A Conceptual Formal Framework for Developing and Maintaining Security-Critical Systems

Habtamu Abie and Asmund Skomedal
Norwegian Computing Center, P.O.Box 114 Blindern, N-0314 Oslo, Norway,
Habtamu.Abie@nr.no, Asmund.Skomedal@nr.no

Abstract

One of the most important challenges, present and future, is that of developing methods and measures to deal with a broad range of threats, ranging from terrorism, organized crime, and natural disasters to electronic intrusions. The complexity of critical systems (CSs) makes the development and maintenance of them susceptible to subtle errors, errors which make these systems vulnerable to the threats mentioned. One of the most important security practices is to integrate the development process of security with the development process of the system itself using formal methods at every stage to increase the level of confidence in the development, deployment and use of the system. Therefore, there is a need to build an overall, flexible (semi)-automated and formalized framework for the development and maintenance of the security of critical systems. In this paper, we propose such an integrated conceptual framework, which will enable us to design, analyze, implement, deploy and use a CS securely and efficiently in accordance with the specific security requirements and relevant security policies.

Keywords: *Critical Systems, Risk Management, Security Requirements, Security Policy, Formal Methods*

1 Introduction

During the past few years we have witnessed enormous and rapid changes in our society and developments in its infrastructure, which has become more sophisticated and efficient and, at the same time, correspondingly more susceptible to disruption and vulnerable to threats of various kinds. Particularly, due to the complexity of critical systems (CSs), the development and maintenance of them is susceptible to subtle errors. The rapid rate of change in the environment in which we operate does not make it easier to assure the security of CSs, since security measures rapidly become outmoded. One of the most important challenges facing us, presently and in the future, is thus that of the preparation of methods and measures to deal with a broad range of threats, ranging from terrorism, organized crime, and natural disasters to electronic intrusions. These methods and measures will inevitably include making security measures normal, established, standard routine, and exchanging the latest and most-up-to-date information on threats, vulnerabilities and best practices. Somehow the security of a system seems, as often as not, to be implemented not as an integral part of the system in question, but rather as an addition to it and an afterthought [1].

Consequently, in order to forestall these errors and problems, there is a need to adopt a systematic formal approach to integrating the development of security requirements and security policies, and risk management process into the actual process of developing the system. While using formal methods aids the early discovery of vulnerabilities, inconsistencies and redundancies in security, applying risk management process throughout the system's life cycle, makes security a built-

in integral part of the system, which adapts to meet changing requirements and conditions [2]. This practice will thus allow us to design, analyze, implement, deploy and use these systems securely and efficiently in accordance with the specific security requirements and relevant rules and policies, thus increasing the level of reliability and confidence in the systems, and our work is a contribution to the development of this approach.

There already exist commonly accepted and publicly available specified standards for managing information security, to wit BS7799 (evolved into ISO/IEC 7799 - a code of practice for information security management in an organization) [11], ASNZS (Australian/New Zealand standard - the most widely recognized standard in the field of risk management) [4], NS (Norwegian Standard - Requirements for Risk Analysis) [5], ISO TR13335 (Guidelines for Management of Information Technology Security) [12], the Common Criteria (a generic framework for common sets of requirements for the security functions of IT products and systems and assurance measures applied to IT functions of IT products and systems during a security evaluation) [13], COBIT (Control Objectives for Information and Related Technology – a generally applicable standard for good IT security and control practices) [14], CRAMM (UK Government's Risk Analysis and Management Method - a framework for a structured and consistent approach to computer security management for all systems) [15], etc.

By being the basis for a structured approach to establishing context, identifying and analyzing threats for the purpose of establishing the security policy of a system, risk analysis forms a basis for designing a secure system. In addition, to increase the reliability of and confidence in the specification, analysis, and verification of the security of a system, it is necessary to integrate risk analysis with security requirements, security policies, and security mechanisms in a framework which uses formal methods and modeling techniques and tools to form an overall computerized (semi)-automated and formalized model for the practice of security for critical systems in the years ahead.

Present state-of -the-art approaches are unable to fulfill this need since they are as yet not sufficiently formalized or computerized. They are not also holistic enough, focusing as they do on some special phase [16], [17] of development in design or implementation for example, or on specific aspects of security, e.g. requirements, policies, etc.

There are several closely related national and international projects that ARM intends to build up on whenever appropriate. **FARES** (Formal Analysis of Risks in Enterprise Systems) [20] is a formal approach to risk analysis and management using formal methods and knowledge science as core precepts. **CORAS** [19] was a project that developed a tool-supported methodology for model-based risk analysis of security-critical systems. **WIN** [21] a service oriented architecture for risk management that has the objective of integrating all existing reference results or initiatives to contribute to the design, the development, and the validation of what could be referred to as a "European Risk Management information infrastructure". **ORCHESTRA** [22] aims to improving the efficiency in dealing with risks by developing an open service architecture for risk management that is based on de-facto and de-jure standards. **PFIRES** [23] is a policy framework for interpreting risk in e-Business security.

As evident from the above, research and systems for risk management exist, but today, “there is limited evidence of credible risk analysis methods and procedures that combine technical and non-technical assessment and analysis methods

satisfactorily" [20]. Therefore there is a need for a holistic and adaptive approach to risk management that comprises technical, operational, market mechanisms and administrative controls and the required assessments to establish their efficacy in managing risks.

2 Critical Systems and Related Security Research

Critical systems are increasingly faced by the danger of intrusion and attack. The critical infrastructures of, for example, medical services, transport, banking and finance, gas and electricity industries, and telecommunications make use of the public Internet for communication, not least for the exchange of business, administrative and research information. Therefore, it is essential to make these security-critical infrastructures as secure and unassailable as possible.

Consequently, improving the ability to spot vulnerabilities is of the essence, and viable strategies must be developed to detect, deter, and counter threats, thus making CSs as unassailable as possible. These strategies must also be maintained and updated to keep abreast of current and future developments in the security situation, which must be continuously assessed and reassessed.

Information Assurance (IA) has traditionally been regarded as one of the methods and measures useful in protecting against a new and emerging broad range of threats. IA is based on operations whose function is to protect information and information systems. This protection is based on ensuring availability, accountability, confidentiality, and integrity. "This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities" [3]. The Church-Turing thesis proves that "any suitably powerful computer can exactly recreate the results of any other one," which implies that IA and other strategies are constantly challenged. This means that research in all areas of security for CSs must be a continuously on-going process, and will necessarily involve among other things, a) identifying necessary security services and improving those already extant, b) improving risk management techniques and methods, c) developing and improving a legal framework, and d) applying formal methods and tools to all these areas.

2.1 A Suite of Security Services

In order to **identify necessary security services and improve those already extant**, it is essential to identify a suite of necessary security services (both at the application level and infrastructure level) such as cryptography, key distribution, public key infrastructure (PKI), protocols, algorithms, security policy, privacy protection, trust management, risk management, forensics, intrusion detection and prevention systems, biometrics, communications security, protection of digital assets (a.k.a. Digital Rights Management), etc.

Secondly, it is essential to identify architectures and frameworks for combining security mechanisms and services in effective and reliable ways.

Thirdly, it is essential to ensure that the security mechanisms implemented (e.g. those for interoperable encoding of security attributes) interact effectively, and to develop both techniques to manage the combination of interacting mechanisms, and methods and tools to assess and guarantee the combinations' security.

Finally, it is essential to demonstrate how already existing applications and new ones can be protected using high level and generic security service APIs (application

interfaces), and how sound security for the protection of the CS's infrastructure can be developed and maintained.

2.2 Improving Risk Management Techniques and Methods

In order to **improve risk management techniques and methods,** it is essential to improve techniques and methods for the analysis, assessment, and management of risk by developing a common framework and architecture supporting applications which deal with all five risk cycles (risk assessment and planning, mitigation, preparedness, response, and recovery).

Secondly it is essential to introduce a software engineering process in which the awareness of risk analysis, security requirements, and security policies are exercised at each stage (specification, analysis, design and implementation).

Finally, according to our prediction it will be essential to meet the following challenges identified in [18]):

- Establishing the appropriate balance between trust, policy, security, and risk management for CSs with a balanced legal framework that takes account of changes in the academic, political, economical and socio-cultural environment.
- Managing in advance and in a number of different ways future possible risks related to CSs.
- Developing a holistic assessment of risks and threats specifically related to CSs, in order to enhance the risk management procedure and ensure its completeness, and learning to manage risks involved in CSs, thereby building trust in those CSs.
- Developing risk management methodologies for CS protection development – especially knowledge bases with specific risk controls.
- Building CS scenarios to support qualitatively and quantitatively appropriate decision-making processes for the minimization of risks, based on "system dynamics based modeling and simulation".

2.3 Developing and Improving a Legal Framework

In order to **develop and improve a legal framework**, a framework which will protect CSs and infrastructures; new legislation will be essential, legislation that will deal with new situations not only by passing new laws, but also by repealing obsolete laws which are now actually in the way. One example of obsolete and now counter productive legislation being the regulations that impede and prevent the voluntary sharing of information so essential to the protection of CS infrastructure.

2.4 Applying Formal Methods and Tools

It is common and well-founded practice to apply formal methods, techniques and tools to increase the reliability of, and level of confidence in, the specification, analysis, design, verification, implementation and secure operation of the system. It goes without saying that in the above areas formal methods, techniques, and tools should be applied at all levels. For example, through their application, the practice of the identification of risks, threats and vulnerabilities, and the application of the appropriate controls to manage risks, can be formalized and (semi)-automated, which will improve overall risk management. Improved risk management will lead to the improved specification of security requirements since the correct specification of security requirements is based on the result of risk management. Improved specification of security requirements will lead to the improved specification of security policy since the correct specification of security policy is based on the specification of security requirements. (See the ensuing chapters).

3 Risk Management, Security Requirements and Security Policies: Their Relationship

Risk Management is inextricably interwoven with security. A security policy is necessary to support the security infrastructure required for the secure transfer of sensitive information across and within national boundaries. To ensure the secure operation of this kind of security-critical infrastructure, it is necessary to have some well-founded practice for the identification of security risks and the application of appropriate controls to manage these risks [reference not disclosed]. The underlying philosophy is to identify specific threats to a system, to determine the costs of possible attacks as well as the costs of protecting against them, to implement protection mechanisms only when the benefits of such mechanisms outweigh the costs of their implementation, and to respond gracefully to break-ins rather than attempting to establish absolute yet brittle security.

The risk management process thus provides a framework for identifying analyzing, evaluating, treating, monitoring and communicating risks relevant to the distribution of valuable digital assets and the proper operation of CSs. Risk management is not a task to be completed and shelved, but an ongoing process (with well-defined steps [4],[5],[6]) that, once understood, should be integrated into all aspects of the development of CSs. Sound risk management will increase confidence in, and the reliability of, the operation of CSs.

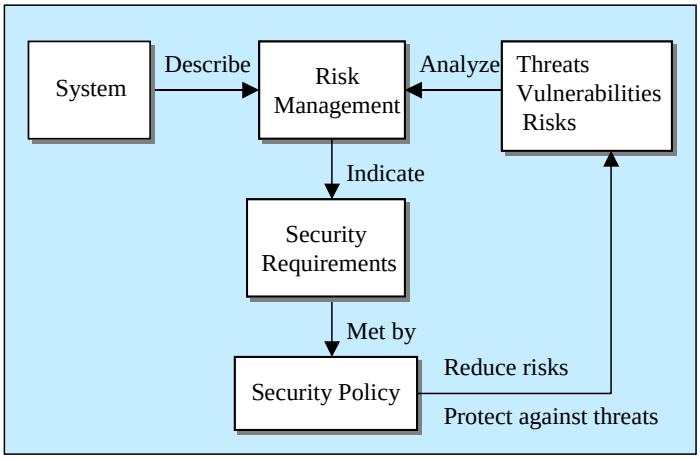

Figure 1 Risk Management, Security Requirements and Security Policies

The concern of **security policy** is the design, analysis, implementation, deployment and use of efficient and secure technology that handles CSs in accordance with the relevant set of rules and procedures. **Security policies** must thus be consistent, complete, appropriate, implementable and verifiable. The security policies of the CS are based on the **security requirements** of the CS. **Security requirements** are high-level statements of countermeasures that will adequately mitigate the identified risk and are dependent on rigorous analysis of risks, the CS's vulnerability, and threats to it. Thus, since improvement in the implementation of policy depends on an improved risk management process, any research must give full attention to enhanced risk management processes, and risk assessment methodologies. Consequently, security policies must be developed and integrated into the development of CSs. Brose et al. [7] have also proposed a systematic approach to integrating security policy design into the system development process. Figure 1 depicts the relationships between risk management, security requirements, security polices, and other related components.

4 Conceptual Framework for Developing and Maintaining Security-Critical Systems

We propose to build an overall, flexible (semi)-automated and formalized framework for the development and maintenance of CSs. This framework will enable us to investigate proactively, and to adapt to, new factors as they emerge due to changes in the environment brought about by new policies, new laws, new technologies and, not least, new threats. It will enable us to deal with these factors in whatever combination they present themselves at any given moment, by using formal specification and verification methods and computerized tools, and by improving understandability, precision, flexibility, ease of automation, and ease of verification. Figure 2 shows our integrated conceptual framework for the development and maintenance of the security of CSs. FARM stands for "A Formal Framework for a Proactive and Adaptive Risk Management" which currently under development applying suitable existing and popular modeling, specification and verification techniques like Petri Nets, Bayesian Network, UML, model checking, etc. as appropriate.

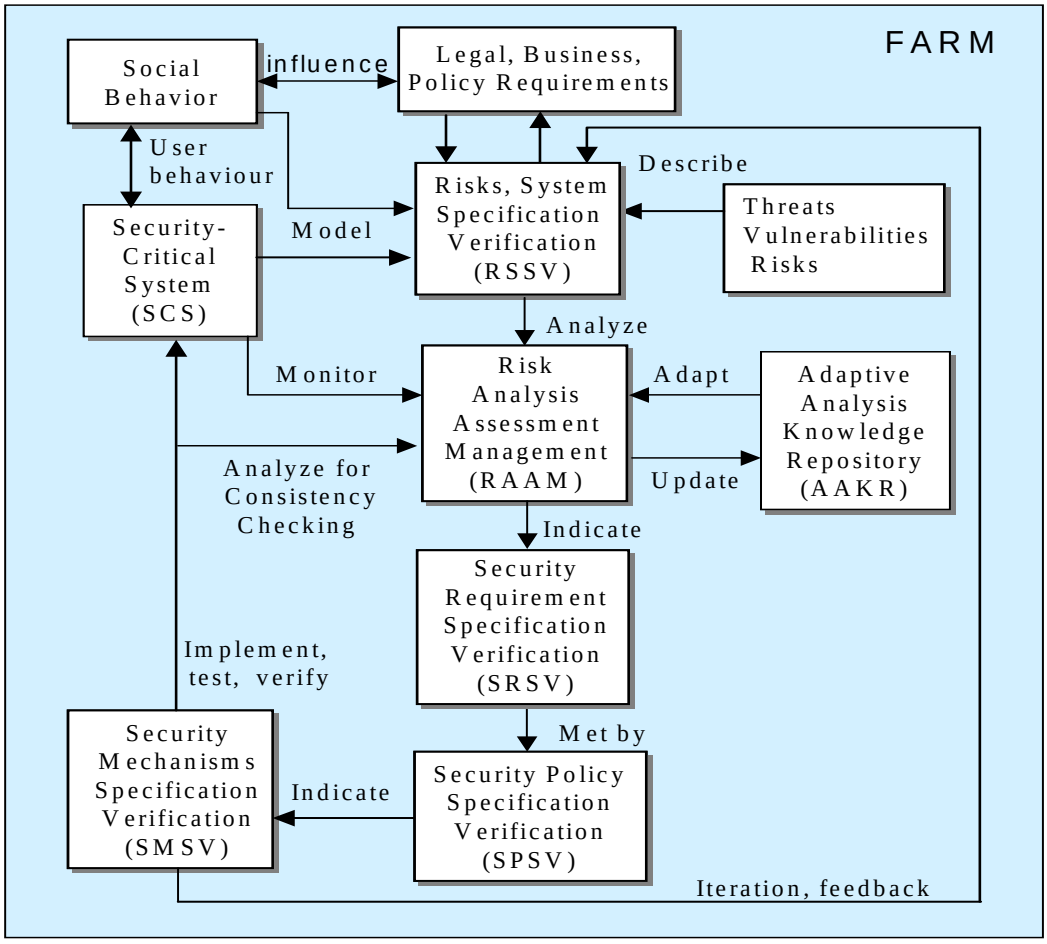

Figure 2 A Conceptual Framework for Developing and Maintaining CS

. In the ensuing sections, we first describe briefly the main components of the framework and the relationships between them, and then give a brief summary of the framework and its advantages.

4.1 Functional Descriptions of the Main Components

The **RSSV** module (see figure 2) will allow the accurate specification and verification of CSs and the vulnerabilities, threats and risks to which they are

exposed, and will take into consideration the legal, business, and policy requirements, and environmental and organizational factors. The result of the RSSV's activities will lead to activities of the **RAAM** module.

The **RAAM** module will allow a more precise and unambiguous identification of potentially vulnerable elements in the system, an evaluation of which problems may emerge due to these elements, and an analysis of the potential consequences these problems may lead to, thereby aiding the early discovery of vulnerabilities, inconsistencies and redundancies in security. Results and documentation from these analyses are stored in the **AAKR** module (an adaptive analysis knowledge repository). The **AAKR** module will allow us to establish methods to check the consistency of the results of risk analysis, and to present and communicate comprehensibly both these results and security requirements, thus making possible the qualitative modeling, management and documentation of risks in a precise, unambiguous and efficient manner. The **RAAM** adapts previous experience to the prediction of events in the future and new situations. Specifically the knowledge gained from the analysis of past situations is used to produce good, and hopefully correct, analyses of future situations.

The results of the **RAAM**'s activities will lead to the accurate specification and verification of the security requirements by the **SRSV** module. Rushby [8] has outlined two main approaches to specifying security requirements in a formal manner. The first consists of presenting a description of a model system exhibiting the required characteristics and then making the stipulation that an acceptable implementation be some suitable refinement of that model system, and the second of specifying the requirements as constraints that an acceptable implementation must satisfy. The **SRSV** module will use both of these. The articulated security requirements form the basis of establishing security policy.

The **SPSV** module will allow the accurate specification and verification of security policies. This will allow security policies to be formulated both comprehensibly and unambiguously in the CS's environments, based on the security requirements that are arrived at through a comprehensive analysis of the security needs of the CS. It will also allow security policies to be checked for consistency and correctness. The articulated security policies form the basis for establishing the security mechanisms.

The **SMSV** module will allow the accurate specification and verification of security mechanisms. It will allow a precise and unambiguous modeling of the individual mechanisms based on the articulated policy, and will allow the implementation, testing and verification of all the security mechanisms for the CS. The module will include a methodology that will assist in transforming the specification of the mechanisms into program code.

The **FARM** module will in a formalized, automated and flexible manner, maintain and manage the operations of the overall framework, and manage the consistency of the relationships (communications and feedback) between the different components as an integral part of the framework. The main challenge to be met by this module is to find a natural formulation of components that are compositional. Two secure components are compositional if they form a secure system when joined together in a suitable way. The natural formulation of components is a systematic and independent process which includes specification, refinement, maintenance, and analysis, and error prone in the absence of a flexible and powerful specification language with which to specify unambiguously CS security, and an accompanying automated management tool to ease this process.

4.2 Summary and Advantages

In summary, the overall framework will be composed of and assembled from independent formal methods, languages, modeling techniques and tools, risk analysis and evaluation techniques and methodologies, and sub-components. How these sub-components and tools communicate and co-operate (protocols and infrastructures) will be formalized and (semi)-automated to achieve dynamically changing CS security objectives. We will apply formal methods techniques and tools to the specification and verification of each component during the life cycle of each phase in its development, requirements, high-level and low-level design, and implementation. The difference between applying formal methods to requirements and to design lies in the level of detail at which we apply the techniques [9].

We believe that this framework will contribute to "Improved Risk Management" whose main aim is as identified elsewhere "to develop open platforms, integrated systems and components for improved risk management, improved civil security applications and environmental management". Other advantages include:

- The formal nature of the framework makes it possible to transform a high-level security policy specification systematically and automatically into an executable security-preserving code.
- The framework makes possible the automated processing of risk analysis, security requirements, and security policies, and the assurance of their consistency across the boundaries between different technologies, platforms and environments.
- The framework, because of the visual comprehensibility of the components and holistic view of security development, raises developers' awareness of security, which will in turn improve the quality of their CSs.
- Monitoring function of the framework helps us to observe what is happening, and to respond when appropriate and to measure the effectiveness of in-place security mechanisms.

Our conceptual framework, **FARM**, embodies all the above advantages by either tightly or loosely integrating the components, and thus contributes to the development of a platform for the unambiguous specification and accurate modeling and development of CSs and applications. The framework will improve the Quality of Security Services (QoSS) [10] by augmenting their security-costing framework, and by taking into account the major influential factors (such as government intervention, market forces, technology, and social norms) in the risk management process, thereby allowing us to measure adaptively how much trust and security we have and can achieve in our CSs.

5 Conclusions

Due to changes in environmental factors and advances in technology, information infrastructure is faced by new threats and is vulnerable in new ways, which makes it difficult to prevent intrusions. We have pointed out that the main challenge facing us, presently and in the future, is the preparation of methods and measures to deal with a broad range of threats, ranging from terrorism, organized crime and natural disasters to electronic intrusions. In this paper, we have identified fruitful areas of security research and demonstrated the need for the continuous development and maintenance of security in critical systems with an integrated, formalized, and automated approach.

We have proposed a conceptual framework for the achievement of this by the adoption of a systematic formal approach to the integration of security engineering (risk management, security requirement, security policy) into the life cycle of CSs. This will allow us to design, analyze, implement, deploy and use these CSs securely and efficiently in accordance with the specific security requirements and relevant policies, thus increasing the level of confidence in them. This solution itself must also be maintained and updated to keep abreast of current and future developments in the security situation, which must be continuously assessed and reassessed. This is achieved by paying correct attention to risk management process throughout a system's life cycle, in which security is a built-in integral part of the system, and adapts to meet changing requirements and conditions. We have also adopted a holistic approach to managing risks, an approach that takes into account legal, societal, technological, organizational, environmental and human factors.

We are currently working on the further development of our framework.

- We are developing module in the framework separately one after the other.
- We are investigating the possibility of incorporating the results of projects FARES, CORAS, WIN, PFIRES, etc into our framework as an integral part or of associating them with our framework, which will then communicate with them in the course of its activities.
- We are also incorporating concepts from the world of trust management into our framework since risk management encompasses trust management.

Acknowledgments

We would like to thank Prof Jacquelyn M. Rees for reading the draft of this paper and for her helpful comments that improved the paper.

References

[1] H. Mouratidis, P. Giorgini, and G.Manson, Integrating Security and Systems Engineering: Towards the modeling of Secure information Systems, Proc. 15th Conference on Advanced Information Systems Engineering, CAiSE'03, 2003

[2] CSE (Canadian Communications security Establishment) guide for Risk Management framework for Information technology Systems, 1996, available from: http://www.cse.dnd.ca

[3] Centers Of Academic Excellence in Information Assurance Education, http://www.nsa.gov/ia/academia/caeiae.cfm http://www.nsa.gov/ia/index.cfm

[4] AS/NZS 4360, Risk Management, Australian Standard, 12 April 1999-09-17

[5] Norwegian Standard (1991), NS 5814, Requirements for Risk Analysis

[6] B. Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley & Sons, Inc., 2000

[7] G. Brose, M. Koch, and K.P. Lohr, Integrating Security Policy Design into the Software Development Process, *Technical Report B-01-06*, Institut fur Informatik Freie Universität Berlin, Germany, 2001

[8] J. Rushby, Security Requirements Specifications: How and What? Invited paper from Symposium on Requirements Engineering for Information security (SREIS), March 2001, Indianapolis.

[9] NASA Formal Methods Guidebook, Vol. I, Release 2.0**,** available from: http://eis.jpl.nasa.gov/quality/Formal_Methods/

[10] C. Irvine and T. Levin, Overview of Quality of Security Service, Center for INFOSEC Studies and Research, Naval Postgraduate School, April 1, 2003, Available from: http://cisr.nps.navy.mil/downloads/QoSS_Overview.pdf
[11] The BS7799 Security Standard, http://www.riskserver.co.uk/bs7799/
[12] ISO/IEC, Guidelines for the management of IT Security – Part 1: Concepts and Models for IT Security, ISO/IEC, TR 13335-1, 2001
[13] Common Criteria Organization, "Common Criteria for Information technology Security Evaluation", http://www.commoncriteria.org/
[14] Control Objectives for Information and Related Technology (COBIT), available from: http://www.isaca.org/cobit.htm
[15] UK Government's Risk Analysis and Management Method (CRAMM), http://www.gammassl.co.uk/topics/hot5.html
[16] T. Tryfonas, E. A. Kiountouzis, and A. Poulymenakou, Embedding security practices in contemporary information systems development approaches, Information Management & Computer Security, Vol. 9, No. 4, 2001, pp 183-197
[17] R. Vaughn, R. Henning, and K. Fox, An empirical study of industrial security engineering practices, Journal of Systems and software, November 2001
[18] H. Abie, B. Foyn, J. Bing, B. Blobel, P. Pharow, J. Delgado, S. Karnouskos, O. Pitkänen, and D. Tzovaras, "The Need for a Digital Rights Management Framework for the Next Generation of E-Government Services", International Journal of Electronic Government", Vol. 1 No.1, pp 8-28, Inderscience Publishers, (ISSN: Print 1740-7494, Online 1740-7508), 2004
[19] CORAS (A Platform for Risk Analysis of Security-critical System), http://www2.nr.no/coras/
[20] CDFS (The Centre for digital Forensic Studies, Ltd), True Risk Management – Benefiting from a Generational Leap in Information Assurance Techniques, http://people.emich.edu/pstephen/my_papers/TRM_Executive_Briefing.PDF
[21] WIN, http://www.win-eu.org/
[22] ORCHESTRA, http://www.eu-orchestra.org/
[23] J. M. Rees, S. Bandyopadhyay and E. H. Spafford, PFIRES: A Policy Framework for Information Security, Communications of the ACM, Volume 46, Issue 7, pp 101 – 106, July 2003,

Biography

Dr. Habtamu Abie has a PhD in computer science and is currently a senior research scientist at the Norwegian Computing Centre. He has previously worked as Senior Engineer and Research Scientist at Telenor R&D Norway and as Scientific Associate and Scientific Fellow at CERN Switzerland. He has also held a research position at ABB Corporate Research and worked as Software Development Engineer at Nera AS and Alcatel Telecom Norway AS. He has solid, extensive background in the development of real-time control systems, the analysis, modeling, developing and maintaining control programs and software development tools for the telecommunications applications using formal methods and tools, the modeling, and the security aspects of distributed object computing systems, DRM, and risk management and security policy related issues.

Dr. Asmund Skomedal has a B.Sc. degree ('87) in Microelectronics from the University of Newcastle (UK) and a Dr. Ing. in Information Security ('94) from NTNU in Trondheim, Norway. He has over the last ten years been involved with large security projects building national and Nordic infrastructures. He has been development manager for digital-TV CA systems at Telenor Conax and he has been CTO at ZebSign responsible for the development of an infrastructure with open interfaces for creating and managing Qualified Certificates.