Journal of Universal Computer Science, vol. 18, no. 12 (2012), 1679-1702
submitted: 15/9/11, accepted: 15/2/12, appeared: 28/6/12 © J.UCS

Risk-Driven Security Metrics in Agile Software Development – An Industrial Pilot Study

Reijo M. Savola
(VTT Technical Research Centre of Finland, Oulu, Finland
reijo.savola@vtt.fi)

Christian Frühwirth
(Aalto University, Espoo, Finland
christian.fruehwirth@tkk.fi)

Ari Pietikäinen
(Ericsson Finland, Kirkkonummi, Finland
ari.pietikainen@ericsson.com)

Abstract: The need for effective and efficient information security solutions is steadily increasing in the software industry. Software and system developers require practical and systematic approaches to obtain sufficient and credible evidence of the security level in the system under development in order to guide their efforts and ensure the efficient use of resources. We present experiences of developing and using hierarchical security metrics and measurements in an industrial pilot study at Ericsson Finland. The pilot focused on risk-driven security design and implementation in the context of an Agile software development process. The pilot target was a well-established telecommunications product of Ericsson and a core component in modern mobile networks. The results of the study demonstrate the practical potential of risk-driven security metrics, particularly in offering some early visibility of security effectiveness and efficiency. Hierarchical metrics models enable the linking of security objectives with detailed measurements. Security metrics visualization was found to play a crucial role in increasing the manageability of metrics. We also found that the practical means of managing larger collections of metrics and measurements are more essential than individual security metrics. A major challenge in the use of risk-driven security metrics is the lack of evidence for security effectiveness evidence in the early phases of product development and Risk Analysis, when the needs for it are at their greatest.

Keywords: Security metrics, Risk Analysis, Agile SW Development
Categories: D.2.2, D.2.8, D.2.9

1 Introduction

Information security issues are a growing concern in the software industry. In order to ensure an adequate security level, systematic and practical approaches are needed for gathering and managing evidence of the effectiveness and efficiency of security solutions. Recently, *security metrics* has become a widely-used term when referring to the interpretation of these measurements or to the indicators of security strength of an SuI (System under Investigation) – a technical system, product, service or organization [Savola 2009]. Security metrics development methodologies have been under research for several years, but there is a lack of experience in applying them in practice [Verendel 2009], [Savola 2010]. Security metrics can be used to support decision-making in Risk Analysis (RA) and Risk Management (RM), secure software development, information security management, comparison of security solutions, software security assurance, security and robustness testing, and security monitoring [Savola 2007]. The intuitive reasoning behind the potential of security metrics is that quantitative estimates are more suitable for decision support and better in the long run compared to qualitative ones, even if they are incomplete.

The meaningfulness of the use of security metrics in engineering and management is highly challenging since human understanding of security risks and their impact on the SuI are often *too abstract and biased* [Savola and Heinonen 2011b], [Verendel 2010]. For example, RA, business and technical experts often have different understandings of the system: Business personnel emphasize business continuity but do not understand technical details enough. Technical experts try to achieve good product quality, but cannot foresee the business impacts. RA experts aim for a high quality of risk prediction, but do not see the situation in detail from technical and business perspectives. High-quality RA requires an active contribution of all the stakeholders, and in practice this cannot often be achieved. If a relevant viewpoint is not adequately taken into account, bias in RA results follows. In addition, the nature of security risks is complex: it is difficult to predict them, and new threats are introduced constantly. This means that security metrics cannot show complete effectiveness, especially when risk management resources are limited. Therefore, RM should not rely exclusively on the presence of these properties in security metrics.

Systematic risk-driven software (SW) development in industry is still rare: security efforts are often driven by the need to demonstrate compliance with standards and best practice specifications rather than risk knowledge. While a lot of detailed security information is available, it is rarely used in a systematic way, and its relation to the actual Security Objectives (SOs) is not understood well enough. Because security risks are complex multi-disciplinary challenges, a large number of security metrics are needed in order to acquire a sufficient understanding of the effectiveness and efficiency of solutions. Many security metrics approaches have emphasized the use of only a few metrics, leading to poor granularity [Savola and Heinonen 2011b]. However, it is difficult to understand the relations between high-level SOs and the detailed level measurements without hierarchical presentation and tool support in a large collection of metrics. Visualization of security metrics may increase the manageability of large metrics collections [Savola and Heinonen 2011b].

The main contribution of this study is in the evaluation of the potential and meaningfulness of a hierarchical risk-driven security metrics development methodology of a real telecommunications product, in the context of Agile software development. The research was carried out within an experimental pilot study at Ericsson's Network Business Unit in Finland during 2011. The metrics development methodology used was originally introduced in an earlier work by one of the authors [Savola and Abie 2009]. In this study, this methodology was applied, enhanced and integrated with a practical RA and Agile SW development processes. This paper does not discuss the details of actual security metrics.

The research was carried out in the following phases (see Fig. 1): (1) identification of the SuI from the pool of products being developed at Ericsson, (2) iterative modeling study focusing on integration of the security metrics development methodology of [Savola and Abie 2010] to risk-driven Agile SW development, (3) semi-structured expert interviews, and (4) conclusive analysis phase. In this paper, we discuss Phases 2-4. The identification of the SuI was an internal process at Ericsson. The SuI addressed in the pilot study was an enhanced version of an existing product, causing considerably new R&D effort. The SuI was not in end-user use during the course of the pilot.

Section 2 discusses the background and our earlier work on security metrics. Section 3 introduces the context of the pilot study, including the SuI, RA and Agile SW development processes used. Section 4 presents results from the modeling part of the study, and analyzes the integration of the [Savola and Abie 2010] metrics development methodology to RA and Agile SW development. Section 5 presents the results from the expert survey, and Section 6 analyzes the results of the modeling and interview parts. Section 7 presents related work, before Section 8 offers some conclusions and poses future research questions.

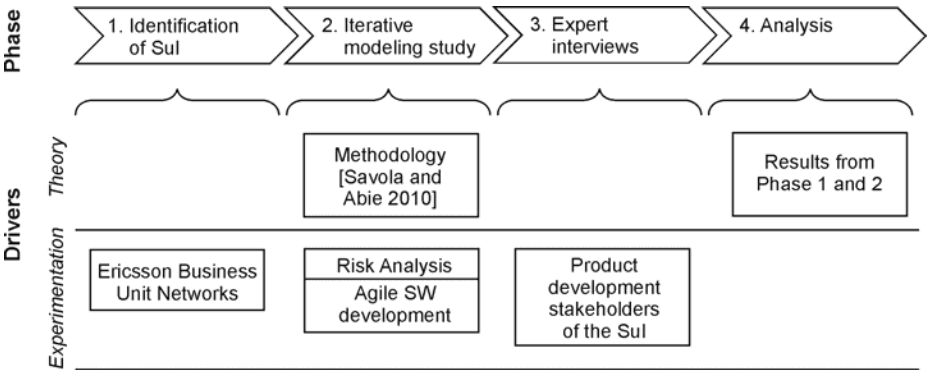
Phase
1. Identification of SuI
2. Iterative modeling study
3. Expert interviews
4. Analysis
Drivers
Theory
Experimentation
Methodology [Savola and Abie 2010]
Results from Phase 1 and 2
Ericsson Business Unit Networks
Risk Analysis
Agile SW development
Product development stakeholders of the SuI

Figure 1: Phases of this study

2 Background and Previous Work

2.1 Key Concepts and Objectives of Measuring Security

The key metrics-related concepts of this study are summarized in Table 1. The terms security performance and level are commonly used in practice to refer to the *security effectiveness* of security solutions, the main objective of security work and solutions. In addition, *security efficiency* is essential because resources are often constrained. In order to be able to reason systematically about security effectiveness and efficiency, and their ratio, there is a need for an abstraction model to explicitly express what kind of solutions are designed and used. The concept of *security controls* can be used for this purpose. In addition to security effectiveness and efficiency, *security correctness* is a fundamental objective [Savola 2009]. Correctness is a necessary *but not sufficient requirement* for effectiveness: it enables effectiveness. It should be a side effect of good security, not its driver. There are various factors which *enable* security effectiveness of the SuI: configuration correctness, correct design, implementation and deployment of security controls and proper security assurance and testing activities.

The term security metrics is misleading, since complexity, limited observability, a lack of common definitions and the difficulty of predicting security risks make it impossible to measure security as a universal property. However, measured data does not need to be perfect, provided that it contains the information required, is adequately correct and practically measurable. In this study, we employ the most widely used term, security metrics. As security metrics are challenging to develop, it is important to associate security metrics with *metric confidence*, an assessed value depicting the metrics developer's confidence in it. The actual measurement results and the metric confidence together indicate *security confidence* [Kanter 2004], i.e. the belief that the SOs are met.

Concept	Explanation	Reference
Security Objective (SO)	High-level statements of intent to counter identified threats and/or satisfy identified security policies and/or assumptions.	[ISO/IEC 15408]
Security Requirement (SR)	Requirement, stated in a standardized language, that is meant to contribute to achieving the SOs.	[ISO/IEC 15408]
Security Control (SC)	Means of managing risk, which can be administrative, technical, management, or legal in nature.	[ISO/IEC 27000]
Security correctness	Assurance that security controls have been correctly implemented in the SuI, and the system, its components, interfaces, and the processed data meet the security requirements.	[Savola 2009], [Jansen 2009]
Security effectiveness	Assurance that the stated SOs are met in the SuI and the expectations for resiliency in the use environment are satisfied in the presence of actual security risks.	[Savola 2009], [Jansen 2009], [ITSEC 1991]
Security efficiency	Assurance that the adequate security quality has been achieved in the SuI, meeting the resource, time and cost constraints.	[Savola 2009], [ITSEC 1991]

Table 1: Key concepts of the study

In practice, there are various gaps (G) and biases (B) between security effectiveness measurement objectives and practical security correctness metrics. Fig. 2 visualizes the concepts of Table 1, partly based on the SO and SC visualization in [Haddad et al. 2011], which emphasized gaps. Security efficiency, not shown in the figure, is a cross-cutting dimension concerned with the costs and time of all security solutions (RA, SO, SR and SC realization in Fig. 2). G_{RA} comes from the fact that in an RA it is not possible to identify and prioritize all the actual risks. Difficulties in understanding the SuI or risk situation can cause B_{RA}. Further gaps G_{SO}, G_{SR}, and G_{SC} are introduced when developing SOs, requirements and the actual SC realization. Additional bias (B_{SO}, B_{SR}, and B_{SC}) is caused at each stage. As shown in the figure, security correctness measurements in practice are always an approximation of security effectiveness, which cannot be measured in an absolute way. In practice, due to the gaps and biases, security effectiveness can be achieved only asymptotically. In high-quality security metrics modeling, an important goal is to minimize the gaps and the biases, making security correctness objectives as close as possible to security effectiveness objectives. Fig. 2 illustrates the achieved effectiveness as the intersection set of RA results, SOs, SRs, and SCs. The gaps and biases can be reduced in making them more evident via metrics, and by adequate reactions to this evidence. The basis of measurement in correctness metrics can be set for different references, depending on the needs, availability and attainability of evidence. In Fig. 2, "α" represents SOs, "β" the SRs, and "γ" the SC realization as the basis.

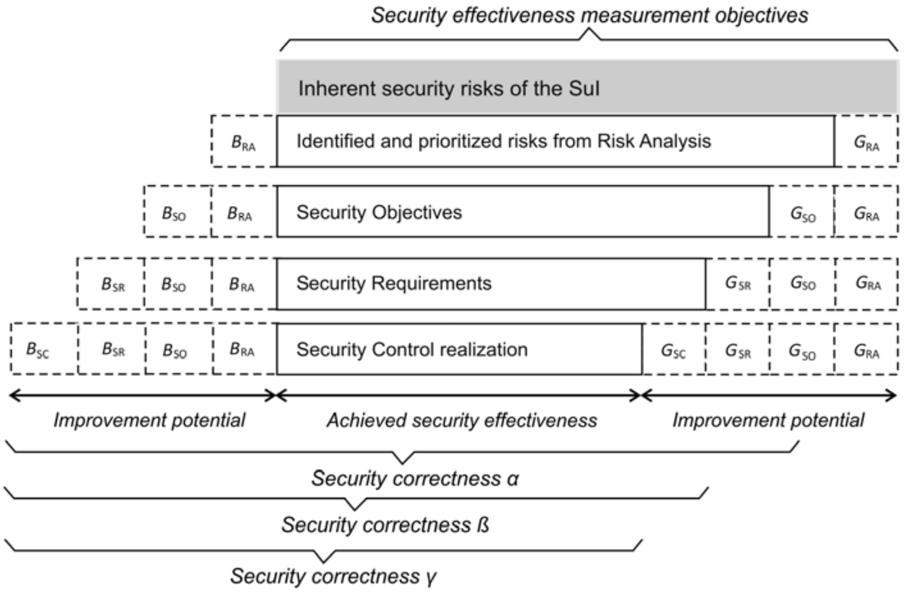

Figure 2: A visualization of the concepts of Table 1. G_x are gaps and B_x are biases between security effectiveness measurement objectives and security correctness metrics. The figure is partly based on in [Haddad et al. 2011].

A further challenge is that many objects of the SuI system architecture are *unmanaged* [Ouedraogo et al. 2008]: they are not under the administration of the stakeholder carrying out security management and/or measurement. Direct security measurements are not possible for an unmanaged object. However, a *trust value*, a certain amount of trust that the security level of the object is at an adequate level, can be associated with the object. This trust can be based on, e.g., assurance claims carried out by a representative of the unmanaged object or by a third party. It can also be based on reputation parameters [Savola, Pentikäinen and Ouedraogo 2010].

Security-measurability-enhancing mechanisms are design choices, which increase the efficiency of adopting security measurement practices, and the availability and attainability of measurement results. They are crucial for efficient measurement architecture. Some examples of these are presented in [Savola and Heinonen 2011a].

2.2 Hierarchical Development of Security Metrics

The pilot used the hierarchical security metrics development methodology introduced in [Savola and Abie 2010]. This work introduced an iterative methodology for security metrics development, simplified in Fig. 3 to Security Metrics Development (SMD) stages. The methodology was modified in this study to better fit the practical RA and Agile software development practices carried out at Ericsson. The methodology is based on the decomposition of SOs. The original idea of decomposing security objectives was proposed in [Wang and Wulf 1997].

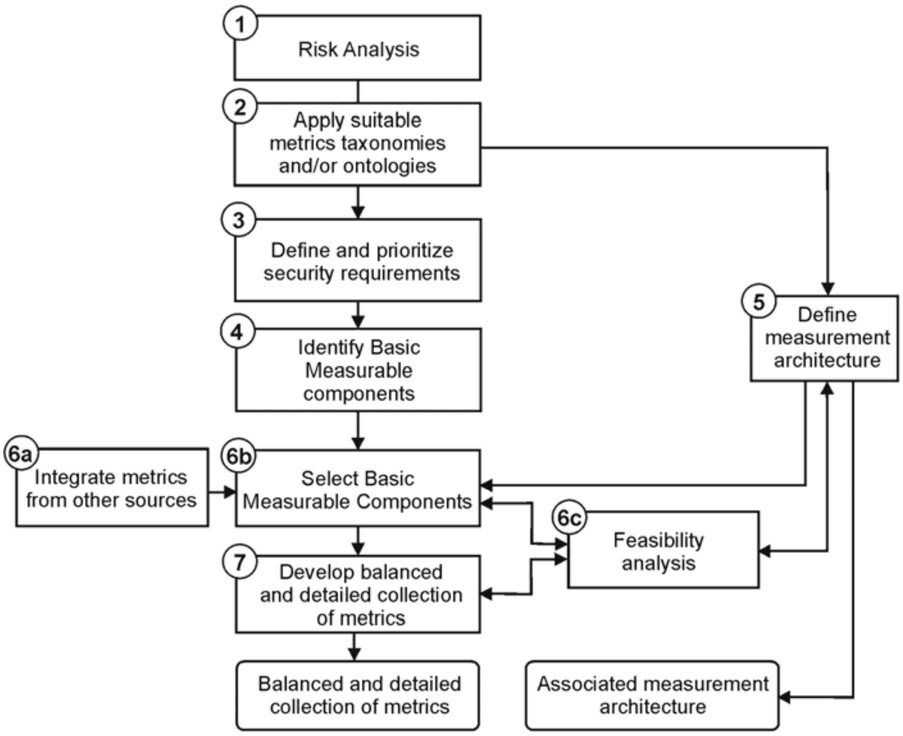
1
Risk Analysis
2
Apply suitable metrics taxonomies and/or ontologies
3
Define and prioritize security requirements
4
Identify Basic Measurable components
5
Define measurement architecture
6a
Integrate metrics from other sources
6b
Select Basic Measurable Components
6c
Feasibility analysis
7
Develop balanced and detailed collection of metrics
Balanced and detailed collection of metrics
Associated measurement architecture

Figure 3: A simplified security metrics development approach based on [Savola and Abie 2010]

The process of Fig. 3 aims at producing (i) a balanced and detailed collection of security metrics, and (ii) associated measurement architecture. In the following, the stages are referred by SMD*n*, where *n* is the stage identifier. Fig. 3 is identical to the description in [Savola and Abie 2010] with the Quality-of-Service (QoS) metrics branch removed, and the term 'threat and vulnerability analysis' replaced by 'Risk Analysis'. RA refers here to architectural-level risk analysis that can be separate, iterative and more frequent-cycle activity from an organizational RM activity. In addition to threat and vulnerability analysis, the terms Architectural Risk Analysis [McGraw 2006] and threat modeling [Howard and LeBlanc 2003] have been used.

Fig. 4 illustrates a highly simplified example of decomposition of the main objectives related to the effectiveness of authentication functionality, based on [Wang and Wulf 1999]. Note that many important practical authentication objectives, such as legal compliance, are not mentioned in this simplified decomposition. Basic Measurable Components (BMCs) are leaf components of a decomposition that clearly manifests a measurable property of the system [Savola and Abie 2010]. The BMCs of Fig. 4 are: Authentication Identity Uniqueness (*AIU*), Authentication Identity Structure (*AIS*), Authentication Identity Integrity (*AII*), Authentication Mechanism Reliability (*AMR*) and Authentication Mechanism Integrity (*AMI*) [Savola and Abie 2010]. The figure is informative, only core objectives being shown. It is assumed that the ID (Identity) concept and authentication mechanism contribute essentially to the security effectiveness of authentication.

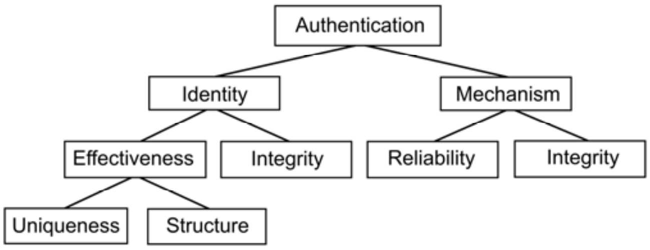

Figure 4: An example authentication effectiveness decomposition based on [Wang and Wulf 1999]

In practical systems, authentication objective decomposition may easily consist of tens or hundreds of sub-nodes, because security configuration correctness and security testing metrics in particular incorporate a lot of details in various infrastructure objects and security protocols. The MVS screenshot in Fig. 7 of Appendix shows an example of how easily the decomposition models can grow in detail. The metrics in this model are still at an abstract level yet contain dozens of sub-nodes.

Security measurement values can be aggregated, e.g. in the form of a weighted sum. Aggregation is troublesome; relying blindly on aggregation can result in the loss of important information. For example, if the measured values under *AIU* are not sufficient (indicating that identity credentials are shared in a way that binding to the real identity is not possible) while other branches result in acceptable values, aggregation results can lead to a false sense of security; they *oversimplify* the situation. Increasing the weight of *AIU* does not help in this case, because similar situations can arise from other branches.

2.3 Security Metrics Model Management by Visualization

In practice, hierarchical SMMs can be constructed based on the RA results and prioritized SOs in the following way. The SMM construction is started from the SOs associated with each risk, which are placed immediately below the root of the hierarchy in the model. The choice of risks to be shown at the highest-level and their order depends on the risk priority. Relevant SCs are listed below the SOs as sub-nodes. Further stages are built based on identifying the most essential goals and subgoals that contribute to the security correctness, effectiveness and/or efficiency. See details and examples of decomposition in [Savola and Abie 2010].

The benefits of visualization for human cognition can be utilized to increase the manageability of security metrics collections. Card et al [Card et al. 1999] proposed methods in which visualization can amplify cognition by perception, such as increasing memory and processing resources by allowing the storage of massive amounts of information in a quickly accessible form and reducing searching by grouping information together. The core needs of security metrics visualization can be summarized as [Savola and Heinonen 2011b]: (i) structured security metrics entities, "building blocks" are needed, (ii) possibility of modeling the relationships between SOs and measurement results, (iii) the problem of oversimplification should be alleviated, and (iv) there should be enough support for automation solutions, including measurement probes and security-measurability-enhancing mechanisms.

In our earlier work [Savola and Heinonen 2011b], we introduced a modeling and visualization tool called Metrics Visualization System (MVS) for the management of hierarchical security metrics and measurements. It was used in the pilot during the iterative modeling phase. In the MVS *security metrics model* SMM, the basic building block is the *security metrics node* SMN. In an SMM, SMNs form a hierarchy. The same sub-hierarchies can be attached to different security controls at the higher level. All SMNs in the SMM have the same default property fields: a distinctive name, metric confidence value (range 0…1), operation specification (logical expression), threshold criteria and associated visualization, poll frequency field for automated measurements, and enable/disable flag for operation value evaluation. JavaScript scripting language is used for logical operations. All nodes can be colored or left blank. The default coloring scheme of the MVS imitates traffic lights: red stands for insufficient level, yellow for intermediate level, and green for sufficient level. More details of the MVS tool are available from [Savola and Heinonen 2011b].

3 Context of the Pilot Study

The context of the pilot study consists of (i) the technical SuI, and (ii) the adaptation of Ericsson's RA Process to Ericsson's Agile SW development process. We refer to this adaptation as RA/AD (Risk Analysis/Agile Development). No long-term experiences of the feasibility of RA/AD were available at the time of the pilot. The pilot focused on the analysis of integration of metrics development and use in RA/AD, but implications from the technical SuI are discussed where applicable.

3.1 Technical System under Investigation: Ericsson's Media Gateway

The pilot study was initiated by identifying a product development team available for it. This team focused its efforts on the secure development of a Media Gateway (MGw) product that is part of a Mobile Softswitch Solution [Ericsson 2009]. More details, such as SIP-I (Session Initiation Protocol with encapsulated ISDN User Part) and SIP NNI (Network to Network Interface) reference architecture including MGw are discussed in [Baldwin et al. 2010]. The SuI to be addressed in the pilot study was further narrowed down to a specific part of the above-mentioned system.

Ericsson generally uses a three-plane reference architecture in its R&D, described in [Eschenbrücher et al. 2004]. The architecture consists of a matrix of horizontal *security planes* (i) end-user security plane, (ii) signaling and control security plane, and (iii) O&M (Operation and Maintenance) plane, and vertical security *services*. In addition, *security domains* are a third dimension. A more detailed description can be obtained from [Eschenbrücher et al. 2004].

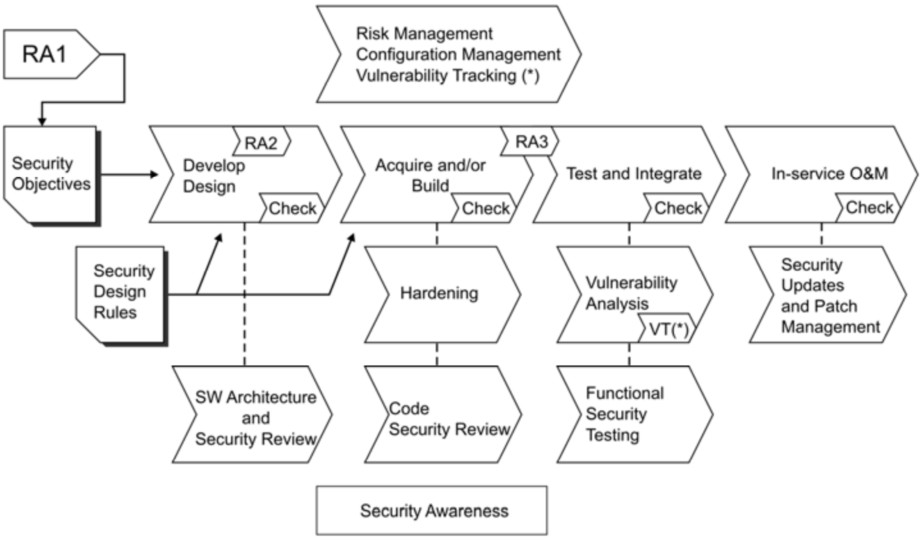

Figure 5: Illustration of Ericsson's RA process in Waterfall SW development.

3.2 Risk Analysis Process at Ericsson

In product development, the objective of RA is to understand what risks the product may encounter in its deployment environment. The RA outcome is used to make business decisions and to choose between implementation alternatives. Ericsson's RA process comprises three iterative instances of RA sessions: (i) RA1, is conducted when product requirements are defined, with the main focus on where the business value chain is subject to risks, (ii) RA2, when the product is being specified, and (iii) RA3, when the product is being designed and verified. The main focus in RA1 is on the points where risks reside in a business value chain. RA2 focuses mainly in analyzing the risk environment from product or solution feature perspective, and RA3 on verifying how the identified risks have been mitigated and what are the residual risks.

The RA process interacts with other activities defined in the Secure Design Lifecycle, as illustrated in Fig. 5. RA1 begins with a Value Chain Analysis (VCA), where the product is defined in the relevant business context. After this, the product requirements are analyzed from a business risk perspective. During RA1, the relevant risks are identified and prioritized, and mapped into SOs, taking into account other requirements, such as legal constraints and best practices. The outcome of RA1 is a set of SOs which can be formulated as product and security requirements, and a list of acceptable risks. The term 'acceptable risk' refers to a risk that is known but needs no further action. RA2 investigates the technical impact of risks identified at RA1 that need to be mitigated. New or out-dated risks since RA1 are taken into account. RA3 analyses the product as it was actually implemented, and verifies the security posture of the product, again updating any changes that have occurred since the previous stages. Vulnerability Analysis and Penetration Testing are closely linked to RA3.

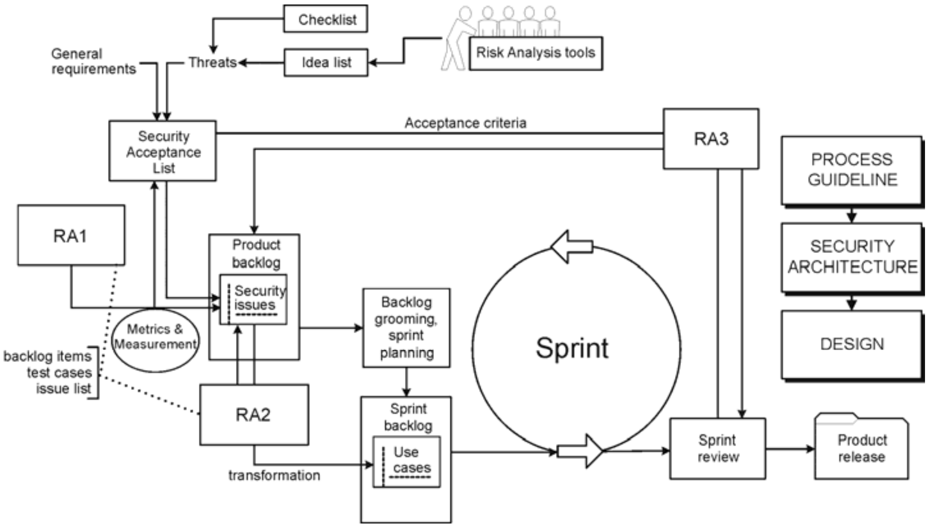

Figure 6: Illustration of the Agile SW development process used in the pilot study

3.3 Agile SW Development Process in the Pilot Study

The Agile software development process deployed in the pilot was a combined Scrum [Schwaber and Beedle 2001] and Kanban [Anderson and Reinertsen 2010] Agile adaptation that Ericsson Finland developed with the help of many contributors in the Agile community. Agile methods in general are challenging from a security perspective. In particular, security work should not create *waste*. In Agile-based development models, eliminating waste, such as unclear requirements, insufficient testing practices, unnecessary code, bureaucracy and human communication problems, is an important principle. To support Agile methods, security requirements must be translated into negative user stories, Misuse Cases (MCs), and into a set of non-functional requirements. Fig. 6 shows the Secure Agile workflow used in the pilot. The RA activities discussed above are also shown. Security metrics are essential in evaluating the effectiveness of integrated security activities in Agile SW development. A core element in the workflow is the Security Acceptance List (SAL). It establishes security criteria that a product should pass. In this way, it is ensured that security is regarded as an inherent part of the development process. The criteria from SAL are transferred to the product backlog, ensuring that security issues are handled adequately in sprint planning and grooming. Throughout the process, care should be taken that security work and solutions are efficient in reducing waste. An Acceptance Verification List (AVL) is used for the management of product acceptance criteria.

4 Iterative Modeling Part

In this section, we discuss our experiences from the investigation of developing and using security metrics in RA/AD. In addition, a simplified illustrative example is presented of a hierarchical SMM developed in the study. The SuI addressed in the pilot study was an enhanced version of an existing MGw product. Because there were no earlier SMMs, modeling started from scratch. From a security perspective the earlier product had many differences compared to the new one. Consequently, security-related RA/AD activities were carried out as if the SuI were a new product.

During the pilot, (i) several partial hierarchical SMMs for the SuI were developed using the MVS tool, and (ii) potential ways of integration of SMMs to the RA/AD were investigated. Exhaustive security metrics modeling was not carried out. Instead, modeling was carried out in sufficient detail to obtain experiences of how security metrics development and use should be integrated into the RA/AD in order to obtain benefits from it. Different security planes typically require different SMMs. The modeling focused on factors that enable security effectiveness. Security efficiency was investigated from the perspective of reducing waste in the RA/AD. SMMs were developed and their use was investigated by researchers in close interaction with Ericsson's product managers, risk analysis experts and developers.

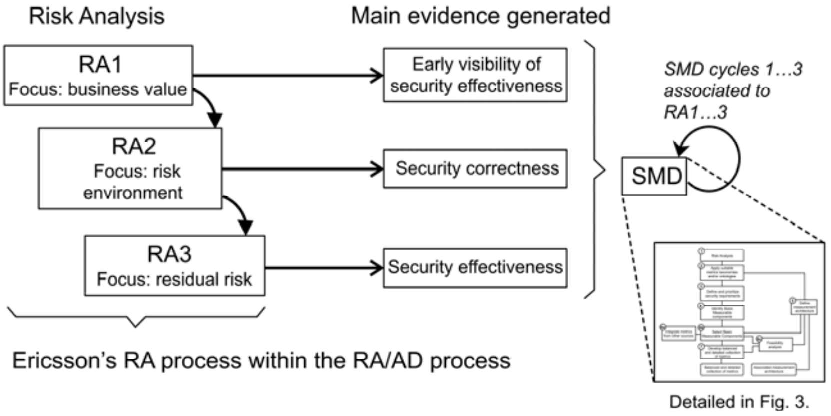

Figure 7: Overview of the relationships between RA and SMD stages, and the main evidence generated from metrics modeling associated with each RA stage.

It became evident that the SMD process presented earlier needed to be enhanced in order to show how to handle security effectiveness, efficiency and correctness dimensions, and how to use them during the different stages. The availability and attainability of data related to these objectives differ at different RA/AD phases and uses of the resulting product. In practice, the most efficient way to arrange iteration is to tie the development and use of risk-driven security metrics to different RA phases, i.e. RA1, RA2 and RA3, in Ericsson's methodology. The phases are 'cycles' of SMD.

In the following, we present in detail our experiences from SMM development at each RA phase or cycle. The main findings are summarized with the results from expert interviews in Section 6. Fig. 7 shows an overview of the relationships of RA and SMD stages to be discussed.

4.1 RA1 – Early Visibility of More Detailed Security Issues by Metrics

SMD1 is closely related to the RA1. This phase concentrates on business-level issues. Later, during the RA2 and RA3, as the RA outcomes will be iterated, SMMs also need to be iterated, offering feedback to SMD1. The output from RA1 is prioritized list of security risks and SOs associated with them. Therefore, in practice RA1 'includes' SMD3. In the pilot, SMD3 was not an explicit a stage outside of RA1.

According to our experiences, *during RA1 SMMs are at their best in offering systematization and early visibility of more detailed security issues to the RA*. This information can be used to reduce the gaps and biases with regard to security effectiveness objectives (see Fig. 2). However, there is no need to construct too detailed SMMs. If earlier SMMs and/or taxonomies or ontologies are available, they can be reused in the models being built. This should be done carefully, as earlier models might include implementation details that are not applicable and can potentially bias the RA outcome.

During RA1, business-level information was iterated in brainstorming sessions, utilizing (i) visualizing mind-maps, (ii) VCA diagrams, and (iii) detailed textual RA documentation of an earlier version of the SuI. Future efforts would benefit from tools making it possible to link risk information in these documents, including the resulting SMM in MVS. Related tools and methods were proposed by [Frühwirth et al. 2010] in the context of SW process improvement. Unclear requirements, a typical waste in security work, can be avoided, because linking enhances risk-driven security issue traceability and management of risk information throughout the RA/AD activities.

Risk prioritization was carried out by a combination of expert voting and an iterative follow-up analysis. Some of the prioritized risks were selected to be modeled in SMMs. It was not feasible to obtain enough critical information from all the identified risks due to the timing constraints of the pilot project. Prioritized security risks to the SuI identified during RA1, abstracted here, included (i) unauthorized access to a configuration file, (ii) unauthorized disclosure of user credentials, (iii) modification of H.248 [ITU-T 2005] signaling, (iv) Internet Protocol (IP) address spoofing, and (v) eavesdropping on user plane data in transit.

SMD2 offers valuable information not only for the SMMs but also the RA. Depending on the RA process, SMD2 can be part of the RA or the SMD. More explicit and detailed taxonomies and ontologies are needed for SMMs than for the RA. In the pilot, we utilized authentication and authorization taxonomy work carried out earlier in [Savola and Abie 2010] and [Savola, Pentikäinen and Ouedraogo 2010]. SMD4 and SMD6b are closely connected 'routine' SMD stages: BMC identification and selection are connected more to the actual metrics activities than to RA activities. During the pilot, the available taxonomies guided this task.

Practical constraints, especially the lack of detailed information about the system architecture, showed that the rest of the SMD stages should only be tentative during the RA1. SMD5 includes only planning, because the actual system architecture is not defined at that phase. However, it is important that measurement architecture requirements are communicated to the actual SuI design, with suitable security-measurability-enhancing mechanisms. Although other types of metrics relevant to security measurements, such as QoS metrics, are not typically available during RA1, SMD6a can be tentatively planned. Utilization of other types of metrics can be planned in more detail during the actual design phase. The SMD6c work comes hand-in-hand with SMD5, requiring a more detailed system architecture knowledge. Therefore, only intuitive feasibility analysis was carried out in RA1. In the development of a new product, SMD7 is not applicable during the RA1, because details are not available. SMMs from an earlier version can potentially be used.

During RA1, *the need for security effectiveness and efficiency information is at its greatest* because of the need for making the right choices as early as possible to ensure an adequate security level. However, not much information is available during this phase because no penetration test results or incident information are available for the resulting product or a close-to-complete version of it. Exploitability and vulnerability information found from open databases can be considered to be *indirect* security effectiveness evidence, and can be used already during RA1. Because of the unavailability of effectiveness information, the SMMs constructed during RA1 focus on risk and countermeasure description, and tentative correctness issues.

The SMMs constructed during RA1 of the pilot included correctness metrics based on telecommunications standards and regulations related to the SuI, and metrics related to the Ericsson's Reference Architecture. The SMM included different administration domains, resulting in the use of trust values. For example, the ID management branch (establishment and maintenance of ID) in the authentication solution of the SuI is carried out by a third party, a different administration domain.

4.2 RA2 – Metrics as Enablers for Correct Security Design

During RA2, the RA practices are continued at a more technical level compared to RA1. This makes it possible to increase the granularity of the SMM compared to the initial model from RA1. In the RA2 of the pilot, the first SMD stages were iterated, aiming at more detailed SMM. The conclusion from RA1 discussed above, that SMD5, SMD6a, SMD6c and SMD7 cannot be carried out at a detailed level, resulted in a situation where the main effort required to these stages is focused on RA2.

SMD5 requires more in-depth knowledge of the SuI design. The measurement architecture and data gathering should be designed "hand-in-hand" with the SMM. The measurement architecture is typically part automated and part manual. In the pilot, it was not possible to deploy automatic measurements due to constraints in the existing infrastructure and the nature of the pilot study. The measurement architecture solution used relied on manual information gathering. Measurements of the SMM were gathered mainly from configuration and deployment documentation.

During RA2, it is crucial to develop metrics for security configuration and operational deployment correctness. Compliance with legal, regulatory and organizational policies is also a part of the correctness. *It is evident that a few metrics are not able to represent sufficient correctness information; a collection of them is needed.* Because no testing results are available during RA2, the SMMs rely mostly on this information. Results from initiatives like Security Content Automation Protocol (SCAP) [Barrett et al. 2009] can be used in the gathering and management of the above-mentioned data. Security configuration correctness checking can be arranged as part of the Configuration Management with proper documentation and verification. Investigation of this was not part of the study. Therefore, the results discussed here do not apply to automated measurement. However, our previous work ([Savola and Abie 2010], [Savola and Heinonen 2011a] includes solutions for that kind of measurements.

Feasibility analysis (Stage SMD6c) should focus especially on correctness, measurability, meaningfulness and usability of the metrics and the overall metrics collection. Despite several feasibility criteria, the main purpose is to find answers to the questions '*Can I trust these security metrics?*' and '*Does the use of these security metrics bring benefits?'* A process for the feasibility analysis of security metrics was introduced in [Savola 2010]. In the pilot, only a brief initial feasibility analysis was carried out, focusing mainly to the correctness of the metrics modeled. It is important, however, to devote enough time to this kind of analysis if metrics are to be used more extensively for decision-support purposes. Our experiences from the pilot raised the concern that it may be difficult in practice to allocate sufficient resources to metrics feasibility analysis. In future efforts, tools and methods designed for this purpose are needed. A full feasibility analysis cannot be carried out as a separate standalone stage, as suggested in the original SMD process. SMD6c requires iterative input from different RA and RA/AD phases. The analysis can come to different kinds of conclusions depending on the type of security metrics use.

SMD6a is an optional stage. It is meant for the re-use of non-security metrics. As shown in [Savola and Abie 2010], QoS metrics are closely related to the availability objectives. The potential of QoS metrics to become part of SMM should be evaluated, if they are available. Other examples of metrics used in telecommunications applicable to security objectives are traffic, load and performance metrics. While no additional metrics were identified in the RA2 phase of the pilot, it is expected that such metrics will become available and attainable later in the product development. The tracking of other metrics to be re-used and incorporated in the SMM is an activity that should be considered along with the SuI becoming more mature.

The first iteration of SMD7 can be carried out during the RA2. However, further details and balancing need to be investigated after more effectiveness information becomes available during RA3. Because only partial SMMs were used in the pilot study, a detailed and balanced collection of security metrics was not achieved.

4.3 RA3 – Incorporation of Security Effectiveness Information to Metrics

RA3 focuses on the verification of the security implementation, taking input from Vulnerability Analysis and Penetration Testing activities carried out during design sprints and integration tests. Security effectiveness metrics relevant to RA3 relate to the remaining residual risks and to the degree of difference in identified risks in comparison with RA2 and RA1. Moreover, the degree of security compliance (part of security correctness) and process quality (part of security efficiency) are addressed in RA3. As a result, the RA3 outputs compliance information of the design towards SAL, a residual risk list, and, optionally, feedback to previous RA stages in the form of new identified risks and potential risk classification errors.

Security effectiveness information plays a central role at this stage, because more and more of it is available during the course of RA3. Security indications from different *security effectiveness enabling factors* should be gathered to the SMM. Security metrics bring benefits to the RA3 work, if enough effectiveness metrics are represented in SMM and actual effectiveness measurement results can be obtained.

During the RA3, the main security effectiveness indications come from testing activities, and especially from Penetration Testing. Note that security incident information during the actual use of the SuI indicates the level of security effectiveness more directly than testing results. In testing, it is challenging to arrange operational conditions similar to actual use. Even the most realistic tests have limitations in this regard. However, some security incident information may become available during the R&D.

During the pilot, the possibilities were investigated of incorporating test results into SMMs were investigated. For instance, if the tests show failures in the authentication mechanism, the types of failures can be associated with the relevant SMNs in the authentication branch. Using the resulting SMM, configuration, architecture, implementation or deployment of the relevant part of the mechanism can be fixed in the SuI. *According to our experience, the test results carried out during the RA3 are often at different detail levels compared to the security correctness information of RA1 and RA2*. We did not anticipate this challenge when planning the pilot. We suggest coping with this challenge by identifying the relevant SMNs and modifying the metrics inside them in order to incorporate the new type of indications. However, test results may be treated alternatively as separate branches in the SMM. Better tool support, for coping with the new evidence in RA3 with regards to the SMM from earlier phases, would be beneficial.

4.4 Simplified Example of Security Metrics Model

In the following, we present a simplified SMM for a risk identified during the RA – unauthorized access to a configuration file. The main security control for this risk is authorization, which is divided into (i) authentication and (ii) access control. The highest levels of the SMM are shown in the MVS tool screenshot of Fig. 8 in Appendix A, the lower levels, the access control branch, and coloring being suppressed for clarity.

The authentication branch of the SMM follows the taxonomical approach in Fig. 3, assuming that the core properties contributing to the authentication effectiveness are the ID strength and the strength of the mechanism. Especially the ID branch contains trust values as the leaf measurements because the IDs are managed outside of the administration domain. There are two main methods for obtaining indications of the authentication effectiveness: (i) security assurance levels, and (ii) operational effectiveness measurements. The former method is mainly applicable during RA2 and RA3, and the latter one during RA3 and the use of the SuI. Security assurance levels for authentication are based on a suitable taxonomy, such as the Electronic Authentication Guideline by the U.S. National Institute of Standards and Technology (NIST) [Burr 2008]. It classifies the Level of Assurance (LoA) according to four different levels ranging from 1 to 4. The guideline applies a weakest-link approach: the resulting overall LoA is the *lowest* LoA level, which is reached from five metrics categories: registration and issuance, tokens, token and credential management, authentication process and assertions. The LoAs represent 'best-practice' reference levels for authentication mechanisms. Consequently, they do not represent authentication strength based on the operational security effectiveness. Using the BMCs of Fig. 3, *AIU*, *AIS*, *AII*, *AMR* and *AMI*, during the operation of the SuI is an example of operational authentication effectiveness measurement.

5 Semi-Structured Interview Part

After the pilot, a group of R&D personnel working on the pilot project for Ericsson (5 persons) and a group of 5 security researchers were interviewed about the potential benefits of security metrics and the preferred visualization method of them. The interviews were semi-structured and anonymous. The questions (Q) are listed in Appendix B.

All respondents shared the opinion that there are benefits from measuring security (Q1). Most of them saw the benefits in determining or improving the security level of the SuI. The main difference between practitioners' and researchers' answers was that all the practitioners emphasized compliance (with legal and industry regulations, customers' needs and organizational policies), whereas 80% of researchers emphasized the metrics' ability to offer a high-level overview of security. Only one respondent from the researchers emphasized compliance. The difference may arise from the fact that product development in the software industry is typically very requirement-driven. The benefits from measuring security and the extra burden from this (Q2) were seen currently to be balanced (5/10), or there is greater burden (3/10), according to the respondents. One respondent answered that currently there are no benefits and one had no opinion on this. 70% or the respondents expect more benefits than extra burden in the future. Two respondents thought that the benefits and burden remain balanced and one had no opinion. In the answers to Q3, most of the interviewees (6/10) preferred Method 5. Moreover, Method 1 (2/10) and Method 4 (1/10) were seen also the most important. Both respondents preferring Method 1 prioritized Method 5 as the second best. Method 5 was seen to be beneficial especially in communication. For example, if a report indicating that O&M security is in red, yellow or green, the immediate reaction would be to see more details explaining that outcome. The preference for Method 1 can be explained because it is closest to the current practices in industry.

6 Enhanced SMD Process for RA/AD and Benefit Analysis

In the following, we propose practical enhancements to the SMD process presented in Fig. 2, and analyze the benefits and challenges of the use of security metrics, based on the findings from the modeling study and expert interviews. The enhancements are shown in in the first part of Table 2 as a matrix of RA and SMD phases. During the pilot, it was found that RA phases constitute iterative 'cycles' for SMD development. The result from RA1 is a prioritized collection of metrics, from RA2 a metrics collection with more details than RA1, and from RA3 a balanced and detailed one. It is proposed that security metrics be developed in three main iterative cycles, each focusing on different type of evidence as illustrated in Table 2.

SMD stage	**Proposed modifications to the SMD process of Fig. 2**		
	RA1	**RA2**	**RA3**
Evidence in focus	Applicable early evidence of any type	Security correctness evidence	Security effectiveness and correctness
SMD1	RA of RA1	RA of RA2	RA of RA3
SMD2	risk-driven taxonomy work	correctness-driven taxonomy work	effectiveness-driven taxonomy work
SMD3	not needed explicitly	not needed explicitly	not needed explicitly
SMD4 / SMD6b	first iteration of the stages	second iteration based on correctness needs	third iteration based on effectiveness needs
SMD5	planning, taking into account security-measurability-enhancing mechanisms	design and use of measurement architecture for the current SMM	design and use of measurement architecture for the current SMM
SMD6c	intuitive feasibility analysis	first iteration of feasibility analysis	second iteration of feasibility analysis
SMD7	not applicable for a new product; earlier SMMs used for existing ones	first iteration of balanced and detailed SMM	second iteration of balanced and detailed SMM
SMD6a	other metrics may be integrated at any phase when they become available		

Interaction point	**Benefits from by the use security metrics and measurements**	
	Security effectiveness	**Security efficiency**
RA1 / product management (new product)	Better systematization, granularity and early visibility of detailed-level security issues	Decision support for Return On Security Investment (ROSI) calculations.
RA1 / product management (new version)	Higher-quality RA through the use of earlier SMMs	Waste reduced by the reuse of earlier SMMs
RA2 / construction of SAL and MCs	Better systematization and traceability between RA results and product requirements	Waste reduced in the effort of mapping RA results and product requirements
RA2 / initial AVL and SAL	Residual risk is illustrated in SMM in a straightforward way	Waste reduced by the need of less communication of residual risks
RA3 / verification of MCs	Better effectiveness evidence by systematic management of test and (incident) information	Waste reduced by increased clarity of effectiveness objectives
RA3 / product backlog	Better systematization, traceability and availability of effectiveness evidence	Waste reduced by discarding backlog items not meeting effectiveness/efficiency criteria
Product release	Evidence of RA and security effectiveness quality. Customers have a higher transparency of security solutions.	*R&D*: systematic feedback to new R&D efforts increasing efficiency *Customers*: increased effectiveness-efficiency ratio
Security updates and patch management	Mechanisms which increase efficiency of adopting security metrics and availability and attainability of measurements	Waste reduced by possibility of systematic monitoring aiming at reduction of the average time/costs-to-patch.

Table 2: Proposed modifications to the SMD process of Fig. 2. (RA stages in Fig. 5), and analysis of benefits from using security metrics and measurements in RA/AD.

The cycles are cumulative: new metrics are added to the existing SMMs at each iteration. Benefits from the use of security metrics and measurements are analyzed in the latter part of Table 2, structured by *critical interaction points* in RA/AD of the many potential benefits listed above, there are a lot of challenges, such as: (i) extra work needed for security metrics modeling, (ii) lack of usable and efficient tools and methods for metrics development and management, (iii) methods for utilizing earlier SMMs in such a way that these do not guide decision-making in the wrong direction, (iv) lack of automated verification tools, (v) undeveloped practices of tagging security issues in backlog and requirements, (vi) lack of information sharing between the product developers and users of the product, and (vii) lack of useful taxonomies and ontologies for security metrics development.

7 Related Work

The state-of-the-art lacks widely accepted and well-validated security metrics approaches, because security is often considered to be an "add-on" property, the security research field itself is in its infancy, and there is lack of suitable data to be used in metrics development [Savola 2010]. Wang Wulf [Wang and Wulf 1997] introduced a pioneering security metrics development approach by decomposition of security objects. Their approach suffered from the lack of validation in realistic cases and larger hierarchies, both of which are addressed in our study. The Goal Question Metric (GQM) software development approach [Basili et al. 1994] also relies on hierarchical metrics. However, GQM is a general framework and primarily intended for software metrics. It is applicable to security too. The metrics development approach discussed in this study can be integrated into a GQM approach. The CELTIC Eureka project Building Security Assurance in Open Infrastructures (BUGYO) Beyond has developed novel solutions for the automation of gathering security (configuration) assurance data [Kanstrén et al. 2011]. This approach can be integrated into SMD5. Surveys of security metrics approaches can be found in [Bartol et al. 2009], [Hermann 2007], [Jaquith 2007], [Savola 2010], and [Verendel 2009].

Another important consideration is that there have not been many tools available for the management and/or visualization of security metrics and measurements. Our MVS tool is a pioneering tool in this regard. However, there are tools and frameworks available for the visualization of security-related data and visualization of information in general. A lot of research has been conducted in the field of information visualization in general, and a variety of tools and frameworks have been developed in order to visualize different properties. Typically general visualization tools do not answer to the core needs of security metrics visualization discussed earlier.

8 Conclusions and Future Work

The integration of hierarchical security metrics in the context of Risk Analysis and Agile SW development has been investigated in an industrial pilot study carried out at Ericsson Business Unit Networks in Finland. In the pilot, security metrics models of a real product under development were developed at a level detailed enough to offer practical experiences. Automated information gathering was not investigated.

The results show that security metrics have great practical potential, especially when there is a need to ensure the security implementation of a software product is systematically based on risk-driven objectives. The measurements offer early visibility of security effectiveness and efficiency during security-critical phases of R&D, and support security assurance activities. Early visibility helps especially in reducing gaps and biases in security correctness with respect to security effectiveness. It is evident from the pilot that individual security metrics do not offer enough benefits; rather, collections of them are needed. Hierarchical metrics models make it possible to relate the security objectives with detailed measurements. Suitable metrics management and visualization tools are needed to manage larger metrics collections. Security metrics mitigate the problem of waste due to security requirements by enhancing risk-driven security objective traceability during all the phases of R&D. Methods capable of visualizing the high-level security objectives and detailed measurements at the same time have especially practical benefits in easing the communication of risk-driven security issues.

An important challenge is that not much security effectiveness evidence is available during the first iterations of Risk Analysis, when the need for it is at its greatest. Other challenges include the extra work needed for metrics development and the lack of advanced tools to support the management and use of metrics.

Our future work includes further analysis of security metrics in practical product development environments, with a focus on gathering value-based and more direct effectiveness information during the R&D phase and the longer-term actual operation of the system under investigation. We aim to further develop prototype tools to support metrics management. Such tools should support the structured gathering, prioritization, alignment, storage, retrieval and visualization of security metrics, measurements and related meta-information. The core research question remains: how can system stakeholders obtain sufficient and credible indications of security effectiveness as early as possible in product development and Risk Analysis.

Acknowledgments

The work presented here has been carried out in two research projects: the BUGYO Beyond Eureka CELTIC cluster project (2008–2011) and Cloud Software Program (2008–2013) launched by the Finnish Strategic Centre for Science, Technology and Innovation TIVIT Plc. We wish to thank our colleagues involved in these projects for their related work and for helpful discussions that made this study possible.

References

[Anderson and Reinertsen 2010] Anderson, D.J., Reinertsen, D.G., “Kanban – Successful Evolutionary Change for Your Technology Business,” Blue Hole Press, Sequiem, WA.

[Baldwin et al. 2010] Balwin, J., Ewert, J., Yamen, S., “Evolution of the Voice Interconnect,” Ericsson Review No. 2, 2010, 10–15.

[Barrett et al. 2009] Barrett, M., Johnson, C., Mell, P., Quinn, S., Scarfone, K., “Guide to Adopting and Using the Security Content Automation Protocol (SCAP),” NIST Special Publication 800-117 (Draft), U.S. National Institute of Standards and Technology, 2009.

[Bartol et al. 2009] Bartol, N., Bates, B., Goertzel, K. M., Winograd, T., "Measuring Cyber Security and Information Assurance: a State-of-the-Art Report," Information Assurance Technology Analysis Center IATAC, May 2009.

[Basili et al. 1994] Basili, V., Caldiera, G., Rombach, H.D., "The Goal Question Metric Approach," 1994.

[Burr 2008] Burr, W.E. et al. 2008. "Electronic Authentication Guideline," National Institute of Standards and Technology, U.S. Department of Commerce, NIST SP 800-63-1, Draft.

[Card et al. 1999] Card, S.K., Mackinlay, J.D., Shneiderman, B., "Readings in Information Visualization: Using Vision to Think," Morgan Kaufmann Publishers, San Francisco, CA, 1999, 686 p.

[Haddad et al. 2011] Haddad, S., Dubus, S., Hecker, A., Kanstrén, T., Marquet, B., Savola, R., "Operational Security Assurance Evaluation in Open Infrastructures", Proc. CRiSIS 2011, pp. 100–105.

[Ericsson 2009] "Efficient Softswitching," Whitepaper, Ericsson, 2009. 11 p.

[Eschenbrücher et al. 2004] Eschenbrücher, D., Mellberg, J., Niklander, S., Näslund, M., Palm, P., Sahlin, B., "Security Architectures for Mobile Networks", Ericsson Review No. 2, 2004, 68–81.

[Frühwirth et al. 2010] Frühwirth C., Biffl S., Tabatabai M., Weippl E., "Addressing Misalignment between Information Security Metrics and Business-driven Security Objectives," Proc. MetriSec '10.

[Hermann 2007] Herrmann, D. S., "Complete Guide to Security and Privacy Metrics – Measuring Regulatory Compliance, Operational Resilience and ROI," Auerbach Publications, 2007, 824 p.

[Howard and LeBlanc 2003] Howard, M. and LeBlanc, D., "Writing Secure Code," Microsoft, 2003.

[ISO/IEC 15408] ISO/IEC 15408-1:2005, "Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model," ISO/IEC, 2005.

[ISO/IEC 27000] ISO/IEC 27000:2009: Information Technology – Security Techniques – Information Security Management Systems – Overview and Vocabulary. ISO/IEC, 2009.

[ITSEC 1991] Information Technology Security Evaluation Criteria (ITSEC), Version 1.2, Commission for the European Communities, 1991.

[ITU-T 2005] International Telecommunication Union, Telecommunication Standardization Sector (ITU-T), "Series H: Audiovisual and Multimedia Systems – Infrastructure of Audiovisual Services – Communication Procedures – Gateway Control Protocol: Version 3," ITU-T Recommendation H.248.1, Geneva, Switzerland, 2005, 195 p.

[Jaquith 2007] Jaquith, A., "Security Metrics: Replacing Fear, Uncertainty and Doubt," Addison-Wesley, 2007.

[Kanstrén et al. 2011] Kanstrén, T., Savola, R., Haddad, S., Hecker, A., "An Adaptive and Dependable Distributed Monitoring Framework," Int. Journal on Advances in Security, 4(1&2), 1–19.

[Kanter 2004] Kanter, R. M., "Confidence: Leadership and the Psychology of Turnarounds," Random House, London, 2004.

[Kuusijärvi 2010] Kuusijärvi, J. "Interactive Visualization of Quality Variability at Run-Time", VTT Technical Research Centre of Finland, VTT Publications 746, 2010, 111 p.

[Marty 2008] Marty, R., "Applied Security Visualization", Addison-Wesley, 2008, 552 p.

[McGraw 2006] McGraw, G., "Software Security – Building Security In," Addison-Wesley, 2006.

[McPherson et al. 2004] McPherson, J., Ma, K.-L., Krystosk, P., Bartoletti, T., Christensen, M., "PortVis: A Tool for Port-Based Detection of Security Events", Proc. VizSE'04, 73–81.

[Ouedraogo et al. 2008] Ouedraogo, M., Khadraoui, D., de Rémont, B., Dubois, E., Mouratidis, H., "Deployment of a Security Assurance Monitoring Framework for Telecommunication Service Infrastructure on a VoIP System," Proc. NTMS '08.

[Savola 2007] Savola, R., "A Taxonomical Approach for Information Security Metrics Development," Nordsec '07 Supplemental Booklet of Short Papers, Reykjavik, Iceland, 11 p.

[Savola 2009] Savola, R., "A Security Metrics Taxonomization Model for Software-Intensive Systems," Journal of Information Processing Systems, Vol. 5, No. 4, Dec. 2009, 197–206.

[Savola 2010] Savola, R., "On the Feasibility of Utilizing Security Metrics in Software-Intensive Systems," Int. Journal of Computer Science and Network Security, 10(1), 230–239.

[Savola and Abie 2010] Savola, R., Abie, H., "Development of Measurable Security for a Distributed Messaging System," Int. Journal on Advances in Security, 2(4), 358–380.

[Savola and Heinonen 2011a] Savola, R., Heinonen, P., "Increasing Measurability and Meaningfulness of Adaptive Security Monitoring by System Architectural Design and Mechanisms," Int. Journal on Advances in Systems and Measurements, 4(1&2), 1–19.

[Savola and Heinonen 2011b] Savola, R., Heinonen, P., "A Visualization and Modeling Tool for Security Metrics and Measurements Management," Proc. ISSA 2011, 8 p.

[Savola, Pentikäinen and Ouedraogo 2010] Savola, R., Pentikäinen, H. and Ouedraogo, M., "Towards Security Effectiveness Measurement Utilizing Risk-Based Security Assurance," Proc. ISSA 2010, 8 p.

[Schwaber and Beedle 2001] Schwaber, K., Beedle, M., "Agile Software Development with Scrum," Prentice Hall, 2001.

[SecViz 2011] Security Visualization. http://www.secviz.org/node/89 [Jan. 15, 2012].

[Verendel 2009] Verendel, V., "Quantified Security is a Weak Hypothesis: a Critical Survey of Results and Assumptions," New Security Paradigms Workshop, Oxford, U.K., 2009, 37–50.

[Verendel 2010] Verendel, V., "Some Problems in Quantified Security," Licentiate Thesis, Chalmers University of Technology, Göteborg, Sweden, 2010.

[Wang and Wulf 1997] Wang, C., Wulf, W. A., "Towards a Framework for Security Measurement", 20th National Information Systems Security Conference, 522–533.

Appendix A: Figure 8

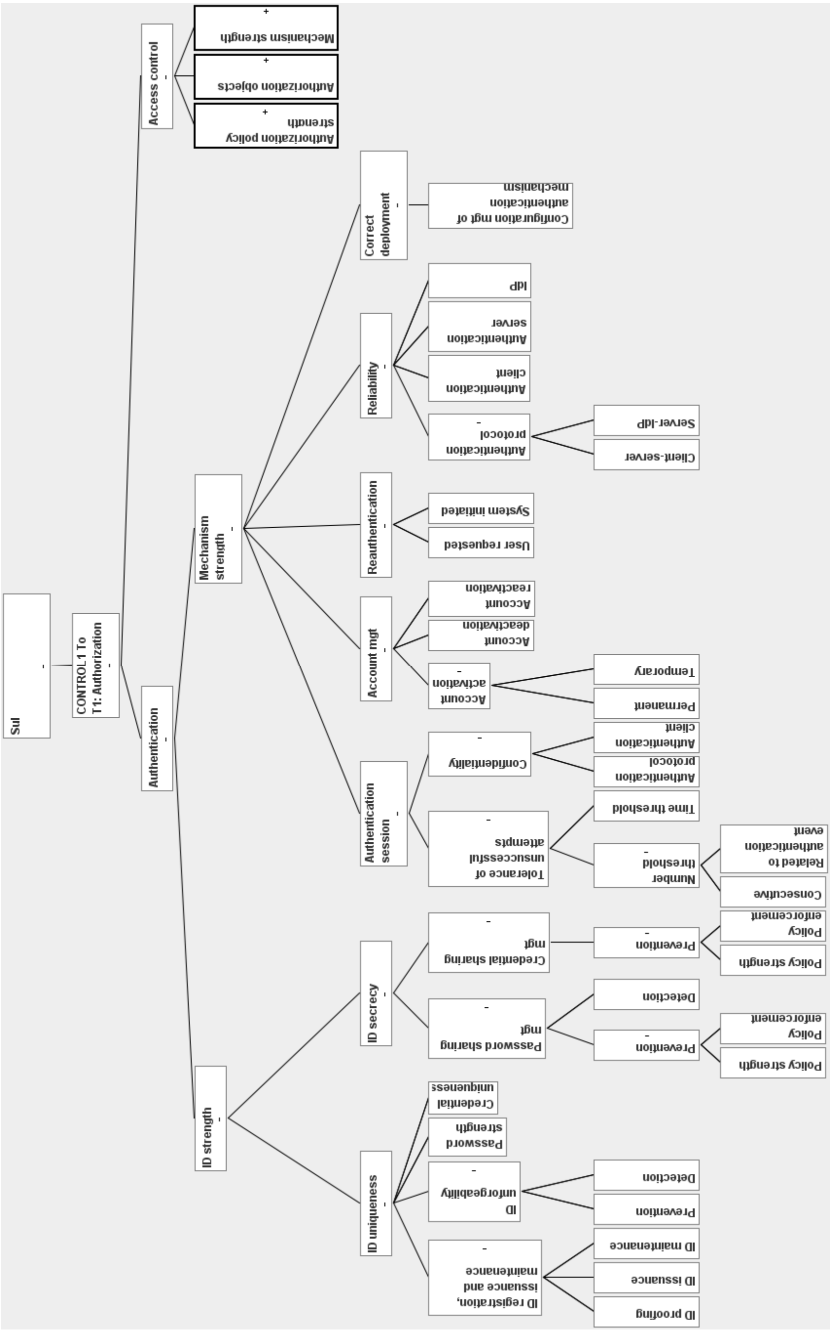

Figure 8: An MVS screenshot of the highest levels of the SMM described in the text

Appendix B: Questions of the Semi-Structured Interview

1. Q1: *Are there benefits from measuring security? Prioritize the three most important ones: (i) determine the security level, (ii) improve it, (iii) performance benchmarking, (iv) more efficient resource allocation, (v) base investment decisions, (vi) high-level overview of security, (vii) compliance with organizational policies, (viii) compliance with legal or industry regulations, (ix) compliance with customer needs, (x) not sure about benefits, (xi) no benefits.*
2. Q2: *Where is the balance between the benefits gained from measuring security versus the extra burden of conducting measurements (1) today, (2) in the future?*
3. Q3: *Which of the following methods would you prefer for the visualization of security metrics and measurements? (i) Method 1: Illustration of detailed information (plain measurements). Relationship to security risks is not shown. (ii) Method 2: Illustration of the assessed security level of high-level measurement goals with no explicit relationship to detailed measurement results, (iii) Method 3: Security level of high-level measurement goals and aggregated calculated measurement results from detailed measurements are shown by numbers. Detailed results are not visualized explicitly, (iv) Method 4: Aggregated calculation with visualization of details, illustrating high-level security measurement goals, detailed measurement results and aggregation results in the same view. Evidence is shown by numbers. Both detailed level and high-level metrics and measurements are available in the visualization approach. (v) Method 5: Same as the former method, but use traffic light type of coloring to show the security level in different branches of the metrics hierarchy. Emphasis is on visualizing the high-level information and detailed information in one view.*

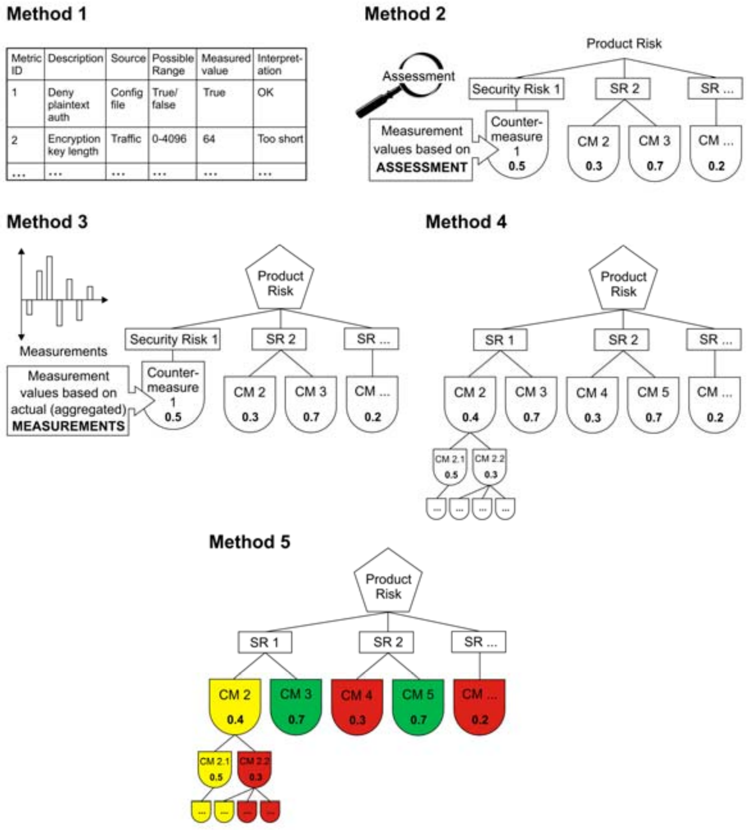

Figure 9: The figure associated with Q3

Appendix C: List of Abbreviations

Abbreviation	**Explanation**
AII	Authentication Identity Integrity
AIS	Authentication Identity Structure
AIU	Authentication Identity Uniqueness
AMI	Authentication Mechanism Integrity
AMR	Authentication Mechanism Reliability
AVL	Acceptance Verification List
B	Bias
BMC	Basic Measurable Component
G	Gap
GQM	Goal Question Metric
ID	Identity
LoA	Level of Assurance
MC	Misuse Case
MGw	Media Gateway
MVS	Metric Visualization System
NIST	U.S. National Institute of Standards and Technology
O&M	Operation and Maintenance
Q	Question
QoS	Quality of Service
R&D	Research and Development
RA	Risk Analysis
RA/AD	Risk Analysis / Agile Development
RM	Risk Management
ROSI	Return On Security Investment
SAL	Security Acceptance List
SC	Security Control
SCAP	Security Content Automation Protocol
SIP-I	Session Initiation Protocol with encapsulated ISDN User Part
SIP NNI	Session Initiation Protocol with Network to Network Interface
SMD	Security Metrics Development
SMM	Security Metrics Model
SMN	Security Metrics Node
SO	Security Objective
SR	Security Requirement
SuI	System under Investigation
SW	Software
VCA	Value Chain Analysis

Table 3: List of abbreviations.