The New Navigators: from Professionals to Patients
R. Baud et al. (Eds.)
IOS Press, 2003

The CORAS approach for model-based risk management applied to a telemedicine service

Yannis Stamatiou[a], Eva Skipenes[b], Eva Henriksen[b], Nikos Stathiakis[c], Adamantios Sikianakis[d], Eliana Charalambous[d], Nikos Antonakis[e], Ketil Stølen[f], Folker den Braber[f], Mass Soldal Lund[f], Katerina Papadaki[g], George Valvis[g]

[a]Computer Technology Institute (CTI), Patras, Greece
[b]Norwegian Centre for Telemedicine (NST), Tromsø, Norway,
[c]Foundation for Research and Technology – Hellas (FORTH), Heraklion, Greece,
[d]Venizelio Hospital, Heraklion, Greece,
[e]Primary Healthcare Centre, Anogia, Greece,
[f]SINTEF Telecom and Informatics, Norway, [g]Solinet, Germany

Abstract

The CORAS risk management process is based on the Australian standard for risk management and aims at improved methodology for precise, unambiguous, and efficient risk assessment of security critical systems. 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 risk assessment, and makes it easier for non-technicians to take part. Telemedicine services and electronic applications used in the health sector have a high demand for security. The medical developers, providers and users of such services and systems are important contributors in the risk assessment of these services and systems. CORAS has successfully been used to involve medical professionals in the model-based risk assessment of a telemedicine system called Tele-cardiology in Crete. This paper presents the use of the CORAS framework to assess this telemedicine system giving some conclusions on the experience gained.

Keywords:

Risk assessment; Risk management; Data security; Semiformal modelling; Tele-consultation

1. Introduction

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 risk analysis 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.

The CORAS model-based risk assessment methodology makes use of semi-formal modelling for three different purposes: (1) To describe the target of evaluation at the right level of abstraction. To properly assess security technical system documentation is not sufficient; a clear understanding of system usage and its role in the surrounding organisation or enterprise is just as important. Semi-formal modelling allows these various aspects to be documented in a uniform manner. (2) To facilitate communication and interaction between different groups of stakeholders involved in a risk assessment. One major challenge when performing a risk assessment is to establish a common understanding of the target of evaluation, threats, vulnerabilities and security risks among the stakeholders

participating in the assessment. CORAS aims to facilitate improved communication during security assessments, by making the semi-formal models easier to understand for non-experts, and at the same time keeping them well-defined. (3) To document risk assessment results and the assumptions on which these results depend to support reuse and maintenance. Risk assessments are costly and time consuming and should not be initiated from scratch each time a new or modified system is assessed. CORAS supports reuse of assessment documentation, both for systems that undergo maintenance and for new systems, if similar systems have been assessed earlier.

During the development of the CORAS model-based risk assessment methodology, the framework is tested through extensive trials within telemedicine and within e-commerce. This paper presents a trial of CORAS on a telemedicine service in Crete.

2. The CORAS risk management process

The CORAS risk management process is based on AS/NZS 4360, the Australian standard for risk management [1] and on the international standard ISO/IEC 17799 [2]. The CORAS risk management process is divided into five sub-processes for context identification, risks identification, risks analysis, risks evaluation, and risks treatment. In addition, there are two implicit sub-processes running in parallel with these five, targeting communication and consultation as well as monitoring and review. Each of the five main sub-processes comprises a number of activities. Different risk analysis methods and semiformal model types are proposed to be used for the different sub-processes and activities. The CORAS methodology also gives proposals for documentation and communication of the risk assessment results. CORAS provides a computer-based platform including a database for structuring the input to and the results of the risk assessment. By use of this platform the results can easily be structured, sorted and retrieved as desired. For details on the overall CORAS approach we refer to [3].

3. Using CORAS for risk assessment of a telemedicine service

The telemedicine service which has been the target for one of the risk assessments in the CORAS trials is a web-based collaboration service within Tele-cardiology in Crete. When a general practitioner at a remote Primary Healthcare Centre has a patient with acute chest pains, this Tele-cardiology service can be used to send a medical request to a cardiologist at the hospital. The service takes the necessary steps to alarm the cardiologist on duty. The medical request from the general practitioner contains a description of the patient and his condition, with all necessary information, such as digital ECG, blood pressure values, X-ray images. The information is stored in a central web-server, where the alarmed cardiologist can read the same information. The cardiologist provides his advice via the same web-server. The web-based infrastructure, "WebOnColl", is developed by FORTH (Foundation for Research and Technology – Hellas).

A first risk assessment of this Tele-cardiology service was performed in the summer of 2002. Both technical and medical providers of the service were able to take part in the risk assessment. The assessment resulted in the identification of 97 unwanted incidents. This section presents the five sub-processes of the CORAS model-based risk assessment methodology that was used to identify and evaluate the unwanted incidents, through examples from this risk assessment.

Sub-process 1, Context identification: Most of the activities in sub-process 1 were performed as preparatory work before the risk assessment meeting. Included in this preparatory work was a first meeting with the medical doctors. The first activity is to describe the system and its environment. The system can be 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 can also be described by use of semiformal modelling techniques. Different types of UML diagrams were used without problems. All participants in the risk assessment of the Tele-cardiology system, both the technical developers 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 is to identify and value assets in order to know what to protect. The different stakeholders were asked to identify assets relevant to them and to give each of their assets a value indicating its level of importance. The third activity of the context identification is to identify security policies and requirements, and to decide on corresponding risk evaluation criteria. In the risk assessment of the Tele-cardiology service this was done in the preparatory meeting by the doctors and the system developers together. In this meeting they also decided to group the security requirements according to importance or priority.

Sub-process 2, Risk identification: The first activity of this sub-process is to identify threats to assets. In the risk assessment of the Tele-cardiology service we mainly used HAZOP – a structured brainstorming method: for each of the *assets* we identify *threats* by the help of predefined *guidewords*. Where possible, we also described the consequences of these threats. The results were documented in a HAZOP-table. Other methods used in CORAS for threat identification FTA(Fault Tree Analysis) and FMECA(Fault Tree Analysis) [include references]. In the second activity the vulnerabilities of the assets to threats were identified a separate meeting with the technical developers, 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 *unwanted incidents*, that will be later analysed as *risks*.

Sub-process 3, Risk analysis: Before assigning likelihood and consequence values for each of the unwanted incidents in the HAZOP table, the stakeholders should define the consequence levels and the likelihood levels to be used. In our trials this was done as part of the preparatory work before the risk assessment 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.

Sub-process 4, Risk evaluation: The first activity of this sub-process is to determine the risk level of each risk. This is 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 are indicated by different shading in the matrix. As part of the preparatory work before the risk assessment meeting, the stakeholders defined the risk levels. The second activity of this sub-process is to do a prioritization among the identified risks. This should be done in cooperation with the stakeholders. The prioritization should be closely related to the risk levels. Other activities of this sub-process are categorization of risks into risk themes and identification of relationships between risk themes. The purpose is to make the risk treatment more effective. Instead of treating each risk independently it could be cost-effective to devise treatment for a theme of risks at the same time. There will, however, often be a few remaining risks that do not fit into any of the risk themes. These single risks will have to be treated separately. Another activity that is useful for the risk treatment sub-process is the prioritization of the risk themes. To be able to do such a prioritization, the risk themes are assigned a risk value based on the risk levels of the associated risks.

Sub-process 5, Risk treatment: The purpose of this sub-process is to propose treatment options for the identified risk themes and single risks. An initial list of treatment approaches is identified. Different approaches to treatment could be: Risk avoidance, Reduction of likelihood, Reduction of consequence, Risk transfer, and Risk retention. For each risk theme or single risk we then try 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 will be the responsibility of the stakeholders, based on a cost-benefit assessment of the proposed treatment.

4. Evaluation of the methodology and the trial's contribution to stakeholders

The experimental risk analysis session described in this paper aimed at applying and assessing the CORAS risk management process and platform within the telemedicine domain. The main idea for the telemedicine trial was for the trials team of CORAS to interact with the stakeholders of the target telemedicine platform to fulfill the following goals : (I) Involve all stakeholders in the risk assessment process to uncover threats to their application (II) Educate the participating doctors in risk analysis concepts and equip them with risk-avoidance awareness for the applications they use for their daily duty (III) Provide the CORAS development team with useful feedback in order to produce an improved version of the CORAS framework.

Regarding the first goal, medical professionals participated and gave valuable input to the risk assessment. In addition, the technical team of FORTH that took part in the risk assessment found the CORAS component methods and models very useful for the detection and categorization of the various problems extant in the platform, especially FTA for its structure and FMEA for its detail.

As for the second goal, the literature shows that the management of information security is inadequate and levels of awareness regarding security issues are low in healthcare environments. The findings of the SEISMED (Secure Environment for Information Systems in MEDicine) survey in security awareness highlighted the low awareness of security issues and proposed means for improving security in medical situations [10]. In health organisations in the UK it was noted that even the lowest levels of security measure were not always in place [8]. The nature of risks in a changing health-care environment is unique [9]. Information security in the health care industry is not purely a technical issue, with social and organisational factors also playing a major part [6]. The concept of user responsibility for information security is still in its infancy. CORAS, by enabling the wide participation of system users in the risk assessment process encourages them to accept responsibility and ownership of information security within their work environment [7]. The idea was that the CORAS project should offer to the participating doctors an education in risk analysis in order to (i) get them to know better the potential threats that can possibly materialize because of some involuntary action of them (ii) provide them with some knowledge in order to avoid some of the risks in which their platform is exposed, and (iii) possibly increase their confidence in formal risk analysis methodologies as a means of providing to them secure applications. The participating doctors agreed that after the trial session they understood far more about their Tele-cardiology application and how it can be exposed to threats than before.

With regard to the third goal, an assessment of the CORAS methodology is being done in parallel with the trials, and feedback is given back to the project for the further refinement and development of the methodology. A full evaluation of the CORAS model-based risk assessment methodology has not yet been performed, but some intermediate discoveries can be mentioned. Prior to the trials of the methodology, the CORAS project

defined evaluation criteria within four main evaluation categories. Briefly, these categories as well as summaries about how well CORAS did along each of them are given below:
Applicability – easiness for CORAS to address diverse types of applications. In parallel to the telemedicine trials, the CORAS project team conducted similar risk analysis sessions in the e-commerce domain where the target was a platform that is used in order to advertise and sell goods through Internet. In both the telemedicine and the e-commerce domains the risk analysis teams observed that all security requirements (availability, integrity, confidentiality and non-repudiation) could be modelled and handled with the same easiness.
Effectiveness – the precision and clarity with which the risk analysis sessions proceed. One of the main strengths of CORAS is the integration of different types of target system models for each type of activity and risk analysis methodology. In relation to the models used during the Tele-cardiology trial, the medical professionals were, generally, in position to understand the information conveyed by them. This was also facilitated by the fact that the doctors took part in preparatory meetings before the trial session and they had already used the target application in real situations. Especially for the sequence diagrams they commented that they are useful in order to explain to them what happens at a low level during the transfer of information related to their patient.
Performance – the effort and time required to understand and apply CORAS and the savings when CORAS is applied in early stages of system development or the maintenance phase. Along this criterion the CORAS framework demonstrated some deficiencies that, however, were natural to be there during this stage of development of the framework and which are being taken care of by the CORAS technical team. However, the main problem in all risk assessments is to find time for meetings, i.e. a time when all participants are available. This is particularly difficult with doctors who are occupied with patient treatment and other duties. An important characteristic of risk assessments is the involvement of stakeholders with different backgrounds and, thus, communication between the different stakeholders was always a critical issue. In particular, the trial highlighted the need for methodology and guidelines for how to reach a consensus among the involved stakeholders.
Usability – the readiness with which the CORAS risk analysis methods and results can be documented and understood by stakeholders. During the risk analysis session, the participation from medical professionals and technical people alike was very intense and they could take part in the discussions related to the risk analysis of the Tele-cardiology platform as well as contribute ideas to it. More specifically, driven by the chosen guidewords in the HazOp table the medical professionals were able to state specific threats that they know about, or think about their causes and consequences.

We experienced a great need for a platform for structured documentation of the input and the results of the risk assessment. Thus, the CORAS platform entails a significant added value to the risk management process.

5. Conclusions (Further/remaining work)

There are other approaches to model-based risk assessment; see for instance CRAMM, ATAM, SA and RSDS [include references]. The particular angle of the CORAS approach with its emphasis on security and risk assessment tightly integrated in a UML and RM-ODP is however new. In particular, the issue of maintenance and reuse of assessment results has received very little attention in the literature.

Since 1990, work has been going on to align and develop existing national and international schemes in one, mutually accepted framework for testing IT security functionality. The Common Criteria (CC) [4] represents the outcome of this work. The Common Criteria project harmonises the European "Information Technology Security Evaluation Criteria (ITSEC)" [5], the "Canadian Trusted Computer Product Evaluation

Criteria (CTCPEC)" and the American "Trusted Computer System Evaluation Criteria (TCSEC) and Federal Criteria (FC)". The CC is generic and does not provide methodology for security assessment. CORAS, on the other hand, is devoted to methodology for security assessment. Both the CC and CORAS places emphasis on semiformal and formal specification. However, contrary to the CC, CORAS addresses and develops concrete specification technology addressing security assessment. The CC and CORAS are orthogonal approaches. The CC provides a common set of requirements for the security functions of IT products and systems, as well as a common set of requirements for assurance measures applied to the IT functions of IT products and systems during a security evaluation. CORAS provides specific methodology for one particular kind of assurance measure, namely security risk assessment

The integration of modelling and risk assessment methodology that is done by the CORAS project is beneficial for risk management for several reasons: It improves the risk analysis itself since the understanding of the target of evaluation is enhanced by precise specifications of how it is structured and how it behaves. The precision level is improved by introducing semiformal notations. In addition, a model-based risk assessment facilitates communication, both internally between the actors involved during risk assessment and externally to the stakeholders.

6. Acknowledgements

CORAS is a European R&D project funded by the 5th framework program on Information Society Technologies (IST-2000-25031). The CORAS consortium consists 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 have benefited from joint efforts of the whole consortium.

7. References

[1] Australian Standard (1999). *Risk management.* AS/NZS 4360:1999.
[2] ISO/IEC 17799:2000 Information technology – *Code of practise for information security management*
[3] den Braber, F., Dimitrakos, T., Gran B. A., Lund, M.S., Stølen, K., Aagedal, J.Ø. *The CORAS methodology: model-based risk management using UML and UP.* Chapter in book titled UML and the Unified Process. IRM Press, 2003.
[4] Information technology security evaluation criteria (ITSEC), version 1.2, Office for Official Publications of the European Communities, June 1991.
[5] ISO/IEC 15408:1999 Information technology – Security techniques – Evaluation criteria for IT security
[6] Anderson, J.G., 1997, *"Clearing the Way for Physicians' use of Clinical Information Systems"*, Communications of the ACM, Vol 40 no 8, pp 83-90.
[7] Armstrong H, 2000, *'Managing Information Security in Healthcare - an Action Research Experience'*, SEC 2000.
[8] Barber B., Davey, J., 'Risk Analysis in Health Care Establishments', in Barber, Treacher, Louwerse, (Eds), *"Towards Security in Medical Telematics"*, IOS Press, Amsterdam, pp 120-124, 1996.
[9] Smith, E. & Eloff, J., *'Modelling Risks in a Health-Care Institution'*, Proceedings of the XV IFIP World Computer Congress, Vienna/Budapest, September 1998.
[10] Treacher, A. Bleumer, G., *'An Overview of SEISMED'*, in Barber, Treacher & Louwerse, (Eds), *"Towards Security in Medical Telematics"*, IOS Press, Amsterdam, pp 4-9, 1996.

8. Address for correspondence

Yannis C. Stamatiou, Computer Technology Institute, Riga Feraiou 61, Patras, Greece.
e-mail: stamatiu@cti.gr
For more about CORAS, please visit the project's site http://www.nr.no/coras, contact the technical manager Ketil Stølen (ketil.stolen@sintef.no) or contact the project manager Tony Price (price@transtrad.com).