to any other medical units.

A. SEPR design

The SEPR encapsulates multiple images, specific patient data and diagnostic information concerning only one examination [5]. Its model has been defined taking into account the observed medical unit workflow, which served as the conducting thread to guide technical decisions. Among the considered elements we found: useful data and information input-output, creation-storage-consultation-acquisition-exchange stages, complemented by users' interactions. Fig. 1 shows a simplified view of the resulting analysis. Initially, a referring physician, requests a particular patient examination. The examination request is then completed with all existing reliable information that would support image interpretation by the NMS specialist. The secretary inputs that information and fixes the appointment date. Then, when the patient is taken in charge three phases can be distinguished:

1. Before image acquisition, provided patient information may be updated (weight, allergies, suspected lesions, etc.) and the image acquisition protocol is defined.
2. Images are acquired and added to the patient SEPR by a technician or a physician. In our case more than 200, 144 x 144 pixels, 2 byte depth images, issued from a PET (Positron Emission Tomography) equipment, are used.
3. Images are interpreted by the NMS specialist who may exploit at the same time any other provided information. Next, the medical report is dictated by the physician and typed by the secretary.
4. After the medical report is added, the SEPR can be archived and shared. Once it is "closed", any other modifications are not allowed. However, authorized corrections can be added within an attached file.

In this scenario multiple authorized users may be able to access, share and handle (consulting and editing) the same SEPR content, at every stage. Even so, specific access rights over data should be attributed to each one.

B. SEPR implementation

Accordingly to the requirement of system interoperability for the exchange of medical data, the proposed SSEPR is based on XML and JPEG2000 which are two open multimedia standards. This approach is combined with the use of open programming languages to develop the SSEPR platform.

JPEG2000 is a still image compression standard. It enables encapsulation, in a single file (with a JP2 name extension), of lossless/lossy compressed image with XML formatted metadata. We have adapted this feature to structure and integrate the SEPR to a related set of multi-component images, with their respective medical data [5].

XML provides means to structure information to be exchanged in various application domains. It conveys syntax and semantics, facilitating therefore information exploitation. In the proposed SSEPR, XML formatted metadata, such as the patient exam related data and medical report, are included within the JP2 file structure (Fig. 3). XML metadata can be easily extracted without decoding the images, and is more flexible than predefined content fields.

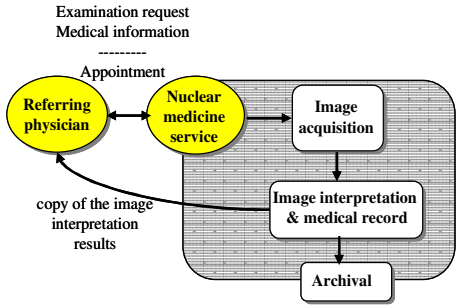

Fig. 1. Simplified workflow of a nuclear medicine service, from the examination request to results archiving.

An alternative implementation could be to group within an XML file, the patient metadata and the pointers to the compressed images. Nevertheless, once the images are interpreted, they constitute with the medical report, a single information. Consequently, they should not be dissociated.

Up to this point, the depicted structure is not secured, needing the application of the security attributes, described in the following sections.

III. Secured SEPR (SSEPR)

A. Security layers

In designing the SSEPR security attributes that will be processed by MIS security mechanisms, we have considered the following security layers: the healthcare institution, the MIS that allows SSEPR handling, the SSEPR and its content.

We consider that MIS is equipped with cryptographic and watermarking services. Cryptography provides confidentiality through encryption, but also integrity control and non-repudiation using digital signatures [6]. As described before, watermarking allows information embedding within images. Therefore, digital signature and encrypted data can be inserted within images allowing, for example, image reliability control. One question remains

though: how to provide the cryptographic keys?

It is assumed that the healthcare institution has defined a security policy specifying, how authorized health professionals access the information. Technically, this authority can be partially denoted by a Public Key Infrastructure (PKI), which provides users electronic

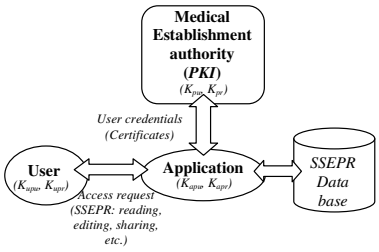

Fig. 2. User authentication and PKI - (K_{upu},K_{upr}) represent the cryptographic user pair of keys.

credentials or certificates. These certificates belong only to one entity (a user or a system), and contain its cryptographic public key. Certificates can't be forged because they are digitally signed by the certification authority represented by the PKI: the healthcare institution. Furthermore, a private cryptographic key, exclusively known by one entity, is linked to a certificate. For one particular user, it is assumed that this private key is stored on a smartcard.

In our approach, the MIS or the SSEPR application acts as an entity, meaning that it is recognized by the PKI, and that it possesses its own certificates and cryptographic key pair (Fig. 2.). Consequently, when a user requests to access the MIS, this one asks the PKI for the user's credentials. PKI recognition is followed by MIS reception of the user's public key. User access will then be granted if the two factor authentication is successful.

B. Security attributes

SSEPR security attributes (Fig. 3) may be distinguished according to different SSEPR use scenarios. Each of them can be seen as using an independent SSEPR feature exploitable by a compliant MIS.

1) Accessing the SSEPR content through a SSEPR secured envelope

In the case of the NMS, retrieving the patient's SSEPR is based on different Unique Identification Numbers (UINs). These UINs establish the link between the SSEPR and the patient, as well as the exam and the healthcare service it belongs to. In the NMS MIS, SSEPR file name (one UIN) computation corresponds to a cryptographic hash or digest [6] of the patient ID concatenated with a system secret key. Linking a JP2 file to a patient needs to know the system secret key, otherwise it will not be possible to retrieve the patient ID from the JP2 file name.

Once the SSEPR is retrieved, its information access is controlled by an Access Control List (ACL) [7], which contains access rules applying the security policy of the institution (Figure 3). A MIS would only be able to decrypt the ACL, using its private key. In fact, the ACL is encrypted by the system administrator using the MIS public key. The ACL content is digitally signed by its author: the security officer (in our case the system administrator). When a user access is requested, the MIS identifies and authenticates it through the PKI, and checks the user rights within the ACL. If the user is allowed to access the records, after ACL integrity verification, the last parts of the XML formatted data are decrypted. To reduce decryption complexity, this second part is symmetrically encrypted, meaning that the same key is used to decrypt and encrypt the information. The key is placed within the ACL. Successful access requests are recorded by the MIS in the SSEPR, in an audit file (access log).

An ACL is added each time the SSEPR is transmitted with a content that satisfies the security policies of both communication channel extremities.

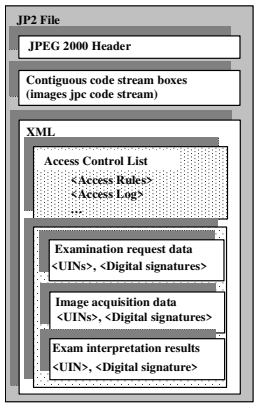

Fig. 3. Organization of the main SEPR tags in the XML box of the JP2 file.

A complementary security attribute can be used to indicate the actual status of the SSEPR: created, available for authorized edition or consultation, closed, archived, or copy of the original.

2) Adding Reliable Information to the SSEPR

Three different kinds of information are added to the SSEPR: information provided by the referring physician, new acquired data and the medical report. The first two have to be reliable before being included into the SSEPR. In such a scheme, a UIN functioning as a data pointer indicates unambiguously the origin and attachment to the same patient. Moreover, data have to be digitally signed by the provider. After the reliability check is performed, data or their UINs are added to the SSEPR with the corresponding digital signatures, allowing compatible systems to verify that the information has not been changed.

The medical report written by the physician includes images' interpretation taking into account available information. This report should be as well, digitally signed by the physician, who will not be able to repudiate its content. However, since the report may depend on several data sources, it should integrate all the data UINs that were used. Furthermore, a link must be established between images and the report content. To obtain it in our scheme, digital signatures computed over the report content, as well

as the report and images UINs, are embedded applying a reversible digital watermarking method to the images. That is, once the watermark is read and removed from the image, the original pixel values are restored, preserving the image quality for the diagnosis.

IV. SSEPR PLATFORM

A. System architecture

Fig. 4 depicts the bloc diagram of the proposed SSEPR platform. It has been developed with Apache2, PHP-5.0.4-Win32 and MySQL Server 4.1. A two factor user authentication with smartcard containing a cryptographic private key, is assumed. This key is used each time the user modifies an SSEPR element, digitally signing the new information, certifying as a consequence its reliability. User's public keys are simulated and known to be available from a PKI. Each class of users interacts with some specific html pages, adapted to their specialty. These pages provide a particular view of the SSEPR content they are authorized to access.

At a functional level, an Apache server handles the requests issued by an internet browser client. Following user authentication, the adapted request processing is activated. Acquired images are compressed in a lossless mode using an open source JPEG 2000 codec called Jasper (www.ece.uvic.ca/~mdadams/jasper/), after they have been

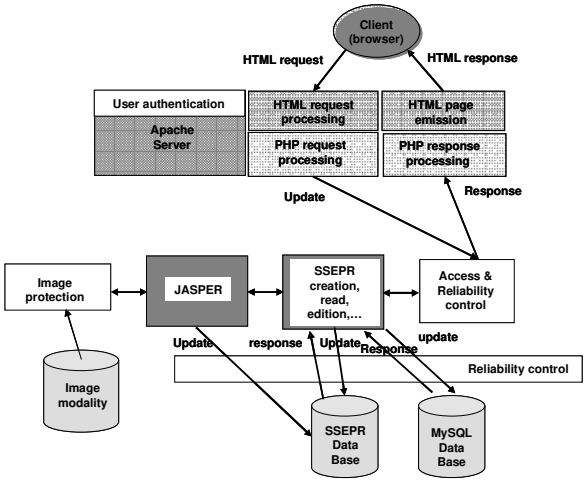

Fig. 4. Platform architecture.

watermarked, and the associated data formatted in XML.

B. Secured archival

Additional security mechanisms are included in the proposed SSEPR platform. One consists in splitting the SSEPRs in different parts: ACLs, image flow and XML data. Combined with secret file name (see §III-B-1) it becomes difficult for an intruder to rebuild a complete SSEPR without knowing the different secret keys. The second mechanism consists in a reversible system watermark that allows file integrity verification. Each time a file is received or created, the system computes a cryptographic hash or digest on a secret bit subset of the binary file representation. This digest is then "xored" with another bit subset of the file. Iteratively applied, at least two times on a file, it provides integrity protection. Cryptographic hashes will be different if the file is modified. These marks should be removed from the file before it is accessed. However, depending on selected bit subsets information may be readable. This enables the platform to check SSEPR data base integrity continuously without having to access information content.

V. CONCLUSION

An XML-JPEG2000 based Secured Specialized Electronic Patient Record which belongs to a patient examination in a technical medical unit has been presented. This SSEPR has been designed considering an EPR security layer that interacts with the MIS security layer. It integrates security attributes that enable access control through an Access Control List in compliance with the healthcare institution policy. Watermarking is combined with cryptographic services, linking medical images with medical data and information, improving at the same time information reliability control, allowing SSEPR exploitation in complete trustiness. The proposed SSEPR design approach is extendable to any other medical unit. Furthermore, SSEPR security attributes may facilitate medical information sharing across different institutions and services. By using open standards, the proposed SSEPR and its platform could be an alternative to overcome some interoperability issues, while preserving security.

ACKNOWLEDGMENTS

This work has been supported by the CRITT Santé, Région Bretagne. Authors are grateful to Anoop Kumar and Nitin Singhal for the programming work.

REFERENCES

[1] G. Coatrieux, H. Maître, B. Sankur, et al., "Relevance of watermarking in medical imaging", Proc 3rd International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine, 2000, pp. 250-55.

[2] CEN/TC251, Env 12924 – "Security categorisation and protection for healthcare information systems", Technical Report, CEN 1997.

[3] AA. El Kalam, R. El Baida, P. Balbiani, et al., "Organization based access control", Proc International IEEE Workshop Policies for Distributed Systems and Networks, 2003, pp. 120-31.

[4] A. Dwivedi, RK. Bali, MA. Belsis, et al. "Towards a practical healthcare information security model for healthcare institutions", Proc 4th IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine, 2003, pp. 114-17.

[5] L. Montesinos, J. Puentes, "Specialized telepathology electronic patient record based on JPEG 2000", Proc. 4th International IEEE EMBS Special Topic Conference on Information Technology Applications in Biomedicine, 2003, pp. 110-113.

[6] B.Schneier, Applied Cryptography, second edition. Paris: International Thomson Publishing, 1997.

[7] RS. Sandhu, P. Samarati, "Access control: principle and practice", IEEE Magazine on Communications, 1994, Vol.32, n°9, pp. 40-48.