SECURE TELEMATIC ARCHITECTURE TO SUPPORT A HOSPITAL INFORMATION NETWORK DEPLOYMENT

M.A. Valero*, V. Hernández*, L. López*, J.F. Martínez* and F.J. Ortega**

* Polytechnic University of Madrid/D. of Telematics Engineering and Architectures, Madrid, Spain
** Fuenlabrada Hospital/Traumatology Unit, Madrid, Spain

mavalero@diatel.upm.es

Abstract: Guarantee of security in Telematic networks is an essential factor to introduce hospital information systems into clinical routine. Increased utilization of electronic health records (EHR) does demand secure access and custody for sensitive information according to European policies about patient autonomy as well as rights and obligations for clinical information. In order to fulfill legal requirements, a reliable telematic architecture has been modeled, designed and verified that facilitates association of security policies according to a hospital unit organization. Based on the principles of MDA (Model Driven Architecture) a Unified Modeling Profile is identified, UML-CDHS (UML for Configuration and Deployment of Hospital Systems), which allows, independently of particular technology, specifying information of configuration. Combination of cryptographic tokens and PKI in designed architecture provides secure mechanisms according to health policies confidentiality. In addition to Advanced Encryption Standard, EHR files are also ciphered with a block identifier and or exclusive operations in order to reduce possibilities of a brute force attack to the hospital network, although it extends the processing time.

Introduction

Electronic Health Records management in hospital information systems requires efficient distributed data services but also security guarantees especially when enormous amounts of sensible information are stored. Both international bodies such us European CEN/ TC251 WGIII and ISO TC/215 WG4 have worked on specific recommendations for secure data flows between EHR Requesters, Providers and Servers [1]. However architecture deployments in commercial solutions do not fulfill standards at telematic network level as they mainly control database access. European Council resolution of February, 2003, on a "European approach towards a culture of network and information security" did state the "need to ensure the development and deployment of an appropriate skill base in the field of network and information security" [2].

In relation to mentioned directives, Spanish legislation already stated in Real Decree 994/1999 safety measures of the automated files that contain personal data. Within this judicial framework, electronic files containing personal health data are subjected to maximum security demands including critical aspects as covered in articles 23, 24 and 26:

23. Media Distribution: Distribution of electronic media containing personal data will be done by ciphering these data or by using whichever mechanism that guarantees that this information might not be legible or manipulated during its transportation.

24. Access Registry: From each health information access, it will be recorded, at least, user identification, access time and date, access type and user authorization or refuse.

25. Telecommunications: Transmission of personal data through telecommunication networks will be done by ciphering these data or using any other mechanism that guarantees that information is not intelligible or manipulated by third.

Later on, Law 41/2002 would regulate in article 19 patient autonomy and rights and obligations in the matter of information and clinical documentation [3]. The obligation to set procedures for clinical data preservation directly mentions the right of patient "to that the health centers may establish a mechanism of active and diligent safekeeping of clinical histories". Furthermore, referred article concretes this obligation by including "the collection, integration, the recovery and the communication of the information subjected to the confidentiality principle" of article 16 of this Law.

National and autonomic legislation also deal with professionals right to access to medical information and to communicate clinical history data: 1) professionals in charge of patient diagnosis and treatment can accede to clinical history prior identification and authentication and 2) the communication of data of clinical history is authorized, even without consent of the interested one, in these assumptions: cession to judicial authorities, urgency situations, epidemiologic studies, public health, investigation and teaching, as well as inspection functions, evaluation, accreditation and planning.

Thus, incorporation in market products of health security requirements in corporative environments such us a hospital requires to solve these two problems:

- Automatisation of pprocesses leading to quick or single tasks independently on health professionals.
- Easy renovation or revocation of keys associated to users or workstations not requiring a big amount of time to ensure that available terminals or health professionals lack of real confidential access.

ISSN: 1727-1983

Reality demonstrates that current EHR solutions are proprietary and not adjusted to standards what forces to modify existing infrastructures for real deployment of security configuration policies. So, the operative necessity arising from the legal and commercial framework described led to the modeling, design and validation of a secure Telematic network architecture independently on the hospital information database originally selected by health authorities. This solution should be able to avoid non authorized storage of clinical information in devices which are external to the health institution and to guarantee confidentiality of clinical information as well as availability of computers for the access to the data of interest in a comfortable, trustworthy and efficient way.

Starting from a case study of rolls and hierarchy of access defined by health policy at a hospital unit, the conceptual bases of the developed model of architecture are described in the following section. Once information flows are modeled according to security policies, an innovative way to combine different cryptographic methods is presented in order to solve the problems referred. A restriction previously imposed to design is the exclusive utilization of security standards which are compatible with available technology and do not depend on the infrastructure or preexisting software in the health institution which permits the validation of the system developed.

Methods

The definition of a precise "knowledge" of the elements and restrictions that make up the system supporting a secure architecture for EHR is a key aspect to be agreed between health institution clients and design engineers. Next, this knowledge must be translated into a type of special "information of configuration" that permits for each component to describe its functionality, implementation, possible configurations at deployment time, environment dependencies, and, security policies conditioning security dependences and security requirements.

In this sense, recommendations from international standardization bodies and industrial consortiums such as ITU-T, OMG and ISO have been followed to specify the distribution and configuration of distributed component-based application for a Hospital Information System. Thus, a language called UML-CDHS (Unified Modeling Language for Configuration and Deployment for Hospital Systems) has been proposed relying on the concepts and principles of what is at present known as an UML-profile [4].

UML-CDHS is foreseen as a platform-independent language for modeling information of configuration in health information systems so that Platform Specific Models are defined at the user domain model. It defines an UML package structure that establishes a relationship between the UML meta-model and the new elements defined by UML-CDHS. As shown in Figure 1, a Configuration Management (CM) Core package contains those virtual meta-classes that represent the different types of configuration information attending to hospital unit security policies, as well as the elements that enable establishing relationships among their instances, at the level of model, of components whose configuration requirements have to be characterized. The CM Model Management package contains virtual meta-classes whose instances facilitate the organization of configuration information specification and their reuse. The CM Core package contains those packages that classify meta-concepts of configuration information depending on their use in the analysis and design phases of system components.

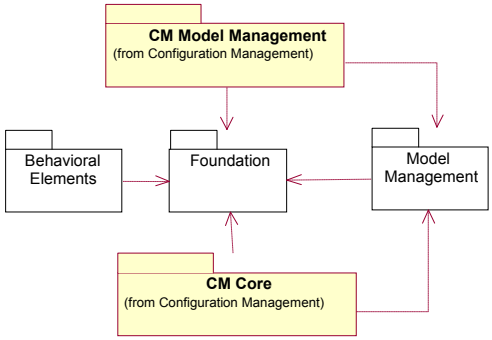

Figure 1: Relationships between UML-CDHS virtual meta-model and UML meta-model

The configuration information types, defined with UML-CDHS, permit to characterize each software component supporting the Hospital Information System, which is related to general definitions of types of configuration information. General concepts defined in UML-CHDS, which describe the different types of component configuration information are summarized as follows:

Policy of Configuration: Defines how configuration tasks related to configuration process are executed. UML-CDHS has simple and composite configuration policies for transaction, security or persistence issues.

General Characteristics of Configuration: Information types of configuration describing the component structure and some of its behavioural characteristics like emitted events, consumed events, supported, used, provision or factory interfaces.

Properties of Configuration: Global properties of components configuration used in the configuration of some type of attribute such us activation criteria, deactivation criteria, reactivation criteria, labels of component instances or internationalization criteria.

Taking into account a standard EHR specification, the three following information types have been distinguished for a health data component belonging an electronic file: Administrative data (identification and contact data), Clinical History (Anamnesis and Medical Episodes) and Nursing Care (Treatment Plan). As extracted from target hospital unit to deploy the secure

ISSN: 1727-1983

telematic architecture, five different categories of health professionals working in the participating traumatology unit were: Head of Service, Medical specialist, Medical assistant, Nursing staff and Administration personnel. So, attending to behavioral characteristics and access restrictions defined with UML-CDHS, closed information groups were defined whose data set is only available for each member group activating or not four attributes to be allowed for an information component: Read, Write, Modification and Erase. Table 1 depicts in a schematic way, policy adopted for information of configuration by associating each category of health professional to the access attributes defined for each type of health data component:

Table 1: UML-CDHS Access Configuration Policy

Roll	Admin Data	Clinical History	Nursing Care
Head of Service	RWME	RWME	RWME
Medical specialist	RWM	RWM	R M
Medical assistant	R M	RW	R M
Nursing staff	R M	R	RWM
Administration personnel	RWM	---	---

The creation of a Platform Specific Model that may respond to the configuration policy addressed in UML-CDHS modeling stage lead to decide the utilization of corporate keys. Integrity data restrictions were considered in order to guarantee authenticity by means of the use of signature and digital certificates working with the same key in the same authorized group of users (rolls) and computers, leading to closed circuits of information. The above mentioned keys are hidden and ciphered in the profile of the users and computers related to every group. Provided that the profiles download in every computer is automatic, taking advantage of the operating systems mechanisms, the user does not have to remember or store all the keys of the groups he belongs to. The management of the keys is designed to be performed from a central computer what simplifies the renovation and revocation process because it is enough to update the profiles of the users and concrete computers in an only one machine: the Keys Manager. All generated claves are stored in a X.500 Directory Service Lite (LDAP-LightWeight Directory Access Protocol-) [5] what guarantees the access to the ciphered information, with independence of the antiquity of the key employee.

The protection level for information interchanged in the local area network has been increased using internally secure communication protocols available on operating systems as IPSec. Thus, a secure point to point tunnel enhances protection in addition to corporate keys and the delivery mechanism defined.

Incorrect uses of the system that should provoke equipments reconfiguration or repair were also a key requirement associated to the priority of providing with high availability to the hospital information system. Therefore protection mechanisms have been added what allows in many cases to avoid not supervised software installation on the part of the hospital personnel or the involuntary introduction of virus that, for example, involves the system arrangement or restoration producing temporary and economic costs.

As General Characteristics of Configuration specify in design stage, the capacities of the users should be limited by the computer systems administrators according to their rolls and profiles. However, this solution is very complex to be administrated in the telematics network of a hospital entity, due to the great diversity of user and machines profiles and the high equipments heterogeneity. The solution proposed to palliate this problem was to include ciphering for all the components containing different information types as recorded in the information storage peripherals of the computers of the network. The result is an impossibility to use any file or information package in an external computer to the network as it has not the required keys. Not only the users should be prevented from introducing virus computer or applications that conflict with already installed others, but besides it should not be able to use programs that compromise the security of the system. The capability of avoiding to install software or to copy files that do not belong to the heath center network as they have not been ciphered added robustness to the system by turning out to be illegible whichever software package in the computers of that network.

Results

Final development of the telematic architecture provided to support the HER management system can be decomposed in two functional blocks: the Keys Manager, component in charge of keys generation and delivery, and the block of components that are executed in every computer and that permit files ciphering whenever read or write functions are performed.

A good balance between security and performance was to generate pseudo-random keys of 256 bits in Keys Manager using standard algorithms as PRNG (Pseudo-Random Number Generator), extensively analyzed as Blum Blum Shub (BBS) and X9.17. These set the base for files ciphering using the secure algorithm AES (Advanced Encryption Standard) [6] on blocks also of 256 bits which is a key size considered inviolable today and in the next 20 years. The Key Manager consists of three components providing the following tasks:

- Keys generation and recording in its Directory Service for all the closed groups of information.
- Digital certificates management by means of a Certificate Authority that can be an eternal one.
- Users and computers profiles storage as well as access to the digital certificates.

ISSN: 1727-1983

The profile server avoids the direct access from the health center network to the Certificate Authority and to the Directory Service which reduces risking vital information for the corporate system security. So, two components are installed in every network computer of the hospital information system:

- Device drivers entrusted to cipher and decipher the content of the sensitive files.
- Management application that configures some device driver parameters besides supervising the proper operation of both components.

Once the computer of the health staff boots, the device driver starts up and the management application authenticity is verified realizing a code checking. It verifies, using predetermined values, the length and the result that is obtained on having applied the operation or-exclusive to the whole code taking blocks of 256 bits. Later, the device driver generates a random key of 256 bits whenever it begins and it is sent to the management application. Next, using the algorithm AES, ciphers with it the configuration file and the corporate keys of the corresponding profile that have been concealed and ciphered in the computer as describe later on. Therefore, it is practically impossible that an attacker could manage to obtain the keys realizing an indiscriminate attack, or brute force attack, to the profile element that stores the keys, though he discovers its location.

If the device driver detects some unusual situation, it blocks devices access, registers the event locally and, if it is feasible, sends to the management application a copy in order that a remote record is also done. The structure that presents a file after being ciphered is the one that is reflected in Table 2:

Table 2: Structure of EHR ciphered files

Closed Group of Information Key Identifier	K_s (K_a)	F (identifying string)	F (length)	F (data)

The key of closed group of information that has been used in the process of ciphering is identified in the first byte. Next, a block of 256 bits results from ciphering a key random K_a of 256 bits for every file with the key of closed group of information K_s using AES, which prevents an attacker from deciphering all the files coded with the same key K_s. The following block of 256 bits is obtained when ciphers a certain string of 32 bytes which allows knowing if a file is or not ciphered. The ciphering algorithm of block F(x) is based on the algorithm AES and ciphers every block of 256 bits in the following way:

$$F(X_i) = K_b(i) \oplus (K_a(X_i) \oplus F(X_{i-1}))$$

K_b is a pseudo-random key of 256 bits obtained, using the AES algorithm, when the key of the closed group of information K_s is ciphered with the random key K_a. The penultimate block of 256 bits contains the ciphering of the file length, which allows detecting the insertion or elimination of blocks. The rest of blocks are the result of ciphering the clear file blocks (original file blocks).

The configuration of some parameters of the device driver can be done by the administrator of a network computer or equipment of the health center through the management application. It also permits:

- Ciphering the configuration file and the keys of the closed groups of information that are activated in the equipment at that precise moment.
- Checking the device driver authenticity in the same way as the device driver does with him.
- Verifying that the device driver is installed and working at all time.
- Reporting (locally and remotely) unusual events as well as blocking the device driver working in those cases.

The **architecture** of the resulting system is depicted in Figure 2, differentiating the components of the designed architecture and the computers of the network of the health center.

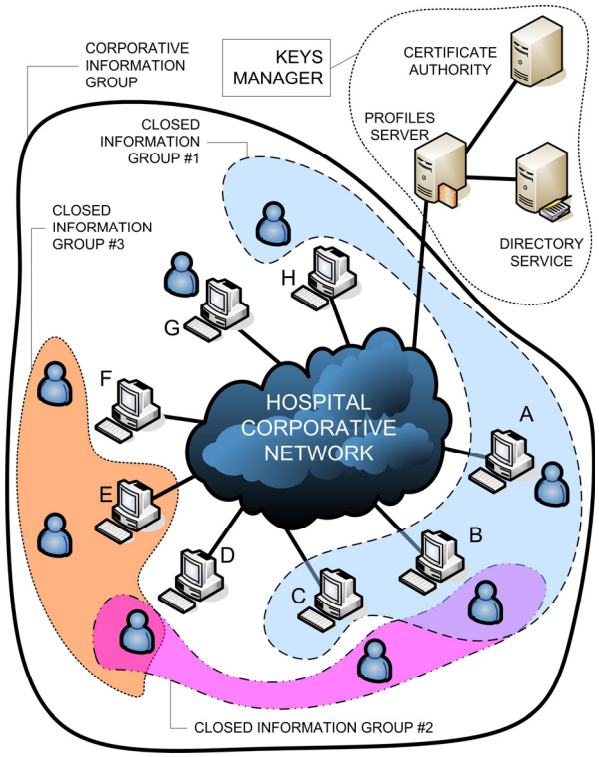

Figure 2: EHR Support System Architecture.

The scenario selected encompasses all the network computers that have the corporate key allowing accessing to public files of the corporation (corporate

ISSN: 1727-1983

group of information). Besides, the A, B and C computers, located for example in a restricted access zone, in a service area of the hospital, can always make use of the key of the #1 group corresponding, in this user case example, to the medical assistant doctors. The H computer also can make use, in that moment, of the #1 group key as the user who is using it is a member of that group. For the same reason that have been exposed for the H computer, the B and C computers have also the #2 group key and the D those of the groups #2 and #3 and the F the one of the group #3. The E computer always has the key of the group #3 as it belongs to this closed group of information. It is interesting to see how user in computer C that belongs to the Head of Service category need keeps all access attributes to the three closed groups.

Policies requests from UML-CDHS lead to define keys of closed groups of information that are secret in the computers. An attacker might locate the file where the keys have been hidden and try to replace or discover them. To obtain the keys from the file in which they have been hidden can be more or less difficult depending on how they have been distributed. Mentioned risk is avoided as the Keys Manager ciphers them in the profiles with the public key of the corresponding user, computer or closed group of information, as the case may be. When the keys are hidden in every computer, they are not altered, and therefore they remain ciphered. The above mentioned keys only will be able to be deciphered by the secret key of the proper hospital professional, computer or closed group of information. The hospital personnel will carry their secret key stored in an smart card or in a similar device, considering its comfort and security characteristics, and the computers that can only be used by a determined closed group of information will have it stored in an internal protected hardware device or software component.

Authenticity of the corporate keys hidden in the profiles is guaranteed as the Keys Manager signs them digitally. The digital signature of the keys concealed in a profile is stored in turn in the same profile. To generate the digital signature the hash function SHA1 (Secure Hash Algorithm review 1) is applied to the corresponding keys and the result, which has a size of 160 bits, is ciphered by the private key of the Keys Manager. Every network computer has to verify the mentioned signature and it is necessary to have installed the digital certificate of the Manager Keys and the CA that issued the mentioned certificate.

In order to make sure of the full confidentiality in the transmission of the information, all the communications among the network computers were decided to be ciphered. IPSec is the technical option chosen as it is the simplest option that needs less additional infrastructure and manages to prevent that anyone that captures the network traffic could know documents interchanged among other users or foreign profiles that contain others keys.

The design and development approach of the system critical components followed in the Telematic Engineering and Architectures Department of the Polytechnic University of Madrid has allowed working in the implementation of the demanded prototype. Full integration with the running EHR system on the user case hospital unit will permit a systematic evaluation of data integrity premises in daily routine context.

Discussion

Provision of security mechanisms according to the confidentiality requirements demanded by health information in the current national legislation and European policies has conditioned much the implemented architecture strategy. In spite of the inherent fortress that supplies the AES algorithm having ciphered a file, an additional ciphering is added based on a block identifier and an or-exclusive operation aiming to reduce the possibilities of a brute force attack to the hospital information network, though it increases the process time.

The keys, besides of being hidden in the profiles, are ciphered by the secret key of a user or computer. So, corporative keys can not be easily obtained. These technologies used to distribute and to store the keys take advantage of automatic mechanisms of the current computer systems but depend on each piece of unit performance

We should not forget that the only attacks that might success are those that pretend to provide administrative rights to any user and to unload from memory the device driver and the management application. On this point, anyone could introduce information in the computer and extract not ciphered data in the hard disk to realize scientific studies on the hospital registers and to modify the behavior of the device driver and the management application. Nevertheless, since the system does not allow the introduction and installation of any foreign software in the network computers of the health center, no specific tools may turn into manager any user of a network computer, reducing that way the possibility of success of the above mentioned attacks.

Conclusions

The analysis of the security requirements demanded for the defined telematic network architecture allows us to extract the following conclusions with regard to its deployment in a hospital information system:

- The health professional access rights to the information are protected by means of the keys associated with the closed groups of information that are hidden and ciphered.
- It has been guaranteed the confidentiality of the stored clinical information and there is no record of ciphering algorithm AES vulnerabilities. It is practically impossible to decipher the content of files in a reasonable time if the used key is unknown.

ISSN: 1727-1983

- The security of the closed groups of information, according to UML-CDHS specification keys, has been achieved by means of a proper distribution of the network elements that prevents a direct connection of the computers to the server that stores the above mentioned keys of the closed groups of information or to the Certificate Authority.
- The confidentiality of information interchanged among network computers can be ensured with IPSec. It prevents that anyone could snoop network communications and capture restricted information.

References

[1] CEN/TC 251. (2005): 'Health informatics — Electronic health record communication — Part 4: Security requirements and distribution rules', pp. 10-15

[2] COUNCIL OF THE EUROPEAN UNION. (2003): 'Resolution of 18 February 2003 on a European approach towards a culture of network and information security', *Official Journal of the European Union*, **28.2.2003**, p. C 48/1

[3] SPANISH PARLIAMENT. (2002): 'Ley 41/2002, de 14 de noviembre', *Boletín Oficial del Estado*, November, 15th, 2002, **274**, pp. 40126-40132

[4] OBJECT MANAGEMENT GROUP. (2004): 'UML Profile for Enterprise Distributed Object Computing – Meta-model and UML Profile for Java and EJB', v1.0, document formal/2004-02-02

[5] INTERNET ENGINEERING TASK FORCE, NETWORK WORKING GROUP (1995): 'RFC 1777 - Ligthweight Directory Access Protocol', Internet site address: http://www.faqs.org/rfcs/rfc1777.html

[6] Federal Information Processing Publication. '197 - Advanced Encryption Standard (AES) ', Internet: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

ISSN: 1727-1983