A NOVEL SECURITY METRICS TAXONOMY

FOR R&D ORGANISATIONS

Reijo Savola

VTT Technical Research Centre of Finland

P.O. Box 1100, FI-90650 Oulu, Finland
+358 40 569 6380
Reijo.Savola@vtt.fi

ABSTRACT

In order to obtain evidence of the security and privacy issues of products, services or an organization, systematic approaches to measuring security are needed. In this study we survey the emerging security metrics approaches from the academic, governmental and industrial perspectives. We aim to bridge the gaps between business management, information security management and ICT product security practices. If appropriate *security metrics* can be to offer a quantitative and objective basis for security assurance, it would be easier to make business and engineering decisions concerning information security. We believe that being able to express a high-level taxonomy of security metrics will help the actual process of developing feasible composite metrics even for complex situations. A well-defined taxonomy can be used to enhance the composition of feasible security metrics all the way from business management to the lowest level of technical detail. Information security management, business management and, on the other hand, software security and network security engineering have been handled as separate areas. Common metrics approaches can be used to bridge the gaps in between.

KEY WORDS

Information security metrics, security assurance, information assurance, taxonomy

A NOVEL SECURITY METRICS TAXONOMY

FOR R&D ORGANISATIONS

1 INTRODUCTION

The field of defining security metrics systematically is young and the current practice of information security is still a highly diverse field, and holistic and widely accepted approaches are still missing. In order to make advances in the field of measuring, assessing or assuring security, the current state of the art should be investigated and structured in a clear way.

The main contribution of this study is an initial proposal for a security metrics taxonomy for the ICT product Research and Development (R&D), supported with a literature survey of the current state of the art in industry strength and academic approaches to measuring security. Section 2 discusses the characteristics of security metrics and Section 3 proposes a taxonomy for security metrics, and finally, Section 4 gives conclusions.

2 CHARACTERISTICS OF SECURITY METRICS

It is helpful to notice the difference between metrics and measurements. Measurements provide single-point-in-time views of specific, discrete factors, while metrics are derived by comparing two or more measurements taken over time with a predetermined baseline [25]. Furthermore, according to Alger [1], measurements are generated by counting, whereas metrics are generated from analysis. According to Jelen [25], a good metric is Specific, Measurable, Attainable, Repeatable and Time-dependent ("SMART"). Payne [31] remarks that truly useful security metrics indicate the degree to which security goals, such as data confidentiality, are being met. Security metrics are used for decision support and very often these decisions are actually risk management decisions – aiming at mitigating, cancelling or neglecting security risks. Consequently, many metrics that might be useful for different purposes will be associated with risk analysis in a direct or indirect way. Security metrics and measurements can be used for decision support, especially in *assessment* and *prediction*. When using metrics for prediction, mathematical models and algorithms are applied to the collection

of measured data (e.g. regression analysis) to predict the security behaviour of an organization, a process or a product in the future. It is important to clearly know the entity that is the target of measurement because otherwise the actual metrics might not be meaningful. FIPS Publication 199 [11] presents a mechanism for investigating confidentiality, integrity and availability separately, emphasizing the *potential impact* assessment. In general, the security measurements can be based on the above-mentioned widely known objectives, augmented with some objectives such as non-repudiation, depending on the needs of situation.

Security and trust metrics can be obtained at different levels within an organization or a technical system. Detailed metrics can be aggregated and rolled up to progressively higher levels. As Yee [46] states, a multi-faceted or multi-dimensional security measure is needed. Security metrics properties can be quantitative or qualitative, objective or subjective, static or dynamic, absolute or relative, or direct or indirect. According to ISO 9126 standard [18], a direct measure is a measure of an attribute that does not depend upon a measure of any other attribute. On the other hand, an indirect measure is derived from measures of one or more other attributes.

2.1 On the Feasibility of Measuring Security

The feasibility of measuring security and developing security metrics to present actual security phenomena has been criticized in many contributions. In designing a security metric, one has to be conscious of the fact that the metric simplifies a complex socio-technical situation down to numbers or partial orders. McHugh [28] and McCallam [27] are skeptical of the side effects of such simplification and the lack of scientific proof. Bellovin [5] remarks that defining metrics is hard, if not infeasible, because an attacker's effort is often linear, even in cases where exponential security work is needed. Another source of challenges is that luck plays a major role [9] especially in the weakest links of information security solutions. Security metrics are difficult because the discipline of measuring security itself is still in the early stages of development. As yet, there is no common vocabulary and few documented best practices to follow. Those pursuing the development of a security metrics program should think of themselves as pioneers and be prepared to adjust strategies as experience dictates [31].

2.2 Related Work: Earlier Security Metrics Taxonomies

The WISSSR workshop [13] did not propose any specific security metric taxonomy. Instead, the workshop was intuitively organized into three tracks: technical, operational and organizational. Technical metrics are "used to describe, and hence compare, technical objects, e.g., algorithms, specifications, architectures and alternative designs, products, and as-implemented systems". Operational metrics are "used to describe, and hence manage the risks to, operational environments." Organizational metrics are "used to describe, and to track the effectiveness of, organizational programs and processes." In general, there would seem to be an intuitive understanding among the workshop participants that these three tracks would provide a useful basis for a taxonomy of security metrics [36].

Vaughn et al. [44] propose a taxonomy for information assurance metrics consisting of two distinct categories: (i) organizational security metrics and (ii) metrics for Technical Target of Assessment (TTOA). As Seddigh *et al*. [35] conclude, this taxonomy is a valuable contribution, but further work is required to make it applicable to an IT organization.

The U.S. National Institute of Information Standards and Technology (NIST) presents its security metrics taxonomy in NIST Special Publication 800-26 [38] and 800-55 [39]. The taxonomy is comprehensive, presenting three categories (management, technical, and operational) and 17 sub-categories. This taxonomy has been written from the point of view of an organization, and technical metrics category assesses the level of technical security controls in the organization rather than the technical security level of specific products, as does TTOA in Vaughn *et al*.'s taxonomy.

Seddigh *et al*. introduce an information assurance metrics taxonomy for IT Network assessment in [36]. Their taxonomy has three categories – security, Quality of Service (QoS) and availability – based on their novel definition of information assurance. Under each of these three they consider technical, organizational and operational metrics.

The Institute for Information Infrastructure Protection (I3P) [14] is also carrying out work on creating a taxonomy for security metrics from the process control systems perspective. Stoddard *et al.*, in [37], propose an initial security metrics taxonomy for process control systems based on the WISSSR workshop taxonomy and ISO/IEC 17799 [23] and ANSI/ISA-TR99.00.01-2004 [2] standards.

3 PROPOSED SECURITY METRICS TAXONOMY

The most direct factor contributing to the quality of the taxonomy is the quality of the *corpus* or source material [45]. As a source material, we present a survey of security metrics in this study.

3.1 Business Level Security Metrics

The highest category (root node) of our taxonomy is the security metrics for business management (Fig. 1). Business goals steer the security and trust management work and, accordingly, security and trust metrics should be defined in such a way that they are *aligned to the business goals* of a company or a collaborating value net of businesses. One way of establishing an overall metrics process is to begin with the business goals and demonstrate the alignment of lower level security management objectives within that context. Note that in any organisation, e.g. a government organization, "business goals" can be replaced by major goals that are specific to that organization (e.g. defined by legislation).

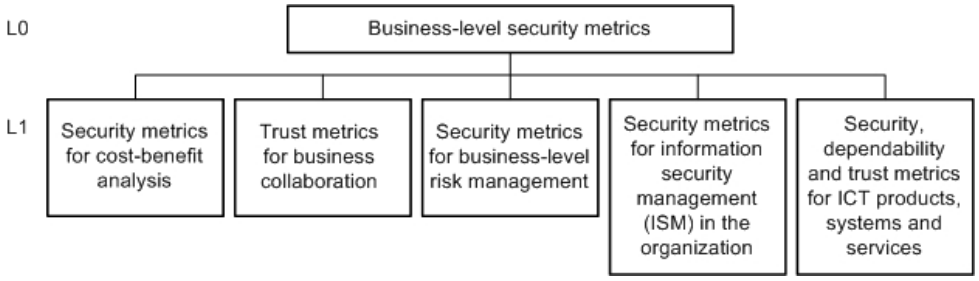

Figure 1. Business-level security metrics

Security ROI (Return On Investment) is quickly gaining popularity because it is a simple metric. Security ROI is defined by Blakley [7] as the amount of this annual benefit over its cost. Trust management is a relatively new research field that aims at understanding, modelling and controlling trust phenomena. Trust evaluation functions, such as Toivonen *et al.*'s work [40] have been defined to set a basis for trust quantification. Basili's [4] Goal/Question/Metric (GQM) approach can be used for establishing a metrics process (or program), beginning with the business goals. Note that regardless of the methodology used, developing business-relevant metrics needs commitment from the business management.

3.2 Metrics for Information Security Management in Organisation

Fig. 2 shows the taxonomy of the security metrics for information security management in the organization. In principal, we here follow the taxonomy definitions of [38] and [36].

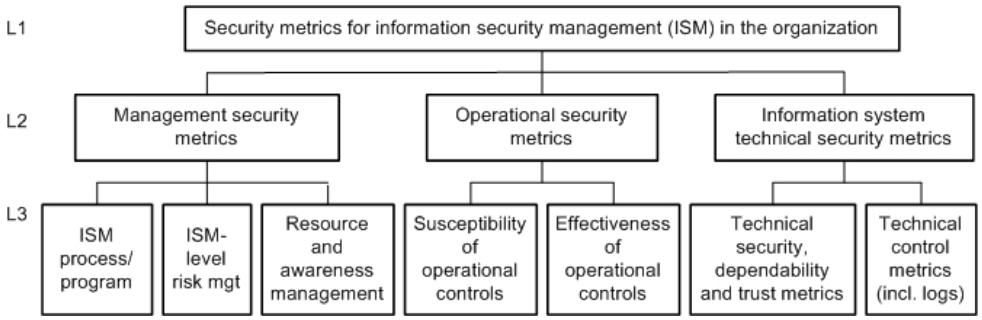

Figure 2. Metrics for ISM

These security metrics support evaluation of the security controls, plans and policies, as well as certification and accreditation activities. Human resource assessment is typically concentrated on training and security awareness polls, and evaluation of the human resource assignments [33]. Operational metrics address the susceptibility and effectiveness of operational security practices (or controls) [36]. They typically concentrate on incident response, the archiving process and the maintenance process of SW, HW and networking equipment. Furthermore, security documentation, data integrity and contingency planning are evaluated [36].

Technical SDT (Security, Dependability and Trust) metrics can be a subset or an instance of the SDT metrics for product life cycle management. NIST SP 800-26 [38] gives guidelines on security self-assessment of information technology systems based on the U.S. Federal IT Security Assessment Framework. NIST SP 800-53A [32] represents assessment methods and procedures for a minimum level due diligence for organizations assessing the security controls in their information systems. NIST SP 800-55 [39] provides guidance on how an organization, by using metrics, identifies the adequacy of in-place security controls, policies, and procedures. An example of an implementation metric is *percentage of NIST SP 800-53A control families for which policies exist*. Effectiveness and efficiency metrics are used to monitor the results of security control

implementation for a single control or across multiple controls. For example, *percentage of security incidents caused by improperly configured access controls* relies on information from or about several controls. NIST SP 80-100 [8], the information security guide for managers, contains a section on security measurements. The Federal Information Processing Standards (FIPS) Publication 199 [11] establishes security categories for both information and information systems. According to [11], the potential impact can be classified as low, moderate or high. According to Lennon of NIST [26], "the universe of possible metrics, based on existing policies and procedures, will be quite large. Metrics must be prioritized."

The Information Security Forum (ISF) [15] is a member-driven non-profit forum that has established the "Standard of Good Practice" (SOGP) [16] and the accompanying "Information Security Status Survey". The survey measures compliance with SOGP and ISO/IEC 17799. ISF offers a benchmark comparison to the members on the total or by business sector. ISF has also developed a simpler metric called "Security Health Check".

3.3 Security Metrics for ICT Products, Systems and Services

Probably the most challenging category of our taxonomy is the security, trust and dependability metrics for products, systems and services, see Fig. 3. For the basic concepts and taxonomy of dependable and secure computing, see the study by Avižienis *et al.* [3].

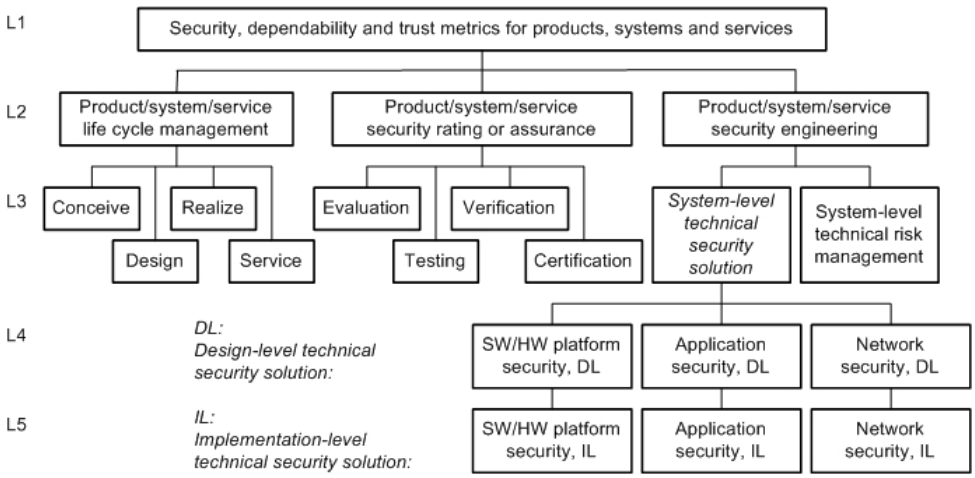

Figure 3. SDT metrics for products, systems and services

During the Conceive phase, the security requirements define the basis for measuring security later by comparing the requirements and actual design or system [34]. The Design phase incorporates activities such as architectural and lower-level design, testing, analysis and validation. As an example of product life-cycle security metrics, Systems Security Engineering Capability Maturity Model (SSE-CMM) ISO/IEC standard 21827 [24] contains security metrics for maturity assessment of the security level of security engineering processes and results of them. The resulting standards are the basis of evaluations by neutral third parties besides manufacturers and procurers. The most widely known of such efforts is the Common Criteria (CC) ISO/IEC 15408 international standard [22]. The CC standard is based on a combination of several other standards for information security, including TCSEC (Trusted Computer System Evaluation Criteria) [41], ITSEC (Information Technology Security Evaluation Criteria) [17], CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) [10] and FC (Federal Criteria for Information Technology Security) [43]. Interpretations of the TCSEC have been published to apply them to other contexts such as the TNI (Trusted Network Interpretation of the TCSEC) [42]. The ISO/IEC technical report ISO/IEC 9126-1 [18] defines a quality model for software, and reports ISO/IEC 9126-2 [19], ISO/IEC 9126-3 [20] and ISO/IEC 9126-4 [21] provide a suggested set of software quality metrics for external, internal and "quality in use" metrics respectively. The particular benefit of this series of reports lies in the overall quality of products – not especially in security.

By "technical security solution" we mean the actual constructs of the system. SDT metrics for system-level technical security solution can be detailed into respective design-level metrics emphasizing either (i) SW/HW platform security, (ii) application security or (iii) network security. Design-level security engineering metrics can be detailed into appropriate implementation-level metrics, mainly representing *vulnerability metrics*. According to CVSS (Common Vulnerability Scoring System), a vulnerability is defined as a bug, flaw, behaviour, output, outcome or event within an application, system, device, or service that could lead to an implicit or explicit failure of confidentiality, integrity or availability [35]. The Forum of Incident Response and Security Teams (FIRST) acts as the custodian of CVSS [12]. NIST's Software Assurance Metrics and Tool Evaluation (SAMATE) project [6] seeks to help answer various questions

on software assurance, tools and metrics. The metrics work being carried out in SAMATE is concentrating on metrics and measures for the software itself and SSA (Software Security Assurance) tools. OWASP (Open Web Application Security Project) [30] is an active discussion and development forum on security metrics. MITRE provides standardized languages as a means for accurately communicating the information and encouraging the sharing of the information with users by developing repositories [29].

4 CONCLUSIONS

"Measuring security" – obtaining enough evidence to be able to make informed decisions on information security issues – is one of the major challenges in information security. Security metrics is an emerging research area rapidly gaining momentum. Unless we are able to measure security phenomena on an adequate level, there will be no advancing leaps in the actual information security field. In this study, we have proposed a high-level taxonomy for security metrics, especially intended for the metrics development for industrial companies producing ICT products. The results of this study can be utilized in the future efforts to form a unified hierarchical security metrics system for ICT industry.

5 ACKNOWLEDGEMENTS

This research has been supported by the European Commission under the 7th Framework Programme through the GEMOM (Genetic Message Oriented Secure Middleware) STREP project, Grant Agreement No. 215327.

6 REFERENCES

1. Alger, J. I.: On Assurance, Measures, and Metrics: Definitions and Approaches. Proc. of Workshop on Information Security System Scoring and Ranking (WISSSR), Williamsburg, Virginia, May, 2001 (2002)
2. ANSI/ISA-TR99.00.01-2004: Security Technologies for Manufacturing and Control Systems Standards. ANSI, Washington, D.C. (2004)
3. Avižienis, A., Laprie, J.-C., Randell, B., and Landwehr, C.: Basic Concepts and Taxonomy of Dependable and Secure Computing. IEEE Trans. on Dependable and Secure Computing. Vol. 1, No. 1. (2004)
4. Basili, V. R. and Weiss, D. M.: A Methodology for Collecting Valid Software Engineering Data. IEEE Transactions on Software Engineering SE-10(6): 728-738, Nov. (1984)

5. Bellovin, S. M.: On the Brittleness of Software and the Infeasibility of Security Metrics. IEEE Security & Privacy, Jul/Aug, p. 96 (2006)
6. Black, P. E.: SAMATE's Contribution to Information Assurance. IAnewsletter, Vol. 9, No. 2 (2006)
7. Blakley, B.: An Imprecise but Necessary Calculation. Secure Business Quarterly: Special Iss. on Return on Security Investment, 1(2), Q4, (2001)
8. Bowen, P., Hash, J., Wilson, M.: Information Security Handbook: A Guide for Managers. National Institute of Standards and Technology Special Publication 800-100 (2006)
9. Burris, P., King, C.: A Few Good Security Metrics. METAGroup (2000)
10. Canadian System Security Centre: The Canadian Trusted Computer Product Evaluation Criteria, Version 3.0e, January 1993, 233 p. (1993)
11. FIPS Publication 199: Standards for Security Categorization of Federal Information and Information Systems. Federal Information Processing Standards Publication (2004)
12. FIRST: Forum of Incident Response and Security Teams. http://www.first.org/cvss/
13. Henning, R. et al.: Proceedings of Workshop on Information Security System, Scoring and Ranking – Information System Security Attribute Quantification or Ordering (Commonly but improperly known as "Security Metrics"), MITRE, Williamsburg, Virginia, May, 2001 (2002)
14. I3P: Institute for Information Infrastructure Protection. www.thei3p.org
15. Information Security Forum (ISF): www.securityforum.org
16. Information Security Forum (ISF): The Standard of Good Practice (SOGP). http://www.isfsecuritystandard.com/index_ns.htm (2005)
17. Information Technology Security Evaluation Criteria (ITSEC) Version 1.2, Commission for the European Communities (1991)
18. ISO/IEC 9126-1:2001: Software Engineering – Product Quality – Part 1: Quality Model. International Organization of Standardization (2001)
19. ISO/IEC 9126-2:2003: Software Engineering – Product Quality – Part 2: External Metrics. International Organization of Standardization (2003)
20. ISO/IEC 9126-3:2003: Software Engineering – Product Quality – Part 3: Internal Metrics. International Organization of Standardization (2003)
21. ISO/IEC 9126-3:2004: Software Engineering – Product Quality – Part 4: Quality-in-Use Metrics. International Organization of Standardization (2004)

22.ISO/IEC 15408-1:2005: Common Criteria for Information Technology Security Evaluation – Part 1: Introduction and General Model. International Organization of Standardization (2005)
23.ISO/IEC 17799:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management. International Organization of Standardization (2005)
24.ISO/IEC 21827:2003: Information Technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM). International Organization of Standardization (2003)
25.Jelen, G.: SSE-CMM Security Metrics. NIST and CSSPAB Workshop, Washington, D.C., June (2000)
26.Lennon, E. B. (Ed.): IT Security Metrics. ITL Bulletin, August 2003. National Institute of Standards and Technology (2003)
27.McCallam, D.: The Case Against Numerical Measures of Information Assurance. Proc. of Workshop on Information Security System Scoring and Ranking (WISSSR), ACSA and MITRE, Williamsburg, Virginia, May, 2001 (2002)
28.McHugh, J.: Quantitative Measures of Assurance: Prophecy, Process or Pipedream? Proc. of Workshop on Information Security System Scoring and Ranking (WISSSR), ACSA and MITRE, Williamsburg, Virginia, May, 2001 (2002)
29.MITRE: Making Security Measurable. http://makingsecuritymeasurable.mitre.org/
30.OWASP: Open Web Application Security Project. http://www.owasp.org/
31.Payne, S. C.: A Guide to Security Metrics. SANS Institute Information Security Reading Room, June (2006)
32.Ross, R., Johnson, A., Katzke, S., Toth, P., Rogers, G.: Guide for Assessing the Security Controls in Federal Information Systems. NIST Publication 800-53A (2006)
33.Sademies, A.: Process Approach to Information Security Metrics in Finnish Industry and State Institutions. VTT Publications 544. 89 p. + app. 2 p. (2004)
34.Savola, R. and Röning, J.: Towards Security Evaluation based on Evidence Information Collection and Impact Analysis. Suppl. Proc. of the 2006 Int. Conference on Dependable Systems and Networks (DSN),

Workshop on Empirical Evaluation of Dependability and Security (WEEDS), June 25-28, 2006, Philadelphia, PA, pp. 113-118.
35. Schiffman, M.: A Complete Guide to the Common Vulnerability Scoring System (CVSS). White paper.
36. Seddigh, N., Pieda, P., Matrawy, A., Nandy, B., Lambadaris, I., Hatfield, A.: Current Trends and Advances in Information Assurance Metrics. Proc. of the 2nd Annual Conference on Privacy, Security and Trust (PST 2004), Fredericton, NB, Oct. (2004)
37. Stoddard, M. et al.: Process Control System Security Metrics – State of Practice. I3P Institute for Information Infrastructure Protection Research Report No. 1, Aug. (2005)
38. Swanson, M.: Security Self-Assessment Guide for Information Technology Systems. NIST Special Publication 800-26, Nov. (2001)
39. Swanson, M., Bartol, N., Sabato, J., Hash, J., Graffo, L.: Security Metrics Guide for Information Technology Systems. National Institute of Standards and Technology Special Publication 800-55, Jul. (2003)
40. Toivonen, S., Lenzini, G., Uusitalo, I.: Context-Aware Trust Evaluation Functions for Dynamic Reconfigurable Systems. Models of Trust for the Web (MTW 06) Workshop, May 22-26, 2006, Edinburgh, Scotland.
41. United States Department of Defense: Trusted Computer System Evaluation Criteria (TCSEC) "Orange Book", DoD Standard, DoD 5200.28-std (1985)
42. United States National Computer Security Center: Trusted Network Interpretation of the Trusted Computer System Evaluation Criteria – Version 1; NCSC-TG-005 (1987)
43. United States National Institute for Standards and Technology and National Security Agency, Federal Criteria for Information Technology Security – Draft Version 1.0, 2 volumes (1993)
44. Vaughn, R., Henning, R. and Siraj, A.: Information Assurance Measures and Metrics: State of Practice and Proposed Taxonomy. Proc. of 36th Hawaii Int. Conf. on System Sciences HICSS 03. (2003)
45. Vogel, C.: Cognitive Engineering. Masson, Paris, France (1988)
46. Yee, B. S.: Security Metrology and the Monty Hall Problem. Proc. of Workshop on Information Security System Scoring and Ranking (WISSSR), ACSA and MITRE, Williamsburg, Virginia, May, 2001 (2002)