Towards a Classification of Security Metrics [*]

Carlos Villarrubia, Eduardo Fernández-Medina, and Mario Piattini

Universidad de Castilla - La Mancha, Alarcos Research Group
Paseo de la Universidad, 4, 13071, Ciudad Real(Spain),

Abstract. For the generation of trust in the use of information and communications technologies it is necessary to demonstrate security in the use of these technologies. Security metrics or assurance metrics are the most appropriate method to generate that trust. In this article we propose a series of features for classifying security metrics. We present the main conclusions obtained through this classification together with the list of metrics analyzed.

1 INTRODUCTION

The information and support processes, systems and networks are important assets to any organization. These assets suffer risks and insecurities continually coming from a wide variety of sources, including threats based in malicious code, programming errors, carelessness of people, sabotages or fires.

According to [1], the loss due to malicious code alone exceeded $13 billion in 2001, and security expenditures are projected at more than $3 billion in 2004.

This concern has prompted many organizations and investigators to propose different metrics to evaluate the security of their information system. In general, there exists a consensus in affirming that the election of the metric depends on those concrete security necessities of each organization. Most of the analyzed proposals propose methodologies for the election of these metrics [2–7]. Even in some cases the necessity is suggested of developing specific methodologies for each organization [8].

In any one of these proposals the necessity is to quantify the different relative aspects of security to be able to understand, to control and to improve the trust in the information system.

If an organization doesn't use security metrics to make decisions, the choices will be motivated by purely subjective aspects, external pressures or even purely commercial motivations.

[*] This research is part of the CALIPO project, supported by the Dirección General de Investigación of the Ministerio de Ciencia y Tecnología (TIC2003-07804-C05-03), and the MESSENGER project, supported by the Consejería de Ciencia y Tecnología of the Junta de Comunidades de Castilla-La Mancha (PCC-03-003-1).

Villarrubia C., Fernández-Medina E. and Piattini M. (2004).
Towards a Classification of Security Metrics.
In *Proceedings of the 2nd International Workshop on Security in Information Systems*, pages 341-350
DOI: 10.5220/0002688203410350

2 SECURITY METRICS

2.1 Metrics Classification

To analyze the different metric proposals it is necessary to use certain approaches to classify them and to be able to obtain conclusions.

The selection of these classification approaches is based on the different previous proposals [9, 3, 4, 7], keeping in mind that they cover the different necessities of the security of an organization, eliminating the repetitions of proposed approaches and selecting those approaches with greater generality.

The approaches selected to classify the security metrics correspond to the different objectives of security pursued, to the control area used to get those objectives, the moment that those controls are applied and to the audience directed with that metric.

1. Security Objective (SO). The security of a system is characterized by information like the persecution of the following objectives:
   - Confidentiality, assuring that only those who are authorized can access the information.
   - Integrity, assuring against the unauthorized modification of the information.
   - Availability, assuring that the authorized users have access to the information and their assets associates when they require it.
   - Authentication, assuring that the identity of a subject or resource is the one claimed.

   In our study, we have included a general objective to characterize those metrics that pursue two or more objectives of security.
2. Control Area (CA). The previous objectives are achieved using different controls in the information system. According to [9], those different types of controls to get the objectives of security can be classified as:
   - Management. Security controls that can be characterized as managerial. In general, they focus on the management of the computer security program and the management of the risk within the organization.
   - Operational. Security controls implemented and executed by people (as opposed to systems).
   - Technical. Security controls that the computer system executes.
3. Temporal Dimension (TD). From the point of view of the risks management, the used controls can be applied in different instants:
   - Preventive. Designed to lower the amount and impact of threat.
   - Detective. Used to detect threat once it has occurred.
   - Corrective. Implemented to help mitigate the impact of a loss event.
   - Recovery. They allow the recovery of the system to the state previous to the attack.
4. Intended Audience (IA). The security metrics are the fundamental mission to inform on the different aspects of security. [7] classifies a metric depending on the following intended audience:
   - Technical. Technical personnel of the company or institution.
   - Decision Makers. Different people responsible for the company.
   - External Authorities. Any external entity to the company that should inform on the situation of the security of the company.

2.2 Metrics features

The information of the previous paragraph can be even more valuable to the stakeholders if it comes accompanied by additional information on the metrics themselves, which may help discriminate between metrics with the same functionality and purpose. Based on the proposal of [10], we will distinguish six features for a given metric. The first group identifies three of the basic (intrinsic) properties of any metric. The three remaining features determine whether the metric has been validated or not, the kind of validation used (theoretical or empirical), and whether the metric has a tool that automates its measurement process or not.

1. Objectivity/Subjectivity (O/S). A metric is objective if its values are calculated by an algorithm or a mathematical formula. On the contrary, a metric is subjective if its measurements are (totally or partially) provided by a human being. In case of subjective metrics, it is very important to record the person or expert that performs the evaluation and provides the values.
2. Direct/Indirect (D/I). According to ISO 9126, a direct measure is a measure of an attribute that does not depend upon a measure of any other attribute. An indirect measure is a measure of an attribute that is derived from measures of one or more other attributes.
3. Run-time/Static (R/S). This characteristic classifies a metric depending on the moment in which it can be measured. Run-time metrics can only be measured during system operation, acting on instances of the component or system being evaluated. Static measures can be evaluated based on the component properties only. Examples of run-time measured metrics are percentage of used media sanitized before reuse or disposal and number of intrusion attempts reported. Static measured metrics include percentage of systems that have a contingency plan or percentage of laptops with encryption capability for sensitive files.
4. Theoretical Validation (TV). The main goal of theoretical validation is to prove that a metric actually measures what it is supposed to measure [11]. Theoretical validation can also help us know when and how to apply the metric. This feature indicates whether the metric has been theoretically validated or not, and how. Even though several methods and principles have been proposed for metric theoretical validation (mainly in the context of software engineering), there is no widely accepted proposal yet. The two major approaches currently proposed are the following:
   - Measurement-theory based approaches such as those proposed by [12], [13], and [14].
   - Property-based approaches (also called axiomatic approaches), such as those proposed by [15] and [16, 17].
5. Empirical Validation (EV). Empirical validation tries to demonstrate with real evidence that the metrics meet their objective, and that they are useful in practice. There are three major types of empirical research strategy:
   - Experiments. Experiments are formal, rigorous and controlled investigations. They are launched when we want control over the situation and want to manipulate behavior directly, precisely and systematically. Hence, the objective is to manipulate one or more variables and control all other variables at fixed

levels. An experiment can be carried out in an off-line situation, for example in a laboratory under controlled conditions, where the events are organized to simulate their appearance in the real world. Experiments may alternatively be carried out on-line, which means that the research is executed in the field under normal conditions [18, 19].

- Case Studies. A case study is an observational study, i.e., it is carried out by the observation of an on-going project or activity. The case study is normally aimed at tracking a specific attribute or establishing relationships between different attributes. The level of control is lower in a case study than in an experiment [20].
- Surveys. A survey is often an investigation performed in retrospect, when, for example, a tool or technique has been in use for a while. The primary means of gathering qualitative or quantitative data are interviews or questionnaires. These are completed by taking samples which are representative of the population to be studied. The results from the survey are then analyzed to derive descriptive or explanatory conclusions. Surveys provide no control over the execution or the measurement, though it is possible to compare them to similar ones [21].

6. Automation (A). This feature indicates whether the metric has specific tool support or not. Not only methodological, but also technological support is definitely required for the effective use of metrics in industrial settings [22].

3 ANALYSIS OF EXISTING SECURITY METRICS

As mentioned in the introduction, we are currently witnessing a proliferation of metrics for security. For the present study, we surveyed the existing literature on these topics, looking for metrics that could provide interesting information for description, comparison or prediction of any aspect related to the security of an information system. Interestingly, we had to discard some of the metrics because they didn't have a sufficient description to be able to determine the values of those characteristics used to classify these metrics. Examples of these metrics include those used as examples in those articles that describe methodologies for the construction of these metrics. We also discarded repeated metrics, i.e., those metrics proposed by more than one author. We included one instance of such metrics only. Finally, 57 metrics from 85 different proposals were selected, which are listed in the Appendix of this paper.

Regarding the specific classification approaches to security, the results have been the following:

- Security Objective: 74% of the metrics were general, while 9% of the metrics were to do with availability and authentication.
  7% were confidentiality metrics and only one was specific to the integrity.
- Control Area: 44% of the metrics were operational, 30% were relative of technical, and the rest were management.
- Temporal Dimension: 84% of the metrics were preventive metrics, 9% were detective metrics, and 2% were corrective metrics and recovery metrics respectively.

– Intended Audience: 44% of the metrics were for decision makers, 39% were for technical people and the rest for external authorities.

After evaluating the features of the metrics, the following list shows a summary of the results obtained.

– Objectivity or Subjectivity: 96% of the metrics were objective, the rest subjective.
– Direct or Indirect: 61% of the metrics were indirect, the rest were direct.
– Static or Run-time: 63% of the metrics were static metrics, the rest were run-time.
– Theoretical validation: None of the surveyed metrics had been theoretically validated.
– Empirical validation: Only one of the metrics had been empirically validated- even worse, and none of the rest of the proposals mentioned empirical validation as something they were planning to achieve as part of their future work.
– Automation: Only one of the metrics had some kind of supporting tool.

These results provide a global picture the profile of the surveyed metrics:

– As expected, most of the metrics defined are general metrics and this type of metric only measures general actions relative to the security and in an indirect way they have the preservation of the confidentiality, integrity and availability as objectives.
– Most of the metrics are of a preventive character showing the importance granted to avoidance of problems of security.
– Regarding the area of the used controls and intended audience they have there exists a reasonable balance indicating that the metric proposals form correct aspects.
– Most of the metrics are objective. This is good, since this kind of metrics are more reliable and easier to automate.
– Most of the metrics are direct metrics. Although these metrics are very important, they are only a first step towards the final goal of satisfying the information needs of a user. Hence, indirect metrics, which usually provide more information than direct metrics, and indicators based on them should also be defined
– The lack of validation and automation of the metrics is common to all the disciplines in which the application of metrics is still immature, and clearly shows an area of research that needs to be addressed in order to be able to rely on real engineering methods and tools.

4 CONCLUSIONS AND FUTURE WORK

In this paper we have presented the results of a survey we have conducted on the most representative existing security metrics.

The results obtained show the distribution of the metrics and, more importantly, the areas with lack of metrics which therefore require the definition of new metrics, specific for these areas.

There are several possible extensions to our work. In the first place, we need to continue classifying forthcoming metrics, in order to confirm and validate the conclusions extracted from this first classification, and to further analyze the tendencies in the time for the proposition of new metrics.

We also want to start analyzing the relative importance among those metrics for the attainment of the objectives of security. In this way, additional approaches will be used to prioritize the use of metrics. We also want to analyze the difficulty in the obtaining of the metric ones or in their use to guide in the modification of those metrics to be more useful.

The characterization of security metrics proposed is not complete because some metrics are the same values for all features. A future work is to refine this characterization so that each metric is different in the classification.

Finally, indicators should be defined in function of the size of the organization and sector (for example, public sector and private sector) because it is not realistic to have a good group of metrics which are useful for all the organizations.

References

1. Mercuri, R.T.: Analyzing security costs. Communications of the ACM **46** (2003) 15–18
2. Swanson, M., Bartol, N., Sabato, J., Hash, .J., Graffo, L.: Security metrics guide for information technology systems. Technical Report NIST 800-55, National Institute of Standards and Technology (2003)
3. Vaughn, Jr., R.B., Henning, R., Siraj, A.: Information assurance measures and metrics - state of practice and proposed taxonomy. In: Proceedings of the 36th Hawaii International Conference on Systems Sciences. (2003)
4. Bouvier, P., Longeon, R.: Le tableau de bord de la sécurité du système d'information. Sécurité Informatique (2003)
5. Nielsen, F.: Approaches of security metrics. Technical report, NIST-CSSPAB (2000)
6. Payne, S.C.: A guide to security metrics. Technical report, SANS Institute (2001)
7. ACSA, ed.: Proceedings of the Workshop on Information Security System Scoring and Ranking, Williamsburg, Virginia (2001)
8. Colado, C., Franco, A.: Métricas de seguridad: una visión actualizada. SIC. Seguridad en Informática y Comunicaciones **57** (2003) 64–66
9. Swanson, M.: Security self-assessment guide for information technology systems. Technical Report NIST 800-26, National Institute of Standards and Technology (2001)
10. Calero, C., Martín-Albo, J., Piattini, M., Vallecillo, M.B..A., Cechich, A.: A survey on software component metrics. Submitted to ACM Computing Surveys (2003)
11. Fenton, N., Pfleeger, S.: Software Metrics: A Rigorous Approach. 2nd edn. Chapman Hall, London (1997)
12. Whitmire, S.: Object Oriented Design Measurement. Wiley, New York (1997)
13. Zuse, H.: A Framework of Software Measurement. Walter de Gruyter, Berlin (1998)
14. Poels, G., Dedene, G.: Distance-based software measurement: Necessary and sufficient properties for software measures. Information and Software Technology **42** (2000) 35–46
15. Weyuker, E.J.: Evaluating software complexity measures. IEEE Transactions on Software Engineering **14** (1988) 1357–1365
16. Briand, L.C., Morasca, S., Basili, V.R.: Property-based software engineering measurement. IEEE Transactions on Software Engineering **22** (1996) 68–86
17. Briand, L.C., Morasca, S., Basili, V.R.: Property-based software engineering measurement: Refining the additivity properties. IEEE Transactions on Software Engineering **23** (1997) 196–197

18. Juristo, N., Moreno, A.: Basics of Software Engineering Experimentation. Kluwer Academic Publishers (2001)
19. Wohlin, C., Runeson, P., Ohlsson, M., Regnell, B., Wesslen, .A.: Experimentation in Software Engineering: An Introduction. Kluwer Academic Publishers (2000)
20. Yin, R.: Case Study Research: Design and Methods. 2nd edn. Applied Social Research Methods Series, vol 5 Sage Publications Inc, Thousand Oaks, CA (1994)
21. Pfleeger, S., Kitchenham, B.: Principles of survey research. Software Engineering Notes **26** (2001) 16–18
22. Lavazza, L.: Providing automated support for the gqm measurement process. IEEE Software **17** (2000) 56–62
23. Departament of the Air Force: AFI33-205. Information Protection Metrics and Measurements Program. (1997)
24. Calero, C., Piattini, M., Genero, M.: Empirical validation of referential integrity metrics. Information and Software Technology **43** (2001) 949–957
25. ISO: ISO 7498-2. Open Systems Interconnection - Basic Reference Model - Part 2: Security Architecture. (1989)
26. ISO/IEC: ISO/IEC TR 13335-1. Guidelines for the Management of IT Security. Part I: Concepts and Models of IT Security. (1996)
27. ISO/IEC: ISO/IEC 15408. Evaluation Criteria for IT Security. (1999)
28. ISO/IEC: ISO/IEC 17799. Code of Practice for Information Security Management. (2000)
29. King, G.: Best security practices: An overview. In: Proceedings of the 23rd National Information Systems Security Conference, Baltimore, Maryland, NIST (2000)
30. Marcelo, J.M.: Identificación y Evaluación de Entidades en un Método AGR. In: Seguridad de las Tecnologías de la Información. AENOR (2003) 69–103
31. McKnight, W.L.: What is information assurance? CrossTalk. The Journal of Defense Software Engineering (2002) 4–6
32. Schuedel, G., Wood, B.: Adversary work factor as a metric for information assurance. In: Procedings of the New Security Paradigm Workshop, Ballycotton, Ireland (2000) 23–30
33. Carnegie Mellon University Pittsburgh, Pennsylvania: SSE-CMM Model Description Document. 3.0 edn. (2003)
34. Vaughn, Jr., R.B., Siraj, A., Dampier, D.A.: Information security system rating and ranking. CrossTalk. The Journal of Defense Software Engineering (2002) 30–32

APPENDIX

This appendix presents, in tabular form, the metrics that we have surveyed for our analysis, and the dimensions and features assigned to each of them.

Metric information is displayed in columns. Column one is a sequence counter (1 to 57). Column two show the metric name and description, together with the reference to the article in which the metric was originally defined. Columns three to six show the dimensions assigned to the metric. Finally, columns seven to twelve display the values assigned to the metric features.

The values assigned to the cells of the columns three at six they have the following meaning:

- Column SO (Security Objective): C (Confidentiality), I (Integrity), A (Availability), AU (Authentication) and G (General).
- Column CA (Control Area): M (Management), O (Operational) and T (Technical).

- Column TD (Temporal Dimension): P (Preventive), D (Detective), C (Corrective) and R (Recovery).
- Column IA (Intended Audience): T (Technical Experts), D (Decision makers) and E (External authorities).

The values assigned to the cells in the last two columns (Empirical validation and Automation) require some special explanations:

- Column ”EV” shows whether the metric has gone through any kind of empirical validation. Cells in this column may be either empty, or have the following values: ”1E” (validated by one experiment); or ”FW” (mentioned as future work by the metric authors).
- Column ”A” shows the kind of automated support for the metric. Cells of this column may be either empty, or have the value ”CT”, indicating that there is a tool that supports the metric. A description of such tool can be found in the paper cited for the metric.

N	Metric Description	SO	CA	TD	IA	O/S	D/I	R/S	TV	EV	A
1	Percentage of critical data files and operations with an established backup frequency [2]	A	O	P	T	O	I	S	N		
2	Percentage of systems that have a contingency plan [2]	A	O	P	E	O	I	S	N		
3	Percentage of systems for which contingency plans have been tested in the past year [2]	A	O	P	E	O	I	S	N		
4	Number of uses of the backups [4]	A	O	R	D	O	D	R	N		
5	Annual down time for a system [3]	A	T	D	D	O	D	R	N		
6	Percentage of systems that perform password policy verification [2]	AU	O	P	D	O	I	S	N		
7	Percentage of users with special access to systems who have undergone background evaluations [2]	AU	O	P	D	O	I	S	N		
8	Number of failed login attempts [3]	AU	O	D	T	O	D	R	N		
9	Percentage of systems without active vendor-supplied passwords [2]	AU	T	P	T	O	I	S	N		
10	Percentage of unique user [2]	AU	T	P	T	O	I	S	N		
11	Percentage of websites with a posted privacy policy [2]	C	O	P	D	O	I	S	N		
12	Percentage of used media sanitized before reuse or disposal [2]	C	O	P	T	O	I	R	N		
13	Number of clock cycles per byte encrypted [3]	C	T	P	T	O	D	R	N		
14	Percentage of laptops with encryption capability for sensitive files [2]	C	T	P	T	O	I	S	N		
15	Frequency of the audits [4]	G	M	P	D	O	D	R	N		
16	Number of rules for security's politics [4]	G	M	P	D	O	D	S	N		
17	Level of maturity in developers' process [33]	G	M	P	D	O	D	S	N		
18	Percentage allocated for security program [3]	G	M	P	D	O	D	S	N		
19	Percentage of systems that have had risk levels reviewed by management [2]	G	M	P	D	O	I	S	N		
20	Percentage of systems recertified if security controls are added/modified after the system was developed [2]	G	M	P	D	O	I	S	N		
21	Percentage of systems that are operating under an Interim Authority to Operate (IATO) [2]	G	M	P	D	O	I	S	N		
22	Percentage of systems with approved system security plans [2]	G	M	P	D	O	I	S	N		
23	Risk assessment [30]	G	M	P	D	S	D	R	N		CT
24	Percentage of systems that had formal risk assessments performed and documented [2]	G	M	P	E	O	I	S	N		
25	Percentage of total systems for which security controls have been tested and evaluated in the past year [2]	G	M	P	E	O	I	S	N		
26	Percentage of systems that have the costs of their security controls integrated into the life cycle [2]	G	M	P	E	O	I	S	N		
27	Percentage of total systems that have authorized for processing following certification and accreditation [2]	G	M	P	E	O	I	S	N		
28	Percentage of current security plans [2]	G	M	P	E	O	I	S	N		
29	Assessment of the execution of the recovery plans [4]	G	M	R	D	S	D	R	N		
30	Percentage of information systems libraries that log the deposits and withdrawals of tapes [2]	G	O	P	T	O	I	S	N		
31	Percentage of data transmission facilities in the organization that have restricted access to authorized users [2]	G	O	P	T	O	I	S	N		
32	Percentage of software changes documented and approved through change request forms [2]	G	O	P	T	O	I	S	N		
33	Percentage of in-house applications with documentation on file [2]	G	O	P	T	O	I	S	N		
34	Percentage of users with access to security software that are not security administrators [2]	G	O	P	T	O	I	S	N		
35	Number of hours employed in formation [4]	G	O	P	D	O	D	R	N		
36	Percentage of formed people [4]	G	O	P	D	O	I	R	N		
37	Percentage of systems compliant with the separation of duties requirement [2]	G	O	P	D	O	I	S	N		
38	Percentage of systems that impose restrictions on system maintenance personnel [2]	G	O	P	D	O	I	S	N		
39	Percentage of systems with documented risk assessment reports [2]	G	O	P	D	O	I	S	N		
40	Number of incidents reported to FedCIRC, NIPC, and local law enforcement [2]	G	O	P	E	O	D	R	N		
41	Percentage of employees with significant security responsibilities who have received specialized training [2]	G	O	P	E	O	I	R	N		
42	Percentage of agency components with incident handling and response capability [2]	G	O	P	E	O	I	S	N		
43	The average time elapsed between vulnerability discovery and implementation of corrective action [2]	G	O	C	T	O	D	R	N		
44	Percentage of security-related user issues resolved immediately following the initial call [2]	G	O	C	D	O	I	R	N		
45	Number of detected attacks [4]	G	O	D	D	O	D	R	N		
46	Number of invalid packets rejected for a firewall [3]	G	T	P	T	O	D	R	N		
47	Number of elements dedicated to network security [4]	G	T	P	T	O	D	S	N		
48	Number of components with audit trail [4]	G	T	P	T	O	D	S	N		
49	Evaluation Assurance Level according Common Criteria for a system [27]	G	T	P	T	O	D	S	N		
50	Percentage of systems with the latest approved patches installed [2]	G	T	P	T	O	I	R	N		
51	Percentage of systems with automatic virus definition updates and automatic virus scanning [2]	G	T	P	T	O	I	R	N		
52	Percentage of systems running restricted protocols [2]	G	T	P	T	O	I	S	N		
53	Percentage of systems on which audit trails provide a trace of user actions [2]	G	T	P	T	O	I	S	N		
54	Adversary work factor [32]	G	T	P	D	O	D	R	N	IE	
55	Number of intrusion attempts reported [23]	G	T	D	D	O	D	R	N		
56	Number of reported successful intrusions with limited access or total access [23]	G	T	D	D	O	D	R	N		
57	Number of systems with functions of integrity in files [4]	I	T	P	T	O	D	S	N		