Model based risk management of security critical systems

I. Djordjevic¹, C. Gan¹, E. Scharf¹, R. Mondragon¹, B. A. Gran², M. Kristiansen², T. Dimitrakos³, K. Stolen⁴ & T. A. Opperud⁵

¹ Department of Electronic Engineering, Queen Mary, University of London, UK
² Institute for Energy Technology, Halden, Norway
³ CLRC Rutherford Appleton Laboratory, Oxfordshire, UK
⁴ Sintef Telecom and Informatics, Oslo, Norway
⁵ Telenor Communications AS R&D, Fornebu, Norway

Abstract

This paper describes a novel framework for a risk management process involving a model-based approach, developed as the main objective of CORAS (IST-2000 25031). The main motivation for this approach is to achieve an improved methodology for precise, unambiguous, and efficient risk analysis of security critical systems. There are several benefits from a model-based approach. Firstly, the description of the target system, its context and all security relevant features required for risk analysis, can be improved by applying state-of-the-art modelling technology. Secondly, it provides a rich set of graphical descriptions that address properties of the target system as well as their context (including the behaviour of humans), which improves communication and interaction between stakeholders involved in a risk analysis and also facilitates the formalization of threats and more precise documentation of risk analysis results and the assumptions. Finally, tighter integration of risk management in the system development process may considerably reduce the development costs.

In this paper we place the emphasis on the proposed guidelines and recommendations for model-based risk management, which will be evaluated through trials in the e-commerce and telemedicine areas. Since CORAS is an ongoing project, the research described here is work in progress.
1 Introduction

There is increasingly widespread recognition of the significant role which information technology plays in supporting and enhancing national infrastructures in the civil, commercial and military areas.

However, the dependencies of any single infrastructure (water, financial operations, services offered by government, etc.) on information processing entities/systems are often not fully understood. Furthermore, the increasing pace of change in the environment in which we operate exacerbates the problems of assuring the continued operation of systems that are taken for granted in twenty-first century Europe. Frequent upgrades to innumerable legacy systems, interconnection with new operators often from abroad, moves to increased use of IP networks, etc., challenge the assumptions made in the 1980s when many of the existing system architectures were designed for reliable support of national infrastructures.

Emerging services in the area of e-commerce and telemedicine impose new and strict requirements to the underlying infrastructure. A proper understanding of the limitations of the existing infrastructures is an important prerequisite for designing new services with a satisfying degree of security.

With this background, the research and technological development project under the Information Society Technologies (IST) Programme (Commission of the European Communities, Directorate-General Information Society) - CORAS [1] (January 2001 – July 2003) was started. The CORAS main objectives are as follows:

- To develop a practical framework, exploiting methods for risk analysis, semiformal methods for object-oriented modelling, and computerised tools, for a precise, unambiguous, and efficient risk assessment of security critical systems.
- To apply the framework in security critical application domains.
- To assess the applicability, usability, and efficiency of the framework.
- To promote the exploitation potential of the CORAS framework.

2 CORAS Framework

A system for CORAS is not just technology, but also the humans interacting with the technology and all relevant aspects of the surrounding organisation and society. CORAS addresses security critical systems in general, but puts particular emphasis on information security defined by: confidentiality (only appropriate access is allowed to data, both from inside or outside the organisation); integrity (no unauthorised changes are made to data, either in storage or transmission); availability (data is accessible as required); and accountability (users are accountable for their security-relevant actions; includes non-repudiation).

The main outcome of the CORAS project is the CORAS framework for Model-based Risk Management. Such an approach is motivated by several factors:
Risk assessment requires correct descriptions of the target system, its context and all security relevant features. The modelling technology improves the precision of such descriptions. Improved precision is expected to improve the quality of risk assessment results.

The graphical style of semiformal modelling technology furthers communication and interaction between stakeholders involved in a risk assessment. This is expected to improve the quality of results, and also speed up the risk identification and assessment process since the danger of wasting time and resources on misconceptions is reduced.

The modelling technology facilitates a more precise documentation of risk assessment results and the assumptions on which their validity depend. This is expected to reduce maintenance costs by increasing the possibilities for reuse.

The modelling technology provides a solid basis for the integration of assessment methods that should improve the effectiveness of the assessment process.

The modelling technology is supported by a rich set of tools from which the risk analysis may benefit. This may improve quality (as in the case of the two first bullets) and reduce costs (as in the case of the second bullet). It also furthers productivity and maintenance.

The modelling technology provides a basis for tighter integration of the risk management process in the system development process. This may considerably reduce development costs and ensure that the specified security level is achieved.

The CORAS framework for model-based risk management has four main anchor-points: a system documentation framework based on RM-ODP [2], a risk management process based on AS/NZS 4360 [3], a system development process based on RUP [4], and a platform for tool-integration based on XML [5].

2.1 The CORAS Risk Management Process

CORAS focuses on applying risk management on security critical systems. Therefore, in addition to [3], input is also taken from information security standards: Australian Standard - Information Security Management [6] and Canadian Institute for Health Information [7]. The CORAS risk management process, as indicated by Figure 1, provides a sequencing of the risk management process into the five sub-processes, where each of those comprises a number of activities:

1. **Identify Context** (of the analysis that will follow). The approach is to select usage scenarios of the system under examination. **Activities:** Identify areas of concern, Identify and value assets, and Identify security requirements.

2. **Identify Risks.** **Activities:** Identify hazards/threats to assets, and Identify vulnerabilities of assets.

3. **Analyse Risks:** Assign values to the consequence and the likelihood/probability of occurrence of each hazard/threat identified in sub-process 2. **Activities:** Consequence/impact evaluation, and Evaluate likelihood of occurrence.
Risk Analysis III

4. **Risk Evaluation**: Identify the level of risk associated with the hazards/threats already identified and assessed in the previous sub-processes. **Activities**: Determine level of risk, Prioritise risks, Categorize the risks, Determine interrelationships among issues, and Prioritise the resulting themes and risks.

5. **Risk Treatment**: Address the treatment of the identified risks. **Activities**: Identify treatment options, and Assess alternative approaches.

![Figure 1: Overview of the CORAS risk management process](image)

In addition, two concurrent sub-processes are implicit: Monitoring and Review, and Communication and Consultation. They are running in parallel with the above five.

The CORAS framework for model-based risk management builds on following six risk analysis methods:

- Hazard and operability study (HAZOP) [8];
- Fault tree analysis (FTA) [9];
- Failure Mode and Effect Criticality Analysis (FMECA) [10];
- Markov analysis methods (Markov) [11];
- Goals Means Task Analysis (GMTA) [12]; and
- CCTA Risk Analysis and Management methodology (CRAMM) [13].

The choice of risk analysis method to be used in the specific sub-process depends on the RM-ODP viewpoint in which the part to be analysed appears, and the detail incorporated in the context of the analysis depends on the phase in the development lifecycle. This will be dealt with in more detail in section 5, and is also summarized in Figure 2.

Further information on the CORAS risk management process, emphasising the roles of different risk analysis methods is provided in [14].

2.2 The CORAS system documentation framework based on a specialised RM-ODP

Risk analysis of a system requires a certain understanding of the system to be analysed, e.g. how the system is built, how it works, and how it is used. Quality and reliability of the risk analysis results depend on the level of this system understanding. Also, what is a sufficient system understanding depends on the system aspects to be analysed and the risk analysis method to be used. A risk analysis typically involves a group of humans with different backgrounds and
different system roles, (e.g., managers, users, system experts), so the quality and reliability of the risk analysis results depends on to what degree these groups are able to communicate with each other and, in particular, with the risk analyst.

In that sense, CORAS project aims to define security relevant models within the various ODP (Open Distributed Processing). RM-ODP (Reference Model for Open Distributed Processing) [15] is a system documentation framework that provides a basic reference model for viewpoint-oriented modelling of distributed systems. A specialised RM-ODP inspired modelling framework aimed towards the identification and analysis of risks in security critical systems is a basic ingredient of the CORAS framework. This modelling framework:

- Provides specialised modelling support targeting the risk analysis methods.
- Offers patterns and rules for reuse and maintenance of results from risk analysis based on the modelling methods provided by the framework.
- Offers a well-suited structure for the organisation and maintenance of standard library components.
- Provides generic scenario-driven design tactics in order to exemplify and facilitate the effective use of the above rules, patterns and library components in specifying a security policy.

Models built upon this framework are designed to provide a well-suited medium for the communication among the risk analysis groups. Each model describes the system to be analysed from a particular viewpoint, and at a certain level of abstraction. These models are not restricted to technical issues only, they are also concerned with the organisations and work processes within which the system is embedded. The models, expressed in format or semiformal modelling method should also capture security requirements like risk acceptance levels and support efficient and comprehensible communication of security requirements to policy makers. In addition, the project aims to develop precise and unambiguous specification methods for the various models and guidelines for their use and addresses security oriented transparencies in the style of the existing ODP distribution transparencies.

So far, a number of complementary modelling paradigms have been assessed and pre-selected for use in the CORAS documentation framework. They include UML [16], SDL [17], MSC [18], for system specification, CQML [19] and Ponder [20], for specifying access control and security management policies. Logic based methods such as OCL [21], subjective logic [22], process calculi [23] [24], are also needed for providing additional expressiveness of more specific tasks. However, a detailed description of such paradigms is beyond the scope of this paper. Further information on the role of modelling in the Model-based Risk Management, as understood in CORAS, is provided in [25].

2.3 The CORAS system development and maintenance process

The CORAS system development and maintenance process is based on integration of Australian Standard for Risk Management Process [3] and an adaptation of the Rational Unified Process (RUP) for development. RUP is adapted to support RM-ODP inspired viewpoint oriented modelling. Figure 2
Risk Analysis III provides an overview of the relationship between the various risk assessment and modelling techniques and their relative position with respect to the RM-ODP viewpoints and RUP. Emphasis is placed on describing the evolution of the correlation between risk management and viewpoint oriented modelling throughout the systems development and maintenance lifecycle.

In analogy to RUP, the CORAS process is both stepwise incremental and iterative. In each phase of the system lifecycle, sufficiently refined versions of the system (or its model) are constructed through subsequent iterations. Then the system lifecycle moves from one phase into another. In analogy to the RM-ODP viewpoints, the viewpoints of the CORAS framework are not layered; they are different abstractions of the same system focusing on different areas of concern. Therefore, information in all viewpoints may be relevant to all phases of the lifecycle. The CORAS risk management process follows the iterations made in the CORAS process. Each iteration adds more detail to the target and the context of the analysis and previous results may need to be re-evaluated.

Figure 2: Overview of the CORAS framework emphasizing its decomposition to the modelling framework, development process and risk management.
The core risk analysis segment of the CORAS risk management process (Figure 1) are three sub-processes (identify risks, analyse risks, risk evaluation), grouped together at the top layer of Figure 2. The CORAS risk management process consists of instantiations of abstract patterns given the CORAS framework using different risk analysis methods in order to analyse different parts of the system. The choice of risk analysis method upon which the abstract pattern is instantiated depends on the viewpoint in which the part to be analysed appears and the detail incorporated in the context of the analysis depends on the phase in the development lifecycle. The specific instances of the CORAS risk management process that are used throughout the system lifecycle depend on the target (sub)system and the context of the analysis. Consequently, it is the viewpoint relevance and not the phase in the development lifecycle that determines which risk analysis method is to be used in each instantiation.

As the system description becomes more elaborate, any combination of refinement and decomposition results into a propagation of the risk analysis from the composite object to the components guided by the system architecture. Furthermore, as more information is incorporated in the context of the analysis there is always the potential that new vulnerabilities are identified and this must be taken into account to the risk analysis of the composite entity. Consequently, the risk management process follows the iterations of the development lifecycle.

2.4 The CORAS platform for tool integration

There are four main strategies for tool integration:

- **Data Integration**: Software systems are integrated by defining a common vocabulary to be used in information exchange and by providing the means for efficient information sharing. Examples of technology are XML and other data exchange formats, and repositories and DBMS with a common data model.

- **Control Integration**: Typically, software systems are integrated by specifying operational service interfaces. Examples of supporting technology are CORBA with its Interface Definition Language (IDL), Microsoft .Net with Simple Object Access Protocol (SOAP), and Java 2 Enterprise Edition with Java interface specifications.

- **Process Integration**: In an enterprise, this means that the actors may share a common process model. A process enactment engine employs this model to guide the users in tool usage. Examples of this technology can be found in most current workflow systems.

- **Presentation Integration**: The degree to which a user-interface program might provide access to the functionality needed by the user through a common look and feel. Typically, this is achieved by a common window management system that includes useful functionality like drag-and-drop, etc.
The CORAS platform is based on data integration implemented in terms of XML (eXtensible Markup Language) technology [5]. Figure 3 outlines the overall structure. We envisage building a platform around an internal data representation formalised in XML/XMI. Based on XSLT, which is a language for transforming XML documents into other XML documents and consists a part of the XSL (eXtensible Stylesheet Language) definition [5], relevant aspects of the internal data representation may be mapped to the internal data representations of other tools and vice versa. Standard XML tools provide much of the basic functionality that allows experimentation with the CORAS platform and can be used by the CORAS crew during the trials.

3 The CORAS trials

There is a twofold motivation behind the trial activities. Firstly, we want to make sure that:

- The framework is capable of handling realistic and up-to-date security problems.
- The framework is practical (e.g. efficiency, user friendliness).
- The results from the CORAS analysis are sensible and useful for improvement of the analysed systems.

Secondly, we want to stay in contact with potential exploitation areas:

- Telemedicine
- E-commerce

In order to plan the assessment of the CORAS framework, success criteria are specified, with respect to applicability, effectiveness, performance and usability. In terms of applicability, CORAS’ framework is expected to: address all security critical aspects (expressiveness), handle diverse applications including technical as well as non-technical system features (generality), be useful for analysing small and medium-sized systems, as well as large and very complex systems (scalability). Regarding effectiveness, the CORAS framework is expected to: increase the probability for finding all significant security risks.
(completeness), facilitate precise and unambiguous description of the security relevant features and risk analysis results (accuracy), reduce the probability that risks are overlooked as a result of misconceptions (clarity). Performance of the CORAS framework should reduce: risk analysis costs by reducing misconceptions (analysis), reduce system development costs (development), reduce maintenance costs (maintenance), reduce costs through reusability of system documentation (reuse). Usability means that CORAS framework should: support intuitive communication of risk analysis inputs and results (communication), support openness and interoperability (tools), provide user-friendly documentation (documentation).

3.1 Trials in the e-commerce domain

The E-commerce platform is a Web application providing basic purchasing services to online customers. The platform is implemented in Java where most functionality is provided by the server using Java Server Pages (servlets). The implementation follows a 3-tier architecture: *client tier* for the presentation of data, receiving user events and controlling the user interface; *application server tier* provides the business logic; and *data server tier* for data storage. A relational database (RDBMS) is used to store consumer and product information and is accessed via the JDBC interface. Figure 4 shows the various components and their connections in the platform. The functionality is provided by the following four software components:

**PSV**: The Personalised Store Visualizer component provides the application’s GUI and the functionality for its customisation.

**VSO**: The Virtual Shopping Operator component provides the purchasing services, like electronic shopping baskets, access to product information through electronic catalogues, and secure payments. This component offers the interface to retailer’s legacy systems for handling the customer orders and payments.

**OLSN**: The On-Line Sales Negotiator component provides agent-based price negotiation for products, following customer’s constrains, and may optionally proceed to automatic purchasing if an agreement is reached.

**SR**: The Shopping Recommender component provides shopping recommendations, like product discounts and special offers, taking into account the customer’s profile stored in the database.
In the course of the CORAS project, the E-commerce platform will be modelled in order to perform risk analysis on the security aspects of the platform, with particular stress on confidentiality (user authentication, secure payments and agents for prices negotiation).

### 3.2 Trials in the telemedicine domain

Platform for the telemedicine trial is the HYGEIAnet, the regional Health Telematics Network of Crete. It is implemented as a Virtual Private Network (VPN) that isolates the HYGEIAnet and the applications using its services from the outside world (i.e. Internet) by means of firewalls. Two trial scenarios have been chosen. The first is the ATTRACT pilot; a program to regularly follow up children with asthma in Crete via videoconferences between a paediatric outpatient clinic specialising in children with asthma at the University Hospital of Crete, two district hospitals and three primary health care centres. Second scenario is the Tele-Cardiology service, a tele-consultation service that provides access to cardiology specialists at the University Hospital of Crete from local physicians in remote areas through a web-based interface.

CORAS framework will be used to model security relevant aspects (availability, in particular) of the HYGEIAnet platform and its applications, and perform risk analysis on the resulting models. This will be done in an iterative manner, providing feedback to the developers of the CORAS platform between the iterations. In addition, different stakeholders of the HYGEIAnet (e.g. developers, managers, medical doctors), will be consulted to provide feedback in order to evaluate the applicability, usability and efficiency of the framework.

### 4 Conclusions

This paper provides an overview of the CORAS framework for supporting Model-based Risk Management. Our approach integrates risk analysis methods; semiformal description methods (viewpoint- and object-oriented modelling methods); and tool-integration technology that support openness and
interoperability. The main motivation for such an approach is an improved methodology for precise, unambiguous, and efficient risk analysis of security critical systems.

The particular angle of the CORAS project (with its emphasis on security and risk analysis tightly integrated in the RM-ODP setting and underpinned by a platform for tool-integration targeting openness and interoperability) is new and has not been tried before. We strongly believe that such an approach will improve risk management of the system through better description of the system, more precise formalisation of threats, improved communication and interaction between stakeholders involved in a risk analysis, and considerable reduction of the development costs.

The CORAS framework will be assessed through two major trials, one within e-commerce and one within telemedicine. The main focus will be put on evaluation of security aspects: confidentiality, integrity, availability and accountability. The main outcome from those experiments will be feedback for further development of CORAS framework and improvements of the systems under trials which will justify overall effectiveness and success of the CORAS approach.

References

264 Risk Analysis III


