Risk Assessment of a Cardiology eHealth Service in HYGEIAnet

N Stathiakis[1], CE Chronaki[1], E Skipenes[2], E Henriksen[2], E Charalambus[3], A Sykianakis[3], G Vrouchos[3], N Antonakis[4], M Tsiknakis[1], S Orphanoudakis[1, 5]

[1]Foundation for Research and Technology – Hellas (FORTH), Heraklion, Greece
[2]Norwegian Centre for Telemedicine (NST), Tromsø, Norway
[3]Venizelio Hospital, Heraklion, Greece
[4]Primary Healthcare Centre, Anogia, Greece
[5]University of Crete, Heraklion, Greece

Abstract

A Risk Assessment (RA) framework was employed to determine what protection would be adequate and reasonable for the assets of a cardiology eHealth service deployed on the island of Crete. In the context of HYGEIAnet, the regional health telematics network of Crete, teleconsultation services for cardiology patients have been installed and are in routine use since December 2000. The novelty of the framework for model-based RA of security critical systems, which developed within the CORAS IST project, lays in its synthesis of risk analysis methods with semiformal specification, supported by an adaptable tool-integration platform. This paper presents the use of the CORAS framework to assess the cardiology eHealth service and the implementation of security controls and mechanisms.

1. Introduction

Medical information is considered sensitive and requires protection since it is directly related to patient's health and safety. Security of data in medical applications is particular complex because patient data is typically fragmented, controlled by whoever provided health services. Moreover, the security mechanism must be arranged so that users can quickly share information in the event of an emergency. On the other hand many healthcare professional are reluctant to use information and communication tools due to the security risks entailed. This fact has delayed the acceptance of the new technology by the users and the routine use of the information systems and the telematics applications by the healthcare organizations. Finally, as stated at the Recommendation No. R (97) 5 on the Protection of Medical Data issued by the Council of Europe "appropriate technical and organizational measures shall be taken to protect personal data – processed in accordance with this recommendation - against accidental or illegal destruction, accidental loss, as well as against unauthorized access".

The cardiology eHealth service is based on WebOnCOLL [1], a web-based collaboration infrastructure that manages episode folders (TCFs) as shared workspaces. Each teleconsultation session is associated with a TCF that includes administrative information as well as relevant clinical data. Medical information comprises medical multimedia documents, such as reports, digitised x-rays, bio-signals, ECGs, progress notes, etc. The TCFs, the data they contain, and the other assets of the cardiology eHealth service should be effectively protected. CORAS framework was employed to identify and analyse possible security threats, to develop security specifications, and to design security policies.

CORAS is a European R&D project funded by the 5th framework program on Information Society Technologies (IST). The objective of CORAS is to develop a framework for precise, unambiguous and efficient RA of security critical systems. CORAS aims to combine methods for risk analysis and semiformal description methods, in particular methods for object-oriented modelling, together with computerized tools.

CORAS addresses security critical systems in general, but places particular emphasis on IT security. For CORAS, a system is not just technology, but also the humans interacting with the technology and all relevant aspects of the surrounding organisation and society. The use of graphical models in CORAS furthers communication between the different stakeholders of a RA, and makes it easier for non-technicians to take part.

2. The CORAS approach

The main result of the CORAS project is the CORAS framework. The framework is characterized by: (1) A careful integration of aspects from partly complementary

RA methods like HazOp [2], and Fault Tree Analysis (FTA). (2) Guidelines and methodology for the use of Unified Modeling Language (UML) [3] to support the RA methodology. (3) A risk management process based on the Australian standard for risk management AS/NZS 4360 and ISO/IEC 17799. (4) A risk documentation framework based on Reference Model for Open Distributed Processing (RM-ODP) [4]. (5) A platform for tool-inclusion based on XML.

The CORAS RA methodology [5,6] is model-based in the sense that models are used:

1. To describe the target of evaluation at the right level of abstraction.
2. As a medium for communication and interaction between different groups of stakeholders involved in a RA.
3. To document RA results and the assumptions on which these results depend.

Sub-process 1: Identify Context	**Sub-process 3: Analyse Risks**
1.1 Identify areas of relevance	3.1 Consequence evaluation
1.2 Identify and value assets	3.2 Frequency evaluation
1.3 Identify policies and evaluation criteria	**Sub-process 4: Risk Evaluation**
1.4 Review and approve	4.1 Determine level of risk
	4.2 Prioritise risks
Sub-process 2: Identify Risks	4.3 Categorise risks
2.1 Identify threats to assets	4.4 Determine interrelationships among risk themes
2.2 Identify vulnerabilities of assets	4.5 Prioritise the resulting risk themes and risks
2.3 Document unwanted incidents	**Sub-process 5: Risk Treatment**
	5.1 Identify treatment options
	5.2 Assess alternative treatment approaches

Figure 1. The CORAS risk management process.

The CORAS risk management process is sequenced into five sub-processes for context identification, risks identification, risks analysis, risks evaluation, and risks treatment. In addition, there are two sub-processes, which are running in parallel with the other five, and targeting communication and consultation as well as monitoring and reviewing. Each of the five main sub-processes comprises a number of activities, as illustrated by Fig. 1. Different risk analysis methods and semiformal model types are proposed for the different sub-processes and activities. The CORAS methodology also gives proposals for documentation and communication of the RA results. CORAS provides a computer-based platform including a database for structuring the input to and the results of the RA. Using this platform the results can easily be structured, sorted, retrieved and reused as desired.

3. Using CORAS for risk assessment of the cardiology eHealth service

The CORAS RA of the cardiology eHealth service took place in the period December 2002 – March 2003. The first months were used for preparatory work. The main RA session was performed at a seven-day meeting and involved RA experts, and service stakeholders i.e. healthcare professionals and computer engineers. The time period after the meeting was used for analyzing and structuring the RA results. This section presents the five sub-processes of the CORAS model-based RA methodology that was used to identify and evaluate the unwanted incidents, through examples from this RA.

3.1. Context identification

Most of the activities in sub-process 1 were performed as preparatory work before the RA meeting. Included in this preparatory work was a first meeting with the medical doctors. The first activity was to describe the system and its environment. The system was described informally in different ways, e.g. in plain text, by use of pictures or illustrations, and by use of prototypes or simulations. The system was also described by use of semiformal modelling techniques. Different types of UML diagrams were used without problems. All participants in the RA of the cardiology eHealth service, both the system engineers and the medical doctors, were familiar with the system we analysed and had a good understanding of the functionality of the system and the information flow. This made it easier for the non-technicians to understand the abstractions of the semiformal models.

The second activity of the context identification was to identify and value assets in order to know what to protect. The different stakeholders were asked to identify assets of interest to them and assign a value indicating its level of importance. Patient care, user password, the medical request including clinical, laboratory, and ECG data, as well as the medical advice were among the assets of great value for cardiology eHealth service. The third activity of the context identification was to identify security policies and requirements, and to decide on corresponding risk evaluation criteria. In the RA of the cardiology eHealth service this was done in the preparatory meeting by the doctors and the system engineers together. In that meeting they also decided to group the security

requirements according to importance or priority.

3.2. Risk identification

The first activity of this sub-process was to identify threats to assets. In the RA of the cardiology eHealth service we mainly used HazOp, a structured brainstorming method: for each of the assets we identified threats by the help of predefined guidewords. The results were documented in a HazOp-table. Other methods used in CORAS for threat identification were FTA (Fault Tree Analysis) and FMECA (Failure Mode and Effect Criticality Analysis). In the second activity the vulnerabilities of the assets to threats were identified by using predefined questionnaires. In addition, a vulnerability assessment tool was installed in the network. In the third activity of this sub-process we combined vulnerabilities with the identified threats in order to identify 22 unwanted incidents. UML diagrams such as Use Case, Activity and Sequence diagrams facilitated the overall process. The unwanted incidents concerned the security aspects of data confidentiality and integrity, and service availability and were documented in UML diagrams as illustrated by fig. 2.

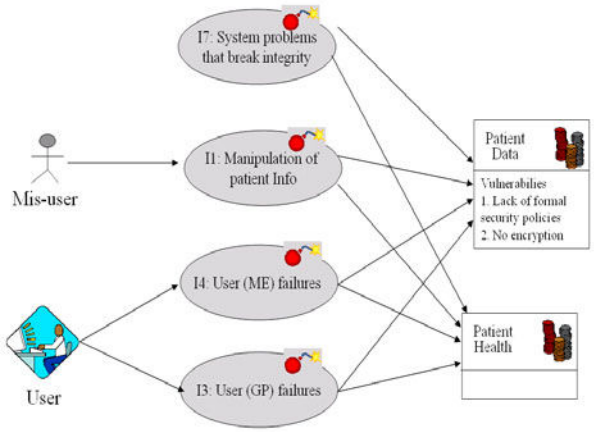

Figure 2. Integrity unwanted incidents and affected assets.

3.3. Risk analysis

Before assigning likelihood and consequence values for each of the unwanted incidents in the HazOp table, the stakeholders defined the consequence levels and the likelihood levels to be used. In our trials this was done as part of the preparatory work before the RA meeting. Predefined consequence and likelihood levels are a prerequisite for being able to agree on consequence and likelihood values, and to achieve approximately the same interpretation of these values. Finally, the relevant stakeholders assigned values for likelihood and consequence to each unwanted incident in the HazOp table. These values were documented in an extended HazOp table, where new columns were added as needed.

3.4. Risk evaluation

The first activity of this sub-process was to determine the risk level of each risk. This was done by placing the unwanted incidents in a risk level matrix, in the cell corresponding to the likelihood and consequence values that were given to this incident. The four different risk levels were indicated by different shading in the matrix. As part of the preparatory work before the RA meeting, the stakeholders defined the risk levels. An example of the risk level matrix is presented in table 1.

Table 1. Example of the risk levels that identified during RA.

Conse-quence	**Frequency**				
	Rare	Un-likely	Poss-ible	Likely	Almost certain
Minor	I2 I6	I5			
Moderate	C2 C7	A2 A4	A1	C5	
Major	I1 I4	C8 I3			

No unwanted incidents were identified to have ‘extreme risk’ level. ‘High risk’ value was assigned to 3 unwanted incidents and ‘moderate risk’ to 11. ‘High’ risks included data confidentiality threats at the cardiologist’s side and at the service centre side, as well as data integrity threats related to the medical request submitted. The second activity of this sub-process was to prioritise the identified risks. The prioritisation was closely related to the risk levels. Other activities of this sub-process were categorization of risks into risk themes and identification of relationships between themes. The aim was to make the risk treatment more effective. Instead of treating each risk alone, it was cost-effective to devise treatment for a theme of risks at the same time. There were, however, a few remaining risks that did not fit into any of the themes. These risks were treated separately.

3.5. Risk treatment

The purpose of this sub-process was to propose and evaluate treatment options for the identified risk themes and single risks. An initial list of treatment approaches was identified. Different approaches could be: risk avoidance, reduction of likelihood, reduction of consequence, risk transfer, and risk retention. The treatment options were grouped into four categories:

security policies and procedures, user training, security mechanisms and other software/hardware improvements. For each risk theme or single risk we tried to identify and describe at least one treatment option within each treatment approach, and describe the possible benefits and cost for this treatment. The final prioritization and selection of treatment was the responsibility of the service stakeholders, based on a cost-benefit assessment of the proposed treatment.

4. Discussion

During the trial session, risks and risk themes were determined and treatment options were suggested for successfully dealing with them. Each treatment option required the adoption of a specific implementation policy, which was associated with a cost, expressed in terms of time and financial funding. In particular, four security treatment categories were studied:

- Definition security policies and operational routines.
- User training.
- Implementation of security mechanisms.
- Other improvements of software and hardware.

For the efficient management and avoidance of the risks mentioned above, special measures were proposed. Particular emphasis was given on data confidentiality threats. Five security treatments were selected for implementation. The treatments, as shown in table 2, varied from definition of security policies to user training and development of security mechanisms.

Table 2. Implemented security treatments for the identified risks.

Security Treatments	C1	C3	C10	I1	A3
Security policy	x	x		x	x
Password policy	x	x		x	
Timeout policy		x		x	
User Training	x	x		x	x
Secure server & https			x		

The implementation of the security treatments decreased the frequency of the confidentiality risks, while the additional implementation cost was of the order of 5500 euros. Assuming that the service is being used 50 times per year, the expected number of violations in data confidentiality was reduced from 9 to 1.85 times annually.

5. Conclusion

The RA of the cardiology eHealth service demonstrated and evaluated the applicability and usability of the CORAS framework and its efficiency in identifying, analyzing and documenting security risks.

The CORAS methodology and approach contributed a lot in the definition and identification of new risks as well as in their effective treatment. In particular, CORAS helped both doctors and system engineers to identify and satisfy their needs in a cost effective way. An investment of 5500 euros in implementing security treatments reduced the expected frequency of violations in data confidentiality from 18 % to 3.7%.

CORAS' structure using consecutive activities makes risk analysis results easier to reuse in whole or in part, thus lowering the cost of assessing other eHealth services in HYGEIAnet regional network.

Acknowledgements

The work reported in this paper was supported by the CORAS, a European R&D project funded by the 5th framework program on Information Society Technologies (IST-2000-25031). The CORAS consortium consisted of eleven partners from industry, research and academia in four European countries: CTI (Greece), FORTH (Greece), IFE (Norway), Intracom (Greece), NR (Norway), NST (Norway), QMUL (UK), RAL (UK), SINTEF (Norway), Solinet (Germany), and Telenor (Norway). The results reported in the paper benefited from joint efforts of the whole consortium.

References

[1] Chronaki CE, Kostomanolakis SG, Lelis P, Lees PJ, Chiarugi F, Tsiknakis M. Integrated Teleconsultation Services In Cardiology. Computers in Cardiology 2000; 27:175-178.

[2] Leveson, NG. SAFEWARE, System, Safety and Computers. Addison-Wesley, 1995.

[3] Rumbaugh J, Jacobson I, Booch G. The Unified Modeling Language, Reference manual. Addison-Wesley, 1999.

[4] Putman JR. Architecting with RM-ODP. Prentice-Hall, 2000.

[5] den Braber F, Dimitrakos T, Gran BA, Lund MS, Stølen K, Aagedal JØ. The CORAS methodology: model-based risk management using UML and UP. Liliana F, editor. Chapter in book UML and the Unified Process. IRM Press, 2003: 332-357.

[6] Fredriksen R, Kristiansen M, Gran BA, Stølen K, Opperud TA, Dimitrakos T. The CORAS framework for a model-based risk management process. In Proc. Computer Safety, Reliability and Security 2002. Springer, 2002:94-105.

Address for correspondence.

Nikos Stathiakis
Center for Medical Informatics and Health Telematics Applications, Institute of Computer Science, FORTH
P.O. 1385 Heraklion, Crete, 71110 Greece