DOI : 10.3745/JIPS.2009.5.4.197

Journal of Information Processing Systems, Vol.5, No.4, December 2009 **197**

A Security Metrics Taxonomization Model for Software-Intensive Systems

Reijo M. Savola*

Abstract: We introduce a novel high-level security metrics objective taxonomization model for software-intensive systems. The model systematizes and organizes security metrics development activities. It focuses on the security level and security performance of technical systems while taking into account the alignment of metrics objectives with different business and other management goals. The model emphasizes the roles of security-enforcing mechanisms, the overall security quality of the system under investigation, and secure system lifecycle, project and business management. Security correctness, effectiveness and efficiency are seen as the fundamental measurement objectives, determining the directions for more detailed security metrics development. Integration of the proposed model with risk-driven security metrics development approaches is also discussed.

Keywords: *Security Metrics, Security Objectives, Taxonomy, Correctness, Effectiveness, Efficiency*

1. Introduction

The increasing complexity and connectivity of software-intensive systems, products and services are boosting the needs for pertinent and reliable software security and trusted system solutions. Systematic approaches to measuring security are needed to obtain evidence of the security level and performance in systems, products and services. In addition, early security evidence will enable cost-effective secure software development. It is easier to make business and engineering decisions concerning security if sufficient and credible evidence of security is available.

The field of developing security metrics systematically is young. The complication behind the immaturity of security metrics is that the current practice of security is still a highly diverse field, and holistic and widely accepted approaches are still missing [1]. , attempts to measure security have only obtained limited success [2]. Lately, security metrics has become an emerging research area rapidly gaining momentum.

The main contribution of this study is to introduce a novel model for security metrics objective taxonomization of technical systems and discuss the motivation for it. The model systematizes and organizes security metrics development. We analyze the role of different emphasis areas and fundamental measurement objectives and show how the model can be integrated with risk-driven security metrics development activities. In our model, we have made a premeditated choice not to divide security metrics into technical, operational and organizational metrics, which is the most common classification.

The rest of this article is organized in the following way. Section 2 analyzes related work, and Section 3 gives a short introduction to security metrics. Section 4 presents our Security Metrics Objective Segments (SMOS) model, and Section 5 discusses the design of security metrics taxonomies with the help of the proposed model. Section 6 analyzes how the model can be integrated with the security metrics development process. Section 7 incorporates a discussion on the results and security metrics in general terms, and finally, Section 8 gives conclusions and finalizes the study with some future research questions.

2. Related Work

Our earlier work includes high-level security metrics taxonomy for ICT product development, emphasizing the roles of business management, information security management and security, trust, dependability and privacy of products, systems and services [1,3,4]. The work presented in this study is a generalization of our earlier work, emphasizing development and maintenance of technical software-intensive systems.

The WISSSR (Workshop on Information Security System, Scoring and Ranking) in 2001 [5] was an early venue and starting point for research on security metrics. The workshop was intuitively organized into technical, operational and organizational tracks. This provided an initial basis around which to organize taxonomy of security met-

Manuscript received November 2, 2009; accepted December 3, 2009.
Corresponding Author: Reijo M. Savola
* VTT Technical Research Centre of Finland, Oulu, Finland (Reijo.Savola @vtt.fi)

rics [6]. The U. S. National Institute of Information Standards and Technology (NIST) presents security metrics taxonomies in NIST Special Publication 800-26 [7] and 800-55 [8], suggesting the same three categories, and 17 sub-categories, mainly from an organizational perspective. In our SMOS model introduced in this article, technical metrics can be mapped to security-enforcing mechanisms and the security quality of system viewpoints, operational metrics to all three viewpoints, and organizational metrics to the secure lifecycle, project and business management viewpoint.

Vaughn *et al.* [9] propose taxonomy for information assurance metrics consisting of organizational security metrics and metrics for "Technical Target of Assessment". The authors divide the latter metrics into strength and weakness metrics – which are also part of the SMOS model, along with further characteristic dimensions.

Seddigh *et al.* [9] introduce an information assurance metrics taxonomy for IT network assessment in [6]. Their taxonomy divides the metrics space into three categories: security, Quality of Service (QoS) and availability. Under each of the categories they consider technical, organizational and operational metrics. We have also investigated the relationships between security, QoS and availability in [10], concluding that, from the security metrics point of view, QoS metrics can be used to obtain evidence of availability and, especially, possible Denial-of-Service (DoS) attacks.

Bartol *et al.* [11], Jaquith [12] and Herrmann [13] provide wide state-of-the-art reviews of security metrics and their development.

3. Security Metrics

The term "security metrics" has become a standard term when referring to security level, security performance, security indicators or security strength. It must be noted that the term "metrics" is used in a misleading way in the context of Information Technology (IT). This term implies that traditional concepts in metrology, as used in physics and other areas, equally apply to IT [2]. However, in IT there are a variety of unknown multi-disciplinary dependencies as well as doubts, subjective opinions and verdicts. In practice, the terms "security strength", "security indicators" or even "security measurement" are often used interchangeably with security metrics. Note that a *measurement result* indicates single-point-in-time data on a specific factor to be measured, while *metrics* are descriptions of data derived from measurements used to facilitate decision making.

3.1 Security Objectives

The most recognized security objectives are Confidentiality, Integrity and Availability (CIA) [14], often referred to as the "CIA model". Confidentiality objectives require that information is only accessible by those authorized to have access. Integrity is concerned with the accuracy and completeness of the information and mechanisms processing it. Availability objectives consider that authorized users have access to the information and associated assets when required.

Even though the CIA model has proved to be a useful guideline for developing practical security objectives and requirements, it has some limitations. For example, authenticity and non-repudiation of critical business transactions are not sufficiently underlined by the model. Consequently, a more concise collection of security objectives includes at least confidentiality, integrity, availability, authentication, authorization and non-repudiation, emphasizing more properly the goals of technical security-enforcing mechanisms [10]. Authentication mechanisms verify the users' identity by using their credentials. Authorization mechanisms are responsible for managing rights and access control based on an authorization policy. Non-repudiation mechanisms prevent users from later denying that they performed an action specified in detail in the non-repudiation requirements.

The International Telecommunication Union (ITU) [15] defines a wider set of security dimensions: access control, authentication, non-repudiation, data confidentiality, communication security, data integrity, availability and privacy. Moreover, there are several other factors that affect the security of information systems, such as accountability, audit, controllability, correctness, functionality, identification, recovery, reliability, robustness, safety, dependability, supervision and trustworthiness [16-18]. Avižienis *et al.* [19] present a detailed taxonomy of security and dependability attributes that can be used in the selection of adequate dimensions to be investigated.

3.2 Needs for Security Metrics

The users of security evidence include system and software developers, operational system managers, risk managers and the executive and organizational management of companies and other organizations. Decision support, monitoring and prediction assessments benefit from security metrics. Examples of using security metrics include [1]: risk management, comparison of security-enforcing mechanisms, software security assurance, security testing,

security performance, adaptive security monitoring and intrusion detection and prevention.

The intended use and target audience greatly affect the type of security metrics to be developed. If the goal is to develop security metrics for a human audience, such as the executive management in an organization, the final set of metrics should be clear to understand, and visualization of the results is crucial. However, more complex metrics structures and dependencies are allowed in calculations and automated decision making, testing and monitoring [10].

4. Proposed Taxonomization Model – SMOS

Yee [20] states that a multifaceted or multi-dimensional security metric is needed. This kind of metric or metrics can be composed of metrics emphasizing different relevant metrics objectives. In the following, we investigate them classified into *metrics objective segments*.

The security measurement target in this study is a (technical) *system*, meaning a software-intensive system, a networked system, a software module, a product or a *service*. To be precise, the purpose of a system is implemented as a service of the system acting as a provider, delivered to a user system [21].

To be precise, overall system is implemented as a service of a provider system to a user system[21].

Consequently, the service can be viewed as a higher-level system. In the following, we use the term *System under Investigation* (SuI) to denote such a system. In addition to the technical focus, we investigate this system from the point of view of different management functions: lifecycle, operational, organizational and business management.

Measuring the security level and/or performance of the SuI is a complex socio-technical problem. It must be noted that it is very challenging, if not impossible, to develop security metrics that are fully able to present real security phenomena. Thus metrics are rather more like "security metrics probes" to the SuI, being able to tell us as much as we are able to design them.

Fig. 1 shows the proposed Security Metrics Objective Segments (SMOS) model, visualized in a nested circle presentation. Details of the outermost disk, "More detailed characteristics of metrics", have been omitted from the figure for clarity reasons, but can be found in Section 4.4 of this article. Taxonomies for different SuIs can be developed with the help of this model; in fact, the circle and its disks generate security metrics taxonomies. The model includes the following main security metrics objective segments:

1. **Level 0 (Target)**: Security (level and performance) of the SuI is the root node;
2. **Level 1 (Main Viewpoints to Target)**: The first level under the root node includes three import segments that affect the security of the SuI: (*i*) security-enforcing mechanisms or control, (*ii*) security quality of the system, and (*iii*) secure system lifecycle, project and business management;
3. **Level 2 (Fundamental Measurement Objectives)**: The second level down in the hierarchy represents three fundamental objectives of security measurement: (*i*) cor-

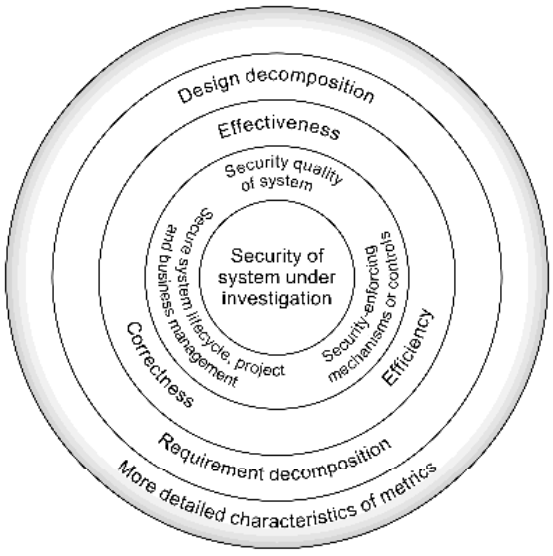

Fig. 1. Security Metrics Objective Segments (SMOS) model

rectness, (*ii*) effectiveness, and (*iii*) efficiency;
4. **Level 3 (Decomposition)**: The Basic Measurable Components (BMCs), the "skeleton" of the collection of security metrics, can be identified by (*i*) requirement decomposition, or (*ii*) design decomposition;
5. **Level 4 (More Detailed Metrics Characteristics)**: This level presents the more detailed metrics characteristics that are selected and designed depending on the feasibility and use.

The proposed hierarchy of metrics objective segments is elaborated on in the following subsections.

4.1 Main Viewpoints on Target

In security engineering of a technical system it is important to analyze the system and obtain security evidence from the following viewpoints (1 to 3):

1. **Security-enforcing mechanisms or controls** are the backbone of the entire security solution of SuI during the course of the system lifecycle;
2. **Security quality of the SuI**, its architecture, functionality, components and interfaces during the the system lifecycle; and
3. **Metrics alignment with secure system lifecycle, project and business management** relevant to the SuI.

The relative importance of the above-mentioned viewpoints varies depending on the system's security objectives and the phase in the system lifecycle. The first two viewpoints are technical and the last one is management-oriented.

The target audience of the first two viewpoints is mainly secure software developers. Nowadays, these developers are often security specialists. However, in the near future, every software developer should be security-aware and capable of understanding security issues and implementing appropriate security solutions. According to [21], the roles identified as being important for software security are security requirements developer, threat analyst, software architect, developer/programmer, tester, verifier, reviewer, auditor, manager of application development, configuration manager and tool developer.

The target audience of viewpoint 3 is management in general: project managers, product managers, Research and Development (R&D) managers, Chief Information Officers and executive managers.

The focus of viewpoint 1, security-enforcing mechanisms (or security controls in information security management terminology), can be defined as safeguards and countermeasures that aim at treating (avoiding, accepting, mitigating or cancelling) security risks. The safeguards and countermeasures implement the policies and requirements of the SuI. Fig. 2 [10] shows an example of the classification of security-enforcing mechanisms that are often used in communication systems.

Viewpoint 2, security quality of the SuI, addresses the overall security level of the SuI, including its design, implementation and functionality in its use environment. Security-enforcing mechanisms are part of the overall system, but the focus of security quality measurements is wider: the whole system. High-quality software design forms the foundation for the high security level of the SuI in general. Management and improvement of software design is one of the core issues in software security engineering. The security quality of the SuI can be increased by security assurance activities, such as security testing, monitoring and analysis. These activities address the whole system, its components and interfaces – the *attack surface* of the system [22,23]. In more detail, the attack surface particularly includes the set of entry points and exit points, the set of open communication channels and the set of untrusted data items [22]. When evaluating the security quality, it is important to note that if all the components of a system are secure, this does not automatically imply that the system as a whole would be secure. The security metrics taxonomy for product/system/security engineering in [1] underlines the difference between security metrics for design and implementation. The former is mainly concerned with correctness and effectiveness, the latter mainly with correctness. This is due to the fact that, in implementation, the requirements are followed as closely as possible, resulting in correct implementation, whereas in the design, the goal is to carry out risk treatment as effectively and correctly as possible.

Development of security metrics with focus on Viewpoints 1 and 2 should be carried hand-in-hand. Especially, the role of design-time security metrics is important in the identification of security weaknesses at early stages of the system lifecycle, increasing the cost-effectiveness of security engineering and the entire system development effort.

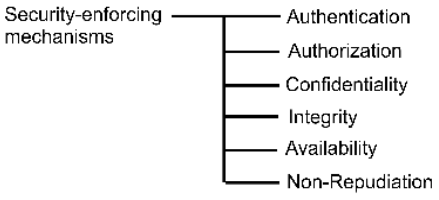

Fig. 2. Example of classification of security-enforcing mechanisms [10]

The phases of the system lifecycle can be defined in many different ways; for example conceive, design, realize and service [1]. Security metrics concerned with configuration management is also an important category. The Systems Security Engineering Capability Maturity Model (SSE-CMM) ISO/IEC Standard 21827 [24] contains a wide collection of security metrics for maturity assessment of security engineering processes. Examples of business-driven metrics categories are: Return of Security Investment (ROSI), business collaboration trust metrics, business-level risk management metrics, cost-benefit analysis metrics and information security management metrics [1].

We claim that viewpoints 1, 2 and 3 form the overall *security posture of the SuI*. This claim can be justified with the following arguments:

1. **The core role of security-enforcing mechanisms**. Security quality objectives do not sufficiently emphasize the role of security-enforcing mechanisms that form the core of the active security solution in the SuI. Therefore, security metrics concentrating on the correctness, effectiveness and efficiency of security-enforcing mechanisms deserve a strong emphasis (viewpoint 1);
2. **Emphasis on a technical target**. There is a strong emphasis on technical metrics because the target of the measurement is a technical system. The often-used division into technical, operational and organizational security metrics (see e.g. [7] and [8]) does not sufficiently emphasize the technical system as a target. Most security metrics are needed during R&D, mainly by secure software developers and other personnel in the development project (viewpoints 1 and 2); and
3. **Metrics alignment with management and business objectives**. Different management activities control the R&D and maintenance of the SuI. Therefore, it is of the utmost importance that the security objectives identified at all relevant levels of management (business, organizational, project, system lifecycle) are part of the overall security solution development of the SuI, and evidence of the resulting security level and performance is communicated to the management. In the long run, lifecycle management has an important role both from the end-user's and the provider/manufacturer's perspective. Security metrics should be aligned to the business goals and other organizational and project management objectives of a company or a collaborating value net of businesses in an appropriate way (viewpoint 3).

4.2 Fundamental Measurement Objectives

In security engineering, *security correctness*, *security effectiveness* and *security efficiency* can be seen as the main fundamental measurement objectives. They address all the main purposes of security engineering work. For the purposes of this study, we define these objectives in the following way:

1. **Security correctness** denotes assurance that security-enforcing mechanisms have been correctly implemented in the SuI, and the system, its components, interfaces and the processed data meet the security requirements;
2. **Security effectiveness** denotes assurance that the stated security requirements are met in the SuI and the expectations for resiliency in the use environment are satisfied, while the SuI does not behave in any way other than what is intended; and
3. **Security efficiency** denotes assurance that the adequate security quality has been achieved in the SuI, meeting the resource, time and cost constraints.

Security correctness can be seen as an objective for security quality and *a necessary but not sufficient* requirement for both "higher-level" measurement objectives – security effectiveness and security efficiency. If the system meets its specification, we can say that it is "correct". Correctness is often discussed together with effectiveness. In some cases, it might be difficult to differentiate them.

Effectiveness and efficiency are widely recognized objectives in the security community.

Intuitively, security effectiveness is the most important fundamental security measurement objective. If the system's security performance and its resilience are at an adequate level in its use environment in the long run, its security effectiveness can be considered to be adequate. In this case, resilience means the system's ability to cope as desired in the presence of security threats. Kailar *et al.* [25] define system security as being effective if its correct operation counters one or more identified threats. This definition can be further enhanced to address the threats that are chosen to be cancelled or mitigated. In other words, effectiveness is the security quality objective of the overall system.

Security efficiency addresses different kinds of metrics since it is a productivity objective. For example, the ROSI metrics concentrate on security efficiency. The role of efficiency objectives is to set constraints and a resource, time and financial framework for the system and security engineering efforts. At the technical level, some security efficiency objectives can also be interpreted as system performance objectives.

Security correctness, effectiveness and efficiency can also be examined separately for each security objective

dimension, e.g. confidentiality effectiveness, integrity effectiveness and availability effectiveness.

4.3 Decomposition

Decomposition is the dismantling of a system into its sub-parts. In [10] we discuss the utilization of a security metrics development process based on security requirement decomposition. The following security requirement decomposition process [10], based on the work by Wang and Wulf [26] is used to identify Basic Measurable Components (BMCs) [10]:

1. Identify successive components from each security requirement that contribute *at an adequate level* to the security correctness, security effectiveness and/or security efficiency of it;
2. Examine the subordinate components to see if further decomposition is needed;
3. Terminate the decomposition when none of the leaf nodes can be decomposed any further, or further analysis of these components is no longer necessary.

In general, the main emphasis of the security metrics development process of [10] is on the security requirement decomposition. However, it is not possible to drive security engineering exclusively from the requirements. The following dual approach is needed [21]: (*i*) *requirements-driven* and (*ii*) *design-driven*. Respectively, the decomposition process can be applied to both the requirements and the design of the SuI. In the design decomposition, the starting point is the system architecture and its environment, which are decomposed into components such as software modules, interfaces and the functionality of the components. Design decomposition is particularly useful when evaluating the overall security quality of the SuI.

Fig. 3 shows an example of security requirement decomposition for authorization as a security-enforcing mechanism [10]. The identified BMCs are Authentication Strength (AS), Reliability of Access Control Mechanism

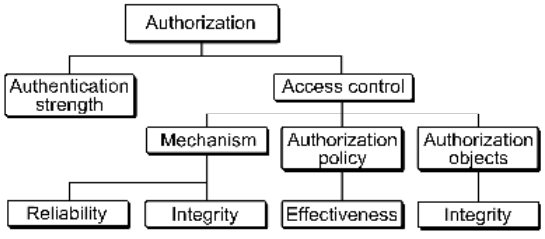

Fig. 3. An authorization decomposition [10]

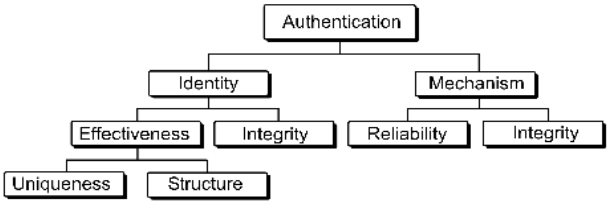

Fig. 4. An authentication decomposition [26]

(RACM), Integrity of Access Control Mechanism (IACM), Effectiveness of Authorization Policy (EAP) and Integrity of Authorization Objects (IAO).

AS is calculated with the help of BMCs identified in the authentication decomposition [26], see Fig. 4. The details of the decompositions vary from system to system, depending on the emphasis of the security-relevant objectives.

4.4 More Detailed Metrics Characteristics

After the BMCs have been identified, more detailed metrics characteristics need to be chosen based on the metrics needs, measurement architecture and evidence collection mechanism.

Security metrics can be classified in many different ways. Table 1 summarizes some two-dimensional security metrics characteristics and Table 2 some three-dimensional ones.

In general, security metrics can vary from *qualitative* to *quantitative*, from *direct* to *indirect*, from close-to-*absolute* to highly *relative*, and from close-to-*objective* to highly *subjective*.

Security metrics focus on either the positive security effects or properties of the system (*strength metrics*) or the negative ones (*weakness metrics*). Vulnerability metrics, such as the Common Vulnerability Scoring System (CVSS) [27], the associated enumeration Common Vulnerabilities and Exposures (CVE) enumeration [28], both part of Security Content Automation Protocol (SCAP) [29],

Table 1. Some two-dimensional security metrics

Characteristics Dimension A	Characteristics Dimension B
Strength	Weakness
Qualitative	Quantitative
Direct	Indirect
Close-to-absolute	Relative
Close-to-objective	Subjective
Attack-oriented	Non-attack-oriented
Online	Offline

Table 2. Some three-dimensional security metrics

Dim. A	Dim. B	Dim. C
Leading	Coincident	Lagging
Technical	Operational	Organizational

Table 3. Scale types of security metrics

Type 1	Type 2	Type 3	Type 4
Nominal: labels	Ordinal: rank order	Interval: [a … b]	Ratio: $\frac{a}{b}$

naturally fall into the category of weakness metrics.

The time-dependent behavior of a security metric can be *leading*, *coincident* or *lagging* [2]. Different timing categories should not be mixed without proper prediction models or heuristics.

Security metrics can also be divided into *attack-oriented* and *non-attack-oriented*. The attack-oriented metrics emphasize attacker strategies. The strategies can be modeled by attack trees [30] and analyzed by cost-benefit analysis. From an adversary's point-of-view, the security strength, in combination with the personal risk of the attack to the adversary's reputation, safety or freedom, are of interest when evaluating a prospective target of attack [31]. Non-attack-oriented metrics do not emphasize the attacker behavior or strategy. They focus on the strengths and/or weaknesses of different security solutions from the point of view of the high-level results of threat and vulnerability analysis or what is generally known about them.

According to the widely-known measurement scaling theory by Stevens [32], there are four basic types of scales: *nominal*, *ordinal*, *interval* and *ratio*, summarized in Table 3. In nominal scales, labels describing certain characteristics of a nominal category are used. In ordinal scales, the numbers of entities represent their rank order. Three or five-level scales are widely used. In interval scale measurements, a certain distance along the scale means the same difference in security strength despite the point on the scale. Ratio scale measurement is an estimation of the ratio between a magnitude of a quantity and a unit magnitude of the same quantity.

According to [10], detailed development of the chosen collection of security metrics aims at defining the following issues for each metric: metric purpose, target description, formalization, value scale or ordering, value range and thresholds, if applicable.

5. Creating Taxonomies using the SMOS Model

Taxonomies are frequently used for classification of objects into a hierarchical structure, commonly displaying parent-child relationships. In taxonomies, there is a root node at the top that applies to all objects under it. Taxonomies will help the actual process of developing feasible security metrics, acting as a tool towards an organized structure of security objectives. Note that the core factor contributing to the quality of taxonomy is the quality of the source material: the early knowledge and evidence of the SuI and sufficient results from threat and vulnerability analyses.

It is possible to construct taxonomies from the proposed SMOS model as follows:

1. Place the innermost circle as the root node of the taxonomy;
2. Identify relevant successive components (children) from the objectives mentioned on the next outer disk of Fig. 1; and
3. Repeat Step 2 until the outermost disk of Fig. 1 has been reached and the balancing and integration of metrics can be initiated.

As an example, Fig. 5 shows the first three levels of a hierarchy of security metrics taxonomy for an example

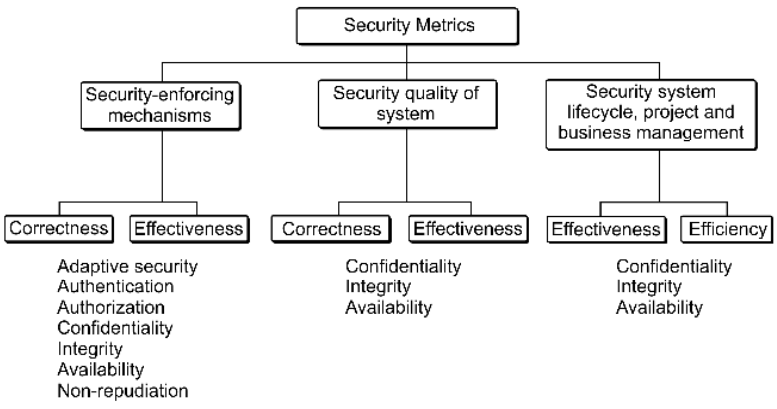

Fig. 5. The first three levels of a security metrics taxonomy example

system (a distributed messaging system with online adaptive security management based on security metrics, [10]). In the example, the security metrics for both security-enforcing mechanisms and the system security quality in general concentrate on correctness and effectiveness. On the other hand, the associated management activities concentrate on effectiveness and efficiency. Efficiency, of course, is also present in the technical work, but security effectiveness dominates it. The security objectives listed under the leaves in the figure are the dimensions to be addressed during security requirement decomposition.

6. Integration of the SMOS Model into Security Metrics Development Process

In [10,33-35], we have iteratively proposed, analyzed and applied the following security metrics development process:

1. Carry out a threat and vulnerability analysis,
2. If applicable, utilize the available taxonomical or ontological information,
3. Define the security requirements and carry out modeling (if applicable),
4. Decompose the requirements and/or design,
5. Develop the measurement architecture, the mechanisms to gather the required measurement data from the SuI,
6. Carry out a feasibility analysis, and
7. Develop a balanced and detailed collection of security metrics.

Sufficient results from threat and vulnerability analysis are the initial starting point in risk-driven security engineering activities. Respectively, application of the SMOS model can be started after the threat and vulnerability analysis stage. From that point on, the model and the taxonomies created from it will help to systematize the whole process of security metrics development, aiming at a balanced and detailed collection of security metrics.

During the requirement development phase (Step 3), the SMOS model can be used to develop the security requirements for security-enforcing mechanisms and the system in general, balanced with the lifecycle, project and business goals. In addition, the model helps to prioritize the requirements and plan modeling efforts.

The viewpoints and main fundamental measurement objectives can be used to systematize and organize the requirement and design decomposition processes (Step 4). The results of the decompositions can be fed back to the taxonomical level.

Development of the measurement architecture (Step 5) is not directly connected to the proposed model or associated security metrics taxonomies. However, it is a core activity in the above-mentioned process, enabling practical and feasible measurement activity in the SuI.

The SMOS model and associated taxonomies also systematize the feasibility analysis (Step 6) and support the more detailed development of metrics (Step 7). When composing integrated metrics from sub-metrics, different weights can be associated with them, presenting their relative importance.

7. Discussion

The state of the art in developing and using security metrics is still in its early stages. The state of the art in developing and using security metrics is still in its early stages. As of yet, there have not been any common and widely-accepted objectives, taxonomies or even vocabulary in use. Organizational and technical security metrics have emerged from different communities, the former from Information Security Management (ISM) needs in organizations and the latter from product-focused R&D activities. Obviously, models and methods to bridge the gaps between secure product, system and service development, business management and ISM are needed. Security metrics and measurements should make a move from ad hoc practices to a more systematic process that is capable of responding to constantly changing threats and business demands.

In this study we have introduced an initial foundation for the organization of security metrics focusing on technical systems while taking business goals into account. Security-enforcing mechanisms and the overall security quality of the system are the most important technical viewpoints of our model. Furthermore, alignment of security metrics to management objectives is crucial.

Obviously, the SMOS model is not well suited to developing security metrics for ISM in organizations since its focus is on technical systems. In ISM, the widely-used division into technical, operational and organizational metrics, if not some other classification, might be more useful.

Security correctness, effectiveness and efficiency as the main fundamental measurement targets well reflect the security evidence needs. In this paper, we have provided definitions for these concepts. However, the definitions might require further elaboration and discussion in security research and practitioner communities. A common agreement on the objectives from a holistic perspective would be valuable.

The feasibility of using security metrics in practice has

been criticized in some contributions. One has to remember that security metrics simplify a complex socio-technical system down to simple values or orderings. McHugh [36] and McCallam [37] are worried about the possible side effects of such a simplification. Nonetheless, it must be noted that an adequate collection of sub-metrics can measure even complex situations. The challenge is in understanding this complex socio-technical system, not in using metrics. Bellovin [38] points out that developing metrics is hard, if not infeasible, because an attacker's effort is often linear, even in cases where exponential security work is needed. In addition, luck plays a major role in security [39]. The weakest-link vulnerabilities cause a lot of trouble while they cannot be fully prevented. However, taxonomies help to increase understanding of the weakest-links and carrying out the prioritization of security requirements accordingly.

8. Conclusions and Future Work

Obtaining sufficient and credible security evidence from the system under investigation is one of the major challenges in information security engineering and management. System developers, project management and executive management need information about the security posture of technical systems during different phases of the system lifecycle.

In this study we have proposed a novel Security Metrics Objective Segments (SMOS) model to taxonomize security metrics for technical systems and to systematize and organize their development activities. The SMOS model enables the design of security metrics taxonomies, which, in turn, the actual practical security metrics development. The model nominates security-enforcing mechanisms, the overall security quality of the system, and lifecycle, project and business management as the main viewpoints. Furthermore, security correctness, security effectiveness and security efficiency are seen as the fundamental measurement objectives. To further elaborate taxonomical work, decomposition of either requirements or design constructs, along with more detailed characteristics, are part of the model. The model can be seamlessly integrated with risk-driven security metrics development approaches.

Our future work includes further evolution and formalization of the proposed model. To gather practical feasibility experience, we intend to use the model in some security metrics development scenarios in telecommunications, software and industrial automation environment fields.

References

[1] R. Savola, "A Taxonomical Approach for Information Security Metrics Development", Nordsec '07 Supplemental Booklet of Short Papers, Reykjavík, Iceland, 11 p., Oct., 11-12, 2007.

[2] W. Jansen, "Directions in Security Metrics Research," NIST, NISTIR 7564, 21 p., Apr., 2009.

[3] R. Savola, "Towards a Taxonomy for Information Security Metrics," QoP '07, Alexandria, VA, USA, pp.28-30, Oct., 29, 2007.

[4] R. Savola, "A Novel Security Metrics Taxonomy for R&D Organizations," ISSA '08, Johannesburg, South Africa, pp.379-390, Jul., 7-9, 2008.

[5] R. Henning et al., "Proceedings of Workshop on Information Security System, Scoring and Ranking – Information System Security Attribute Quantification or Ordering," ACSA and MITRE, Williamsburg, VA, USA, May, 2001, Publ. 2002.

[6] N. Seddigh, P. Pieda, A. Matrawy, B. Nandy, I. Lambadaris, A. Hatfield, "Current Trenes and Advances in Information Assurance Metrics," PST '04, Fredericton, NB, Canada, Oct., 2004.

[7] M. Swanson, "Security Self-Assessment Guide for Information Technology Systems," NIST Special Publication 800-26, Nov., 2001

[8] M. Swanson, N. Bartol, J. Sabato, J. Hash, L. Graffo, "Security Metrics Guide for Information Technology Systems," NIST Special Publication 800-55, Jul., 2003.

[9] R. Vaughn, R. Henning, A. Siraj, "Information Assurance Measures and Metrics: State of Practice and Proposed Taxonomy," HICSS '03, Hawaii, USA, 2003.

[10] R. Savola, H. Abie, "Identification of Basic Measurable Security Components for a Distributed Messaging System," SECURWARE '09, Athens/Glyfada, Greece, pp. 121~128, Jun., 18-23, 2009.

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

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

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

[14] D. B. Parker, "Computer Security Management," Reston Publishing Company, Reston, VA, USA, 1981.

[15] ITU-T Recommendation X.805, "Security Architecture for Systems Providing End-to-End Communications," 2003.
[16] D. Longley, M. Shain, "Data and Computer Security: Dictionary of Standards, Concepts and Terms," Macmillan, 1987.
[17] D. Gollmann, "Computer Security," John Wiley & Sons, 1999.
[18] R. C. Summers, "Secure Computing, Threats and Safeguards," McGraw-Hill, 1997.
[19] A. Avižienis, J.-C. Laprie, B. Randell, C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing," IEEE Tr. on Dependable and Secure Computing, Vol. 1, No.1, pp.11-33, Jan./Mar. 2004.
[20] B. S. Yee, "Security Metrology and the Monty Hall Problem," Workshop on Information Security System Scoring and Ranking (WISSSR), ACSA and MITRE, Williamsburg, USA, May 2001, Publ. 2002.
[21] Practical Software & Systems Measurement Safety and Security Technical Working Group, "Security Measurement – White Paper," Vers. 3.0, 67 p., Jan., 2007.
[22] M. Howard, J. Pincus, J. M. Wing, "Measuring Relative Attack Surfaces," Workshop on Advanced Developments in Software and Systems Security, 2003.
[23] P. K. Manadhata, D. K. Kaynar, J. M. Wing, "A Formal Model for a System's Attack Surface," Technical Report CMU-CS-07-144, Jul., 2007.
[24] ISO/IEC 21827:2003, "Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM)," ISO/IEC, 2003.
[25] R. Kailar, V. D. Gligor, L. Gong, "On the Security Effectiveness of Cryptographic Protocols," 4th IFIP Working Conf. on Dependable Computing for Critical Applications, Vol.9, 1994.
[26] C. Wang, W. A. Wulf, "Towards a Framework for Security Measurement," 20th National Information Systems Security Conference, Baltimore, MD, USA, pp.522-533, Oct., 1997.
[27] M. Schiffman, G. Eschelbeck, D. Ahmad, A. Wright, S. Romanosky, "CVSS: a Common Vulnerability Scoring System," U.S. National Infrastructure Advisory Council (NIAC), 2004.
[28] R. A. Martin, "Managing Vulnerabilities in Networked Systems," IEEE Computer Society Computer Magazine, Vol.34, No.11, Nov., 2001.
[29] M. Barrett, C. Johnson, P. Mell, S. Quinn, K. Scarfone, "Guide to Adopting and Using the Security Content Automation Protocol (SCAP)," NIST Special Publication 800-117 (Draft), NIST, 2009.
[30] B. Schneier, "Attack Trees," Dr. Dobb's Journal, Vol.24, No.12, 1999.
[31] S. E. Schechter, "Computer Security Strength & Risk: a Quantitative Approach," Ph.D Thesis, Harvard University, Cambridge, MA, USA, 2004.
[32] S. S. Stevens, "On the Theory of Scales of Measurement," Science, Vol. 103, Issue 2684, pp.677-680, Jun., 7, 1946.
[33] R. Savola, "Requirement Centric Security Evaluation of Software Intensive Systems," DepCOS-RELCOMEX '07, Szklarska Poreba, Poland, pp.135-142, Jun., 14-16, 2007.
[34] R. Savola, "Development of Security Metrics for a Distributed Messaging System," AICT '09, Baku, Azerbaijan, 6 p., Oct., 14-16, 2009.
[35] R. Savola, "A Security Metrics Development Method for Software Intensive Systems," ISA '09, Seoul, Korea, Jun., 25-27, 2009, Springer CCIS 36, pp.11-16, 2009.
[36] J. McHugh, "Quantitative Measures of Assurance: Prophecy, Process or Pipedream?" Workshop on Information Security System Scoring and Ranking (WISSSR), ACSA and MITRE, Williamsburg, VA, USA, May, 2001, Publ. 2002.
[37] D. McCallam, "The Case Against Numerical Measures of Information Assurance," Workshop on Information Security System Scoring and Ranking (WISSSR), ACSA and MITRE, Williamsburg, VA, USA, May, 2001, Publ. 2002.
[38] S. M. Bellovin, "On the Brittleness of Software and the Infeasibility of Security Metrics," IEEE Security & Privacy, p. 96, Jul./Aug., 2006.
[39] P. Burris, C. King, "A Few Good Security Metrics," METAGroup Inc., Oct., 2000.

Reijo M. Savola
He received MS degree in Electrical Engineering (with honors) from the University of Oulu, Finland, 1992, and Licentiate of Technology degree in Computer Science from Tampere University of Technology, 1995. Mr. Savola has worked as a Digital Signal Processing consultant for Elektrobit Group Plc. in Oulu, Finland and in Redmond, Washington, United States. He is now working as a Senior Research Scientist at VTT Technical Research Centre of Finland. His research interests include security metrics, modeling of security, and bridging the gaps between different aspects of security engineering and management.