HMM: HIPAA Modeling Method for Modeling Security in e-Health

Abdelhay Haqiq and Bouchaib Bounabat

***Abstract*—Constructing secured health-care information systems requires collecting relevant information concerning the security safeguards and the ways to set them up. This information is the base for defining the targeted security system. In order to facilitate this knowledge gathering process, we propose throughout this paper, HMM (HIPAA -Health Insurance Portability and Accountability Act- Modeling Method) especially set-up so as to guide the interview process with healthcare security experts and computer engineers and grasp their know-how as well as their security needs. Based on UML (Unified Modeling Language) notation, HMM aims at transforming the HIPAA security requirements into models in order to define the process of the implementation of security policies, and therefore help the development teams to take into account the security aspect when setting-up e-Health systems.**

***Index Terms*—E-Health, information security, HIPAA standard, UML notation.**

I. Introduction

The health system consists of all the organizations, institutions, resources and people whose work together to provide and improve health care services. Over the last decade, information technology has emerged as an essential health tool [1]. It provides the possibility to have a new relationship between patient and health professional, to increase the efficiency and improve the quality in health care and to exchange the information in a standardized way between health care establishments [2].

However, the health information technology (e-Health) is exposed to many challenges [3]. As any other Information system, there is a huge need to implement the appropriate security safeguards which protect the electronic healthcare information that could be at risk [4]. Furthermore, in the context of health care, the consequences of lower security can be particularly important [5]. It is for these reasons that several standards have been elaborated so as to define security policies and procedures that determine the way how sensitive information and other resources have to be managed, protected and distributed inside the information system [6]. These standards are national (HIPAA: Health Insurance Portability and Accountability Act [7], PCHI-PCF: Pan-Canadian Health Information Privacy and Confidentiality Framework [8], HIPC: Health Information Privacy Code -New Zealand [9]), regional (The European legal framework 95/46/EC [10], or international (ISO/IEC 27001:2005 [11]).

Manuscript received March 10, 2013; revised June 17, 2013.

The authors are with the AL-QualSADI research team, ENSIAS (National Higher School for Computer Science and System Analysis), Mohammed V Souissi University (UM5S), Rabat, Morocco. (e-mail: abdelhay.haqiq@um5s.net.ma, bounabat@ensias.ma).

Nonetheless, in spite of the fact that the standards above give the best practices to implement security, there is a need in methods, models and tools to transform the security requirements into process dedicated to help development teams to take into account the security aspect when setting-up e-Health systems [12]. In this context the present paper proposes HMM (HIPAA - Health Insurance Portability and Accountability Act- Modeling Method) based on UML (Unified Modeling Language) notation, and aiming at transforming the HIPAA security requirements into models so as to define the process of the implementation of security policies.

The remainder of this paper is organized as follows: Section 2 sets out e-Health Security modeling issue. Section 3 presents the HIPAA (Health Insurance Portability and Accountability Act) standard and exposes the proposal approach HIPAA Modeling Method (HMM). Section 4 presents an example of HMM application and its support tool. Finally, we conclude and propose a global planning about our future work.

II. Healthcare Information System (HIS) Security Modeling

A. Necessity of Modeling Security in HIS

The Security of Healthcare Information System is a subject of a major concern. Indeed, over the years, there has been much technological advancement that has led to the healthcare industry leaning towards the use of electronic systems and leaning away from the old paper-based systems. This means that the medical workforce is more mobile and efficient, but the use of these technological systems creates an increase of possible security risks [13] and therefore, all healthcare organizations have to be aware that there is an urgent necessity to secure the vast information resource through effective management of the security of Information and communication technologies (ICT) systems and to maintain a high level of confidentiality, integrity and availability [14].

It is for these reasons that critical issues related to the security requirements have to be dealt with in the earliest phases of HIS architecture description and design [15]. Therefore, it is essential to provide completed models not only to describe how health information will be protected from security risks as it travels throughout the infrastructure, but also to ensure that the whole lifecycle of healthcare information protection and security is auditable. In this paper, we propose the use of UML (Unified Modeling Language) to describe Healthcare Information System (HIS) security specifications and requirements.

DOI: 10.7763/IJCEE.2013.V5.779

B. Using UML to Model Security in E-Health

UML is an object modeling standard for specifying, visualizing, constructing, and documenting the artifacts of software systems. Building secure systems in health care using UML has been realized in different projects [16]-[18]. The [19] presents a UML 2.0 profile for secure business process modeling of the health-care system through activity diagrams, the approach allows business analysts to specify security requirements in the business process, these requirements will be transformed, by the security experts, into technical specifications that include the necessary details for their implementation [20]. The [21] introduces an information security evaluation methodology for health information systems based on UML in order to improve the analysis of security countermeasures; assist in establishing an appropriate level of security; and, help organizations wishing to certify against an information security management standard. The [22] proposes an approach to use UML in the context of an extension of the processing of clinical data to provide a "patient-based electronic record," the project scope included the specification of software to provide interim access control, consent management and user registration services in a number on National Health Service care providers.

Using only UML to deal with Healthcare Information System (HIS) security modeling cannot be sufficient. There is a crucial need of the adoption of recognized standards for securing health information. In this paper, we propose to use Health Insurance Portability and Accountability Act (HIPAA) as a knowledge basis to determine HIS security specifications and requirements.

III. HIPAA Modeling Method (HMM)

A. HIPAA Overview

The Health Insurance Portability and Accountability Act (HIPAA) is an American standard created in 1996 in order to maintain the privacy of protected health information, to establish security requirements, and to develop standard identifiers [23]. The security and privacy standards promote a higher quality care by assuring to consumers that their personal health information will be protected from inappropriate uses and disclosures. Moreover, HIPAA defines the security standard as a set of requirements with implementation features that providers, plans, and clearinghouses must include in their operations to assure that electronic health information pertaining to an individual remains secure. There are five security Standards defined by HIPAA so as to protect the confidentiality, integrity, and availability of electronic protected health information [24].

1) **Administrative Safeguards**: Security measures are set-up in order to protect health information and manage the covered entity's workforce conduct related to the protection of that information. This part covers over than the half of the HIPAA Security requirements
2) **Technical Safeguards**: technology, policy and procedures that protect electronic protected health information and control the access to it
3) **Physical Safeguards**: measures, policies, and procedures are established in order to protect a covered entity's information systems, related buildings and equipment from natural and environmental hazards, and unauthorized intrusion
4) **Organizational Requirements**: essential to check if all security safeguards are implemented and if every staff member, temporary employee, sub contractor or third party has understood and comply with organizational policies when using electronic Health information
5) **Policies And Procedures And Documentation Requirements**: essential to implement and document any change in security policies and procedures made by a covered entity

The adoption of HIPAA as a fundamental basis for the proposed Healthcare Information System security modeling method has been done according to different reasons; on the one hand, the implementation of HIPAA safeguards is clear and well defined which facilitates the listing of all the HIS security data and specificities, on the other hand, although HIPAA standards are only specific to USA, they have positively affected the development of HIS world-wide [25].

B. HMM Phases

The HMM (HIPAA Modeling Method) approach aims at transforming the HIPAA security requirements into models so as to define the process of the implementation of security policies. Also, in order to guide the interview process with healthcare security experts and computer engineers and grasp their know-how as well as their security needs, HMM defines five main phases to follow:

1) **Definition Phase:** defines the requirements to establish in order to secure the e-Heath system
2) **Identification Phase**: identifies the actions to use
3) **Analysis Phase**: specifies security policies to follow
4) **Application Phase**: establishes the security procedures
5) **Post-application Phase**: verifies the progress of implementation of the security

The implementation of each HIPAA safeguard (Administrative, Technical, Physical, Organizational, Policies and Procedures and Documentation), can be made through the five HMM phases. Thus, we can represent HMM as a matrix presented in Fig 1. Its lines and columns correspond respectively to the requirements of HIPAA Safeguards and to the HMM phases. Definition and Identification phases describe HIPAA rules, while Analysis, Application and Post-application phases define the operations to achieve.

HMM phases / HIPAA requirements	Definition (*HIPAA Standards*)	Identification (*HIPAA Implementation Specification*)	Analysis	Application	Post-Application
Administrative Safeguards					
	...	..			
Technical Safeguard					
	...				
Physical Safeguards					
	...				
Organizational					
	...				
Policies And Procedures And Documentation					
	..				

Fig. 1. HMM matrix

The Fig. 2 below presents an example of describing HIPAA compliant technical safeguards through **Definition**

and **Identification** phases.

Once completed, HMM Matrix can be used to model security policies and procedures through HMM Business Requirements View.

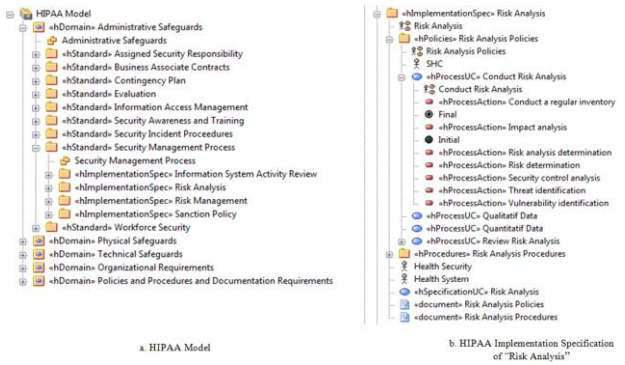
HMM phases / HIPAA requirements	Definition (*HIPAA Standards*)	Identification (*HIPAA Implementation Specification*)	Analysis	Application	Post-Application
TECHNICAL SAFEGUARDS	Access Control	Unique User Identification			
		Emergency Access Procedure			
		Automatic Logoff			
		Encryption and Decryption			
	Audit Controls				
	Integrity	Mechanism to Authenticate Electronic PHI			
	Person or entity Authentication				
	Transmission Security	Integrity Controls			
		Encryption			

Fig. 2. HMM technical safeguards description

C. HMM Business Requirements View

The HMM Business Requirements View (HBRV) uses existing "Security business" knowledge gathered in HMM Matrix specifications. It identifies the Security business in the domain and the security problems which are important to the organization. HBRV describes policies and procedures using UML description to model security policies by determining e-health security domains to be studied, and modeling the processes related to each identified use case.

The description of the HMM Business Requirements View begins by classifying the "security business" into categories specified in HIPAA Model (see Fig. 3.a). A HIPAA Model is the highest level of the HMM, which include one or more <<hDomain>> (Administrative, Physical, Technical, Organizational, Policies and Procedures and Documentation), each <<hDomain>> is divided into <<implementation specifications>> that delineate how each of the standards should be implemented. In some cases, the standard itself contains enough information to describe implementation requirements.



a. HIPAA Model

b. HIPAA Implementation Specification of "Risk Analysis"

Fig. 3. HIPAA structure

In addition, Health System and Health Security participate to specify implementation requirements which are supported by <<hSpecificationUC>>. In the <<hSpecificationUC>> the user defines the <<hpolicies>> and/or <<hprocedures>> and mentions the progress status linked to the security application using <<Curent_Status>>. The study of the use case of policy or procedure involves the use of <<hProcessUC>> with its association stereotypes as it is defined in UML. However, <<hProcessUC>> could not provide the semantic of policies itself. For this reason, <<Security_Service>> and <<Bool_Constraint>> are created to indicate the constraints of security policies. Also, we can use them with the same way in the activity diagram that uses <<hProcessAction>> and refines <<hProcessUC>> by describing its dynamic behavior (see Fig. 3b).

Moreover, the HIPAA policies do not only offer to users the mechanism to define the security requirement using stereotype and tagged value, but it also gives the ability to express easily the needs and to make understanding all participants the security requirements. The Fig. 4 and 5 below indicate the main stereotypes defined in HMM with description.

Base class		
Package Diagram	Name	**hDomain**
	description	Indicates the HIPAA requirements categories (Administrative, Technical, Physical, Organizational, and Documentation Requirements)
	Name	**hStandard**
	description	Presents the recommendations defined by HIPPA Standards section
	Name	**hImplementationSpec**
	description	Corresponds to the operations to ensure e-Health security. The operations are defined in the HIPAA Implementation Specification / Specification section
	Name	**hPolicies**
	description	The *HIPAA Policies* describes the security policies that an organization must follow
	Name	**hProcedures**
	description	The *HIPAA Procedures* describes how to apply the security policies
Use Case	Name	**hSpecificationUC**
	description	The *HIPAA Specification Use Case* corresponds to the *Implementation Specification* used
	Name	**hProcessUC**
	description	*HIPAA Process Use Case* is used to describe the Use Case for implementing policies or procedures, it can also be linked with other hProcessUC or actor
Action	Name	**hProcessAction**
	description	*HIPAA Process Action* corresponds to a step in the execution of a *HIPAA Process UC*
Object Node	Name	**hEntityState**
	description	*HIPAA Entity State* represents a state of action in the activity process

Fig. 4. HMM diagram

Base class		
Constrai-nt	Name	**Current Status**
	description	describes the progression state of an application security. The status corresponds to: Completed , Not Implemented , Review , Working
	Name	**Equivalent Constraint**
	description	means that a *constraint* must be appeared or used minimum or maximum of times
	Name	**Boolean Constraint**
	description	determines whether the *constraint* should be applied or not.
	Name	**Equivalent Restriction**
	description	means that a *restriction* must be appeared or used minimum or maximum of times
	Name	**Boolean Restriction**
	description	determines whether the *restriction* should be applied or not
	Name	**Requirement**
	description	corresponds to different actions that a covered entity must be complied with
	Name	**Security Service**
	description	defines the properties of security: Availability, Integrity, Confidentiality, Non-repudiation

Fig. 5. HMM constraints

The relationships between HBRV levels and HMM phases are described in the Table I.

TABLE I: HBRV LEVELS AND HMM PHASES RELATIONSHIPS

HMM phase	UML Diagram	HBRV level
HIPAA Standard (*hStandard*)	Package Diagram	Definition
HIPAA Implementation Specification (*hImplementationSpec*)	Package Diagram	Identification
HIPAA Process Use Case (*hProcessUC*)	Use Case Diagram	Analysis
HIPAA Process Action (*hProcessAction*)	Activity Diagram	Application
Current Status (*Current_Status*)	Tagged value	Post-Application

IV. EXAMPLE OF HMM

This section presents a simple example that illustrates the using of HMM. The example deals with "Data Backup Plan" corresponding to the standard of "Contingency Plan," the latter is included in "Administrative Safeguards" domain. The "Contingency Plan" establishes (and implements as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems which contain electronic protected health information. This standard includes different requirements that should be specified, in this paper we focus on "Data Backup Plan" which establishes and implements procedures to create and maintain retrievable exact copies of electronic protected health information.

The specification of "Data Backup Plan" begins by defining the **Definition** and **Identification** phases which correspond respectively to "<<hStandard>> Contingency Plan" (Fig. 6) and "<< hImplementationSpec>> Data Backup Plan" (Fig. 7). The Analysis phase is illustrated in Fig. 8 and 9 that describe the security policy to apply, also, the <<hSpecificationUC>> use case depends on the constraint <<Current_Status>> indicating that the security policy is in "Review".

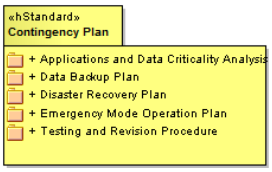


Fig. 6. "<<hStandard>> Contingency Plan

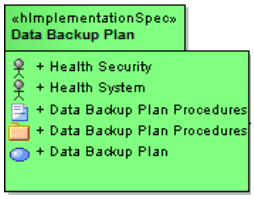


Fig. 7. "<< hImplementationSpec>> Data Backup Plan

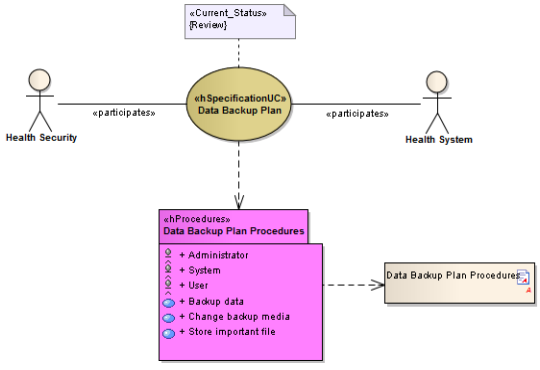


Fig. 8. Data backup plan procedures

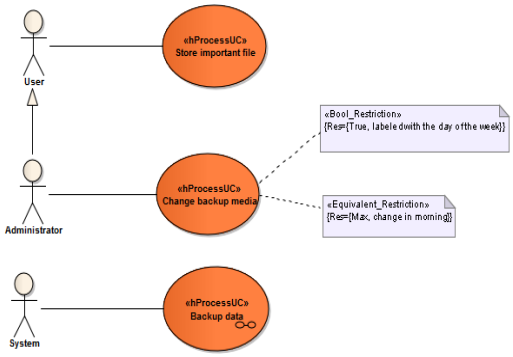


Fig. 9. <<hProcessUC>> Data backup plan

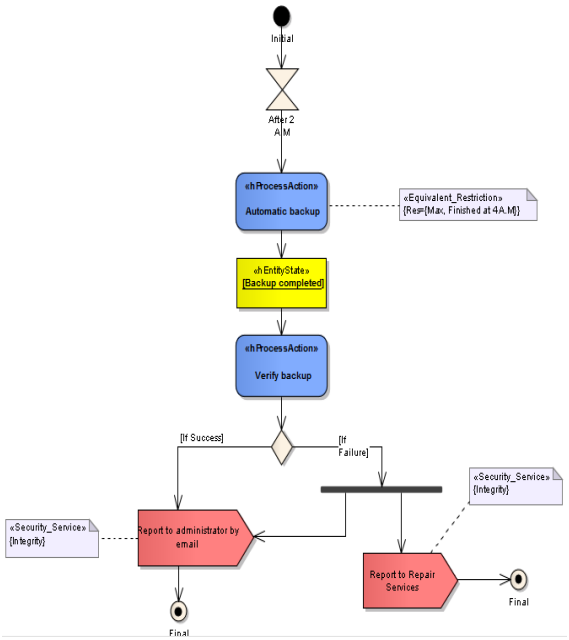


Fig. 10. Activity Diagram "Data Backup Plan"

Besides, the <<Current_Status>> corresponds to the **Post-Application** phase and moves from *Current_Status= "Not implemented"* until *Current_Status = "Completed"*. The **Application** phase being reached, here, we can implement mechanisms to carry out so that to apply directly the policies throughout the Activity Diagram (Fig. 10).

The Fig. 9 depicts a UML activity diagram for the "Data Backup Plan" use case, the activity begins by waiting 2 A.M. before starting the automatic backup which is illustrated as <<hProcessAction>> Automatic backup, the latter is relied on the constraint *Equivalent_Restriction {Max, Finished at 4 A.M}* which **means** that the backup is usually ending at 4 A.M. After this action, the backup program verifies that the backup is completed and all files are written out correctly. The success or failure of the backup program will be reported to the System Administrator by email. If the backup fails, it will also be reported to Repair Services. In order to ensure that the report is arrived successfully, the system should take into account the constraint *Security_Service{Integrity}*.

All the models above are generated by the plug-in developed in order to implement the HMM (see Fig. 11). This plug-in is accessible from the tool "Sparx Enterprise Architect". The HMM Modeling Tool has 5 customized toolboxes to assist the modeler to create HMM Models.

These Toolboxes are HIPAA {Standard, Implementation Specification, Specification UC, Use Case, and Process Activity}. Once a HMM diagram is opened or created, the corresponding HMM Toolbox is also opened. The User may simply drags elements from this toolbox into the opened diagram. The HMM element will be created in the project browser and also represented in the diagram where it was situated before. Relationships may also be created by dragging a relationship type from a HMM Toolbox.

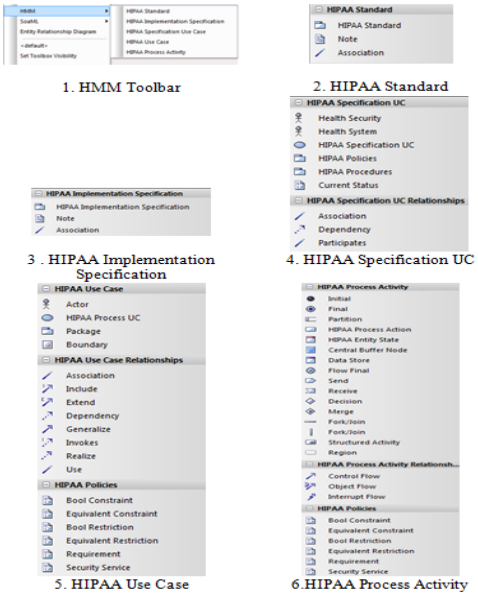


Fig. 11. HMM tool

V. Conclusion

The contribution of this paper is to propose HMM (HIPAA Modeling Method), a new approach dealing with Health Information System (HIS) security, and helping the development team to take into account the security aspect when setting-up e-Health systems. HMM is based on UML, it provides a guidance to capture all security requirements and decisions through package diagram, use case diagram and activity diagram and being in the same time compliant with HIPAA. Likewise, we have developed a plug-in accessible from the tool "Sparx Enterprise Architect" in order to make easier the HMM modeling. The works coming in the future will be converged on the examination of the use of other UML diagrams so as to extend the HMM to cover other specificities of HIPAA.

References

[1] R. G. Fichman, K. Kohli, and R. Krishnan, "The Role of Information Systems in Healthcare: Current Research and Future Trends," *Information Systems Research*, vol. 22, no. 3, September 2011, pp. 419-428.

[2] B. Chaudhry, J. Wang, S. Wu, M. Maglione, W. Mojica, E. Roth, S. C. Morton, and P. G. Shekelle, "Systematic review: impact of health information technology on quality, efficiency, and costs of medical care," *Annals of Internal Medicine*, no. 10, pp. 742–752, 2006.

[3] S. Jafari, F. Mtenzi, R. Fitzpatrick, and O. S. Brendan, "Security metrics for e-healthcare information systems: A domain specific metrics approach," *International Journal of Digital Society*, vol. 1, Issue 4, December 2010

[4] R. E. Scott, P. Jennett, and M. Yeo, "Access and authorisation in a Glocal e-Health Policy context," *Int. J. Med. Inform*, vol. 73, no. 3, 2004, pp. 259–266.

[5] F. S. Tsai, "Security Issues in E-Healthcare," *Journal of Medical and Biological Engineering*, vol. 30, no. 4, pp. 209-214, 2010.

[6] A. K. Jha, D. Doolan, D. Grandt, T. Scott, and D. W. Bates, "The use of health information technology in seven nations," *International Journal of Medical Informatics*, no. 12, pp. 848–854, 2008

[7] *Health Insurance Portability and Accountability Act*. [Online]. Availbale: http://www.cms.gov/Regulations-and-Guidance/HIPAA-Administrative-Simplification/HIPAAGenInfo/index.html.

[8] *Pan-Canadian Health Information Privacy and Confidentiality Framework*. [Online]. Available: http://www.hc-sc.gc.ca/hcs-sss/pubs/ehealth-esante/2005-pancanad-priv/index-eng.php

[9] *Health Information Privacy Code 1994*. [Online]. Availble: http://privacy.org.nz

[10] *The European Union Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of suchdata*, July 1995.

[11] *Information technology Security techniques - Information security management systems – Requirements*, International Standards ISO/IEC 27001, 2005.

[12] D. Mellado, E. Fernandez-Medina, and M. Piattini, "A common criteria based security requirements engineering process for the development of secure information systems," *Computer Standards & Interfaces*, vol. 29, no. 2, pp. 244-253, 2007.

[13] S. Adibi and G. B. Agnew, "On the diversity of ehealth security systems and mechanisms," in Proc. *Engineering in Medicine and Biology Society: 30th Annual International Conference of the IEEE*, pp. 1478 - 1481, Vancouver, 2008.

[14] E. Smith and JHP. Eloff, "Security in health-care information systems—current trends," *Int J Med Inform*, 1999, vol. 54, pp. 39–54.

[15] P. Guarda and N. Zannone, "Towards the development of privacy-aware systems," *Information and Software Technology*, vol. 51, no. 2, pp. 337-350, 2009

[16] C. Talhi, D. Mouheb, V. Lima, M. Debbabi, and L. Wang, "Usability of security specification approaches for uml design: A survey," *Journal of Object Technology*, vol. 8, no. 6, pp. 103-122, 2009.

[17] H. Mouratidis, A. Sunyaev, and J. Jürjens, "Secure Information Systems Engineering: Experiences and Lessons Learned from Two Health Care Projects," *CAiSE, LNCS 5565*, pp. 231-245, 2009.

[18] J. Pavlich-Mariscal, L. Michel, and S. Demurjian, "Enhancing UML to Model Custom Security Aspects," in *Proc. 11th International Workshop on Aspect-Oriented Modeling*, 2007.

[19] A. Rodriguez, E. Fernandez-Medina, and M. Piattini, "Security requirement with a uml 2.0 profile," in *ARES '06: Proceedings of the First International Conference on Availability, Reliability and Security*, Washington, DC, USA, 2006, pp. 670-677.

[20] A. Rodriguez, E. Fernandez-Medina, and M. Piattini, "Towards a UML 2.0 Extension for the Modeling of Security Requirements in Business Processes," in *TrustBus*, pp. 51-61, 2006.

[21] W. Brooks and M. Warren, "Health information security evaluation: continued development of an object-oriented method," in *Proc. 2nd Australian Information Security Management Conference, Perth*, Western Australia, 2004, pp. 135-150.

[22] C. Raistrick, "Applying MDA and UML in the Development of a Healthcare System," N. Jardim Nunes *et al*. (Eds.): UML 2004 Satellite Activities, LNCS 3297, Springer-Verlag Berlin Heidelberg, 2005, pp. 203-218.

[23] R. Gomes and L. V. Lapão, "The adoption of IT security standards in a healthcare environment," in *Proc. MIE2008, Studies in Health Technology and Informatics*, vol. 136, pp. 765–770, 2008.

[24] *HIPAA Security Series- Security Standards, CMS – Centers for Medicaire & Medicaid Services*, vol. 2, pp. 2-5, 2007.

[25] S. Kokolakis and C. Lambrinoudakis, "ICT Security Standards for Healthcare Applications," *UPGRADE*, vol. 6, no. 4, August 2005.

Abdelhay Haqiq was born on April 5, 1986 in Rabat (Morocco). He received Master degree in computer Engineering from ENSIAS (National Higher School for Computer Science and System Analysis), Rabat, Morocco, 2010. Since 2011 he is a Ph.D. candidate at ENSIAS, member of AL-QualSADI research team (Quality of Software Architectures, their Development and Integration). His field of interest includes information systems, UML Profile, Multi-Agent and formal specification and verification of reactive systems.

Bouchaib Bounabat was born on March 8, 1966 in Marrakesh (Morocco). He is a Professor in ENSIAS, Rabat, Morocco. He received his Master degree in Computer science from Faculty of Science and Technology, Lille 1, French, 1989, Master of Advanced Studies in Engineering Sciences, Paris XII, 1990, and Ph.D. in Computer Sciences from Institut National des T đ écommunications, 1993.

He is Responsible of "Computer Engineering" Formation and Research Unit in ENSIAS, International Expert in ICT Strategies and E-Government to several international organizations, Member of the board of Internet Society - Moroccan Chapter. His research interests include Quality of software architectures, Software Engineering Methodology and formalization, generic infrastructure development and integration.