MODEL-BASED SECURITY ANALYSIS OF HEALTH CARE NETWORKS

Breu R[1], Innerhofer-Oberperfler F[1], Mitterer M[1], Schabetsberger T[2], Wozak F[2]

Abstract

In this position paper we present basic concepts and requirements of a model-based method targeted towards the security analysis of health care networks.

1. Introduction

The realization of shared electronic health data records (SEHRs) is commonly recognized as an important factor for advancements in health care [6]. Many models for the realization of SEHRs have been proposed and implemented. An example of a government initiative is NICTIZ in the Netherlands [10]. Other models propose independent Health Record Banks [14] or patient-managed EHR infrastructures [12]. This paper is written in the context of the project health@net, an Austrian initiative to develop concepts and an implementation of distributed cross-institutional health data records [16], [13].

Independent of the underlying model *security* is one of the key factors for the success and social acceptance of a SEHR infrastructure. In the sequel we will use the term *health care network* to denote any of these kinds of systems targeted to support workflows between stakeholders in the health care domain. Security requirements of health care networks are closely related with strict legal regulations and social matters. Most important this comprises confidentiality and integrity of health data, and rules for authentication and authorization, but also sophisticated objectives like the right of the patient to control his or her data and the possibility to delegate rights.

The solutions to these complex security requirements have to be realised in environments which are even more complex due to the following factors.

- The stakeholders involved are highly heterogeneous in their kind of organisation and security-awareness (hospitals, surgeries)
- The high number of stakeholder instances (e.g. millions of patients, thousands of surgeries) require complex infrastructures (e.g. for electronic signature)

[1] Research Group Quality Engineering, Institute of Computer Science, University of Innsbruck

[2] Research Division for eHealth and Telemedicine, University of Health Sciences, Medical Informatics and Technology, Hall in Tirol

- The networks are highly dynamic, both concerning stakeholder instances, stakeholder types and workflows to be run

- The available technical platforms (IHE IT Infrastructure Technical Framework [8]) and standards (Web Services, Web Service Security [15], [17]) are not yet stable and require constant further system development

Our claim is that it is of vital interest for all stakeholders to accompany the development of a health care network by a systematic security analysis. Taking into account the factors stated above the main requirement to the security analysis method is modularity. More precisely, *modularity* of the analysis method addresses the following aspects.

- Different levels of abstraction can be analysed independently of each other (e.g. separating health care oriented requirements from technical requirements)

- Different subdomains can be analysed independently of each other (e.g. separating the analysis of the organizational structure of hospitals and surgeries)

- The notions of requirements, risks and safeguards are clearly separated and may be analysed independently of each other (e.g. requirements to surgeries may be stated in early stages, whereas the implementations are available in later stages)

Currently we are developing a security analysis method meeting these requirements and targeted towards health care network applications. Our method is *model-based* in the sense that the analysis of security requirements, risks and safeguards is driven by models describing functional system views. The rest of this position paper is structured as follows. Section 2 gives a short overview of state of the art. In Section 3 we present the basic concepts of our approach with examples and Section 4 gives a conclusion and identifies next steps.

2. State of the Art

Our work is based on our experiences in the field of Model-Based Security Engineering. In [5] and [9] we defined a software process integrating aspects of security. The approach presented in this paper reuses some of the core artefacts and the security meta model of this security process but focuses on service oriented systems. In [7] we presented SECTET, a framework for Model-Driven Configuration of Security-Critical B2B-Work-flows. In this paper we rely on the SECTET model views but focus on security analysis rather than on software construction.

The OCTAVE [2] method uses a three phase approach to identify and manage information security risks. This comprises the identification of critical assets, threat analysis and security strategy planning. OCTAVE provides strong support for the overall process and management aspects whereas our approach focuses on the systematic integration of modeling artefacts and security analysis. In this respect OCTAVE could perfectly be used complementarily to our approach.

An approach that is following a model-based risk analysis is CORAS [4]. CORAS uses UML models mainly for descriptive purposes to foster communication and interaction during the risk analysis process. A strength of CORAS are the methodological foundations on which it is built, like Failure Trees, Event Trees, HazOp and Failure Mode Effect Analysis (FMEA), that help to identify vulnerabilities and threats. To depict identified assets, sources of threats and threats CORAS uses dia-

grams inspired by UML. Our method uses text-based representation of threats and security requirements but supports a security analysis process driven by the functional system properties.

Blobel and Roger-France [3] developed an approach to design and analyse secure health information systems. They identified abstract use cases and security concepts present in such scenarios. They also follow a modular approach and provide abstract solutions for security services that can be combined to build more complex architectures. Our method differs in the respect that we focus much more on the underlying process and the conceptual and methodological issues related with the identification and analysis of security properties inherent in a distributed health care network.

3. Basic Concepts

Security requirements often have been categorised along the notions of confidentiality, integrity and availability [11]. We agree with this or similar other classification but stress that the security requirements have to be put into context with the functional system requirements. In Subsection 3.1 we shortly present our system view targeted towards the modeling of heterogeneous distributed systems. In Subsection 3.2 we enhance this view by security related concepts and sketch the analysis process in Subsection 3.3.

3. 1. The Functional Models

We identified four different views modeling the functional aspects of health care networks. These views are classified along two orthogonal strands. *Table 1* shows the core models along this classification.

- *Level of Interaction*: The *Workflow View* describes aspects related with the interaction of different stakeholders (i.e. autonomous partners in the network), whereas the *Endpoint View* describes aspects related with the behaviour and structure of a specific stakeholder (like a hospital or a surgery).

- *Level of Abstraction*: The *Business View* describes the requirements at business level and consists of common model types like Process Model, Class Model, Organizational Model and Interface Model [5]. The *Application View* concentrates on the description of the solution and is described by the Software Architecture.

Table 1: Functional System Views

	Business View	*Application View*
Workflow View (WV)	WV Business Model	WV Software Architecture
Endpoint View (EV)	EV Business Model	EV Software Architecture.

As an example, *Figure 1 (a)* shows portions of the WV Business Model modeling a case of emergency (Workflow Business View). *Figure 1 (b)* is a schematic WV Class Model describing the structure of the health record (Workflow Business View) and *Figure 1 (c)* sketches the logical components of the health@net system (Workflow Application View).

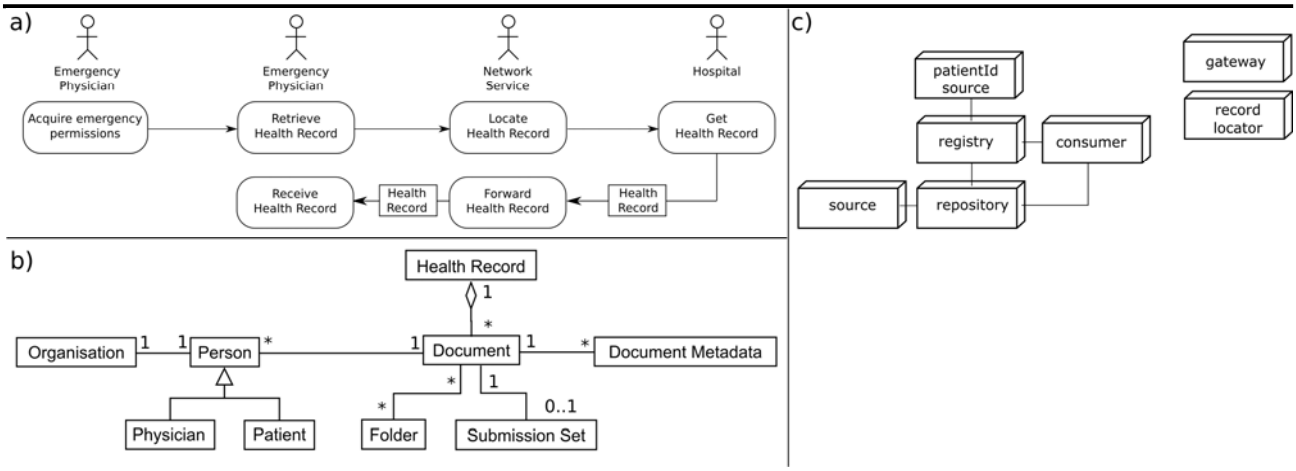

Figure 1: Health@net - Functional Models

3. 2. Security Concepts

In our framework the security analysis is tightly integrated with the Functional Model Views. In particular we associate model elements in the Functional Models (like classes in the Class Model and actions in the Process Model) with security related information as shown in *Figure 2*.

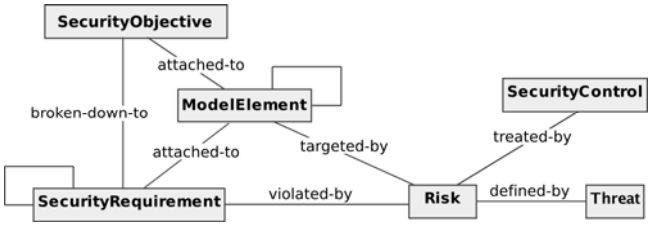

Figure 2: Meta-Model of Security Concepts

A *Security Objective* describes the overall security goals of the system, in particular general legal requirements, specific availability and integrity requirements of various institutions and privacy requirements of patients. Security Objectives are defined for a set of model elements that are dependent on each other.

A *Security Requirement* is a detailed context-dependent explication of a Security Objective. It breaks a Security Objective down in several more detailed descriptions. The context of a Security Requirement is derived from the model element for which it is defined. Security Requirements are linked to Security Objectives to depict paths of inheritance. Security requirements may be described informally by text, but we also provide a formal language for specifying dynamic access rights [1] and an UML Profile to integrate security requirements directly in the Functional Models [7].

A *Threat* is the description of an adverse event that is considered as potentially having a negative impact. A Threat by itself is not interesting for our analysis; it only becomes relevant, if we further identify a targeted model element and a related security requirement. Once the threat has been assessed and estimated regarding its impact, it becomes a risk.

A *Risk* is therefore defined as a triplet consisting of a targeted model element, a related security requirement and a threat that potentially undermines the requirement.

A *Security Control* is any measure or control in place to mitigate the identified risks.

At each point during the security analysis, the system is described by a set of interrelated model elements, where these model elements either adhere to the Functional Model Types of *Table 1* or to the Security Meta Model of *Figure 2*. We call each such set of interrelated model elements Security Model.

3. 3. The Security Analysis Process

The task of the Security Analysis Process is to support the security analyst in developing, evolving and analyzing Security Models. In particular, this process provides propagation rules for security related information along the functional model elements. In the sequel we sketch the main actions of the Security Analysis Process together with examples.

A1 - Select the Functional Model Element to be Analysed and Determine Model Context: This action refers to the modularity of the approach and sets the context for the security analysis.

Example 1: The security analysis may refer to the process of granting emergency permissions to a physician (c.f. *Figure 1*). In this context the focus is on the logical workflow between stakeholders and systems and its technical realization.

Example 2: From an Endpoint View the security analysis may refer to the local systems that are used in a hospital to access health data records in an emergency situation. The contexts are internal roles, the logical and technical Endpoint architecture.

A2 – Elicitate Security Objectives and Requirements: During security requirements engineering general security objectives attached with some model elements have to be defined. This overall security objective is then broken down into concrete requirements based on the model element's context and relations with other model elements. Therefore security requirements engineering is a top-down process driven by security objectives.

First example above: Security requirements will e.g. concern authentication and authorization of stakeholders and the availability and integrity of access and permission logs.

Second example above: Security requirements will e.g. concern internal physical and logical access control, internal usage and control of the lifecycle of the received health data record.

A3 – Analyse Threats and Evaluate Risks: A further action in the security analysis process is the identification of possible threats and the assessment of their impact – hence risk. A risk is always related to a model element and a security requirement. Threats are identified separately on the Workflow and on the Endpoint View. However the Endpoint View inherits the relevant security objectives, threats and risks that are defined on the workflow view.

First example above: The threats and risks of accessing confidential health data records by simulating an emergency access or by not adequately controlling the access and permission logs.

Second example above: The threats and risks of internal access control systems and rules that could lead to a non-authorized access to emergency health data records.

A4 – Identify and Evaluate Possible Security Controls: After threat identification and risk assessment have been completed the security analysts will propose various measures and controls to mitigate the identified threats and therefore protect the general security objectives.

First example above: Authentication mechanisms on the workflow level could prevent unauthorized connection and simulated emergency access to health data records. Later authorization of the emergency access by the respective patient combined with a process to control and check every emergency access can help to detect and reduce unauthorized access.

Second example above: Restricted physical access to the systems involved in processing emergency health data record requests and improved authentication mechanisms on the Endpoint for physicians.

4. Conclusion

In the preceding sections we have presented basic concepts and requirements of a framework for security analysis targeted to applications in health care. Main aspects of this framework are a tight integration of security analysis with the functional view of the system and the support of modularity concerning the chosen system context, level of abstraction and security aspects.

Since we presented current research most of the work has still to be done, in particular concerning

- support of health care applications through reference models (e.g. organizational models of hospitals) and security patterns (e.g. compliance objectives, requirements and threats)
- development of propagation rules for security related model elements along the dependencies of the Functional Model (e.g. Security Requirements of the Workflow View propagating to Security Requirements of the Application View)
- support for checking the state of a Security Model (e.g. concerning missing elements, consistency of the security related model elements)
- traceability of security related model elements (e.g. retrieving the technical threats related with a security requirement of a superior business model element)
- safeguards planning and evaluation
- information aggregation and report generation

Both the development of our method and future tool support are accompanied by our activities in the Austrian project health@net where our task is to develop and to realize security concepts for a national virtual distributed health record.

This work has been supported by health@net, coordinated at CEMIT - Centre of Excellence in Medicine and IT.

5. References

[1] ALAM, M., HAFNER, M., BREU, R., Constraint-Based Role-Based Access Control in the SECTET-Framework. Journal of Computer Security 16(2), 223-260, 2008.

[2] ALBERTS, C. J., DOROFEE, A. J., Managing information security risks: the OCTAVE approach. Addison-Wesley, Boston, 2002.

[3] BLOBEL, B., ROGER-FRANCE, F., A systematic approach for analysis and design of secure health information systems. International Journal of Medical Informatics, Elsevier Science, 62, 51-78, 2001.

[4] BRABER DEN, F.; HOGGANVIK, I.; LUND, M.; STØLEN, K.; VRAALSEN, F., Model-based security analysis in seven steps: a guided tour to the CORAS method. BT Technology Journal, Springer, 25, pages 101-117, 2007.

[5] BREU, R., BURGER, K., HAFNER, M., POPP, G., Towards a Systematic Development of Secure Systems. Information Systems Security 13(3), 2004, p.5-13.

[6] eEurope 2005, http://ec.europe.eu/

[7] HAFNER, M., AGREITER, B., BREU, R., NOWAK, A.., SECTET - An Extensible Framework for the Realization of Secure Inter-Organizational Workflows. Internet Research, Emerald Press, Inc, 2006.

[8] IHE.net: IT Infrastructure Technical Framework, Nov 2006, http://www.ihe.net/Technical_Framework/

[9] INNERHOFER-OBERPERFLER, F., BREU, R., Using an enterprise architecture for IT risk management. In Proceedings of the ISSA 2006 conference, ISBN 1-86854-636-5.

[10] NICTIZ – National IT Institute for Healthcare in the Netherlands. http://www.nictiz.nl/

[11] PELTIER, T. R., Information security risk analysis. Auerbach Publications Boston, MA, USA, 2001.

[12] RAMSAROOP, P., BALL, MJ., The Bank of Health: A Model for More Useful Patient records. MD Computing 17(4), 2000, 45-48.

[13] SCHABETSBERGER, T., AMMENWERTH, E., BREU, R., HOERBST A., GOEBEL, G., PENZ, R., SCHINDELWIG, K., TOTH, H., VOGL, R. AND WOZAK, F., E-Health Approach to Link-up Actors in the Health Care System of Austria. Stud Health Technol Inform, vol 124, 2006.

[14] SHABO, A., A Global Socio-Economic-Medico-Legal Model for the Sustainability of Longitudinal Electronic Health Records. Part 1. Methods of Information in Medicine 45 (3), 2006, 240-245.

[15] Web Service Security Specifications, available at http://www.oasis-open.org/

[16] WOZAK, F., AMMENWERTH, E., BREU, M., PENZ, R., SCHABETSBERGER, T., VOGL, R. AND WURZ, M., Medical Data GRIDs as approach towards secure cross enterprise document sharing (based on IHE XDS). Proc. of MIE2006., volume 124, pages 377–383, 2006.

[17] XACML 2.0 Specification, available at http://oasis-open.org/