A Framework for Security Metrics Based on Operational System Attributes

Erland Jonsson
Department of Computer Science and Engineering
Chalmers University of Technology
Göteborg, Sweden
erland.jonsson@chalmers.se

Laleh Pirzadeh
Department of Computer Science as Engineering
Chalmers University of Technology
Göteborg, Sweden
laleh.pirzadeh@chalmers.se

***Abstract*— There exists a large number of suggestions for how to measure security, and in many cases the goal is to find a single overall metric of security. Given that security is a complex and multi-faceted property, we believe that there are fundamental problems to find such an overall metric. Thus, we suggest a framework for security metrics that is based on a number of system attributes taken from the security and the dependability disciplines. We then regroup those attributes according to an existing conceptual system model and propose a metrication framework in accordance. We suggest that there should be metrics related to protective attributes, to behavioural attributes and possibly to system correctness. Thus, the main idea is that security metrication should be split up and related to a number of specific attributes, and that a composite security metric is hard to define.**

Keywords: operational security; security metrics; modelling; protective metrics; behavioural metrics

I. INTRODUCTION

In this paper we will suggest a novel security metrication approach that is based on a combined security/dependability model [11]. There have been several previous attempts to present various frameworks and directions in the security metrication research field. The first comprehensive attempt towards structuring the security measurement and metrication research was carried out at the WIISSR workshop [18]. Other proposals and extensions to this were made in e.g. [2-5], [7], [12-17] and [20].

In this paper we start out from a conceptual security/dependability model that describes a system's interaction with its environment via the system boundaries [11]. Based on the model we regroup the traditional security and dependability attributes into protective attributes, behavioural attributes and correctness and we suggest a framework for how to define metrics in accordance.

In the following, section II briefly describes the security model. In section III two main approaches toward model-based security metrication are suggested and the implication of the security model for metrication is discussed. Section IV highlights some important relations among the protective and behavioural attributes. Finally, we conclude the paper in section V.

This work has been sponsored by the *Swedish Civil Contingencies Agency* (*MSB*).

II. A PROPOSED SYSTEM SECURITY MODEL

This section gives a brief description of the system model for security and dependability attributes originally proposed in [11]. Once again, for simplicity, we use the term *security* to denote the combined concept of security and dependability. Normally security is decomposed into three different aspects: *confidentiality*, *integrity* and *availability* [6], whereas dependability is decomposed into the attributes: *availability*, *reliability*, *safety*, *integrity* and *maintainability* [1].

Our approach is that the security of a system should be understood in relation to its environment, in terms of system input and output. First, we define the system that we are considering, the ***object system***. It is important to clarify the boundaries of the object system, since the subsequent discussion of the security model is based upon a well-defined system. The object system may be arbitrarily complex: a single computer, a computer network or possibly a whole organisation, including people. Note that by studying a larger system more of the potential problems are "embedded" into the system as internal or insider problems. These problems are not directly addressed in the paper. Conceptually, the object system interacts with the environment in two basically different ways. The object system either receives an *input* from the environment, or delivers an *output* to the environment. See figure 1. The input to the system is denoted ***environmental influence***. The environmental influence may be of many different kinds. It may be the "normal" input provided by the authorized user of the system. We have termed this concept *accessability*. However, the type of interaction we are mostly interested in here is that which involves fault introduction. Malicious, external faults, i.e., attacks, are particularly interesting. Such faults originate from a ***threat*** in the environment. The threat may be a human being, a natural phenomenon or another computer system, among other things. The threat launches an ***attack*** towards the system. The attack will be successful if it can exploit a ***vulnerability*** in the system so that an intrusion results. The presence of the intrusion can be regarded as an ***error*** (or erroneous state) in the system. Note that a vulnerability is a passive feature of the system as opposed to an error. The error may (or may not) propagate and lead to a

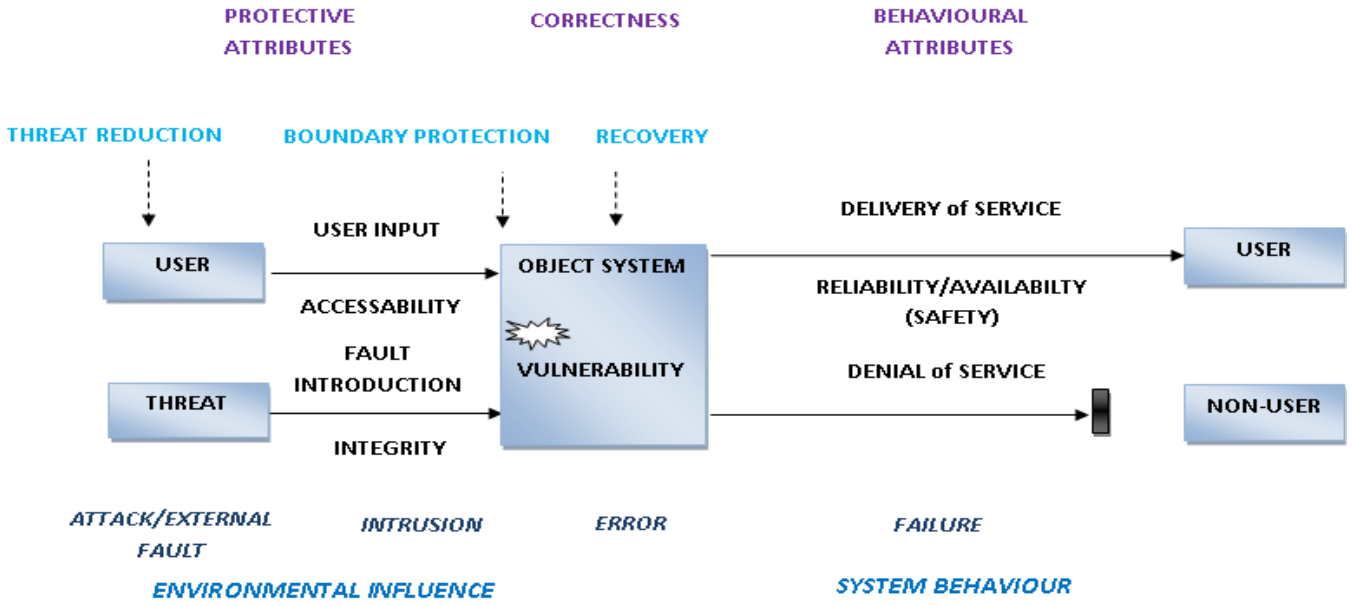

Figure 1. An Integrated Model of Security and Dependability

system ***failure***. This depends on the implementation of the system, how it is operated, what defensive mechanisms are active etc. Thus, there is a causal relationship between those ***impairments***: external fault/attack, error/intrusion and failure. We can also see that there are three basic ways to break the causal chain of unwanted events and to counter the propagation of impairments: *threat reduction*, *boundary protection* and *recovery*. See figure 1. Further details on impairments and their interaction can be found in [10] and [1].

We will now discuss the relation between these impairments and security aspects. Since faults are detrimental to the system, we seek to design the system such that the introduction of faults is prevented. We denote this ability ***integrity***. It is thus a ***protective attribute*** of security. It is our opinion that the integrity attribute is in effect the essence of security. The conceptual output from the object system is the ***system behaviour***. The system behaviour includes the notion of service delivery to the USER(s). As originally observed in [11] there are two fundamentally different types of users: authorized users (called ***USERs***) and unauthorized users (called ***NON-USERs***). This in itself might be evident, but the importance of the observation lies in the fact that the required system behaviour is different for USERS and NON-USERS. Thus, the behavioural attributes are of two types: delivery-of-service and denial-of-service. The desired (and preferably specified) ***delivery-of-service*** to the USER is described by the ***availability*** and ***reliability*** aspect.

Another desired quality is that the system shall have an ability to deny service, denoted ***denial-of-service***, to the NON-USER. (This is marked as a bold "stop-bar" in figure 1.) Note the duality of these concepts. The normal and preferred situation for the USER, i.e. that the service is indeed delivered, implies a failure with respect to the NON-USER and vice versa. If the service denied relates to information it is described by the behavioural attribute ***confidentiality***. In case it relates to other services we use the word ***exclusivity*** [21]. Thus, exclusivity is the ability of the system to deny any unauthorized use of system service.

Finally, the ***safety*** attribute introduces another aspect of system behaviour. It models the severity of a failure. In its most primitive, binary form it maps failures into catastrophic and non-catastrophic failures. Safety failures represent subsets of reliability/availability failures or confidentiality/exclusivity failures. An example of a "catastrophic failure" is a failure in the drive-by-wire system of a car that would lead to an accident, with possible casualties. Another example is the unauthorized disclosure of secret, military information that would have disastrous consequences in case of war.

The ***maintainability*** attribute has no place in our model, as it does not describe an operational system-environmental interaction.

III. Security Metrics Based on the System Model

A. Defining Two Different Types of Security Metrics

The conceptual system model presented in section II suggests that security metrics could be defined according to the suggested two types of system-environment interaction. Thus, we could define ***protective security metrics*** (referring to the input) and ***behavioural security metrics*** (referring to the output). As already noted, we believe that protective security captures the most important characteristics of security, and in particular the notion of protection. Consequently, it could be launched as a new security definition. Behavioural security is dependent on protective security and in this respect it is secondary to it. One could chose to call behavioural security something else, e.g. dependability or trustworthiness.

It should also be possible to define some kind of ***internal*** metrics that would reflect the ***correctnesss*** of the system. It could be discussed whether correctness is really a security attribute or not. We have chosen to

handle it as a separate concept as it does not directly interact with the environment.
In the following we will define and discuss these kinds of metrics in some detail.

B. Protective Security Metrics

1) How could protective security be measured?

Protective metrics should assess the extent to which the system is able to protect itself against unwanted external influence, e.g. external attacks. Normally, we assume that there is some kind of malicious intent involved in this influence, but you could also think of situations when the unwanted input is the result of e.g. a mistake made by an "ordinary" USER. We do not attempt to suggest a more exact definition for this case, as it will not affect the overall reasoning or treatment of the situation.

There are at least two different approaches to measure protective security. The first one is called ***system-related*** and refers to the system's ability to protect itself in terms of protection mechanisms. The other one is called ***threat-related***. It measures security in terms of the effort an attacker has to expend in order to make an intrusion. These two approaches are detailed below.

2) Metrics based on security protection mechanisms

As mentioned in the preceding section, one approach toward protective security measurement is to measure security based on the three fundamental methods to avoid failures in a system ("defence lines"): threat reduction, boundary protection and (internal) recovery. The measure would be based on the combined strength of all involved security mechanisms. It is not a priori evident how to calculate the combined strength. The input protection will not necessarily be higher if stronger mechanisms are involved. This is due to the fact that the protective strength rather lies in the fact that there are no weak mechanisms. Or in other words, there should be no vulnerabilities or "holes" in the system in order for it to be well protected. Therefore, it is a non-trivial task to find a method for such a combination of the effect of a number of protective mechanisms.

3) Using attacker effort as a protective security metric

The second way to measure security is to base the metric upon the *effort* that has to be expended by an attacker in order to make a breach into the system, i.e. to compromise integrity. This approach was first proposed by Littlewood et al. [19]. The idea is that an effort-based measure should be representative of all environment factors having effect on the attacker's effort to make a successful intrusion. The main contributing factors of effort are the *time* it takes to carry out the attack and the *skill level* of the attacker. However, many other parameters have to be considered: population of attackers, attack space size, reward effect on attackers' behaviour, system feedback to the attacker, attackers' willingness, etc.

An attempt to make a real measurement by performing supervised attack experiments was reported in [8]. This work showed that it is in principle possible to find a metric for effort. In this simplified case the metric was Mean Time To Intrusion[1] (MTTI), i.e. the average time used by an attacker to make an intrusion. It was also shown that, given certain pre-conditions the MTTI metric could be combined with a MTTF metric derived from random errors, such as component errors. However, the practical metric from such an experiment has limited applicability and does only reflect the security of the used system at the time of measurement. It remains to be demonstrated how to make measurements that are generally applicable and that could serve to make predictions of the security of other similar systems.

C. Behavioural Security Metrics

As suggested by the model, the behavioural security attributes[2] are: reliability, availability, safety, confidentiality and exclusivity. There are already a large number of metrics suggested for reliability, availability and safety and they could readily be incorporated into the framework. Confidentiality and exclusivity metrics are less well investigated. Below we shortly describe existing or proposed metrics for behavioural security attributes.

Reliabilty is the expected time duration the system is operating before it fails in delivering its service. The common metric for this purpose is Mean-Time-to-Failure (MTTF).

Availability on measures to which degree, often expressed in percent, the system is capable of delivering its service taken into account the alternation of service delivery and non-delivery [22]. A common steady-state availability metric is calculated as: Mean Time To Failure/ (Mean Time To Failure + Mean Time to Repair)).

Safety evaluates the absence of catastrophic consequences on the USERs and the environment in case of a failure [22].
A common metric for safety is Mean Time to Catastrophic Failure (MTTCF) and it is defined in analogy with Mean Time To Failure.

Confidentiality is the ability of the system to keep sensitive information confidential with respect to NON-USERs. We have not found many proposals for how to measure confidentiality [9].

The concept of ***exclusivity*** is not widely used and we know of no suggestions for how to measure it. However, it seems plausible that an approach similar to that of confidentiality could be adopted.

D. Correctness Metrics

Correctness should be assessed with respect to the internal state of the system. This means that we have to define a state that could serve as a template for "full"

[1] Sometimes referred to as Mean Time To Compromise (MTTC).
[2] Or more accurately: security and dependability related attributes

correctness and then measure the actual deviation from this state. However, there are several problems to define correctness in practice. For one thing we have to distinguish between correctness of the data in the system and the system itself, i.e. the programs, mechanisms, hardware, etc. It should be possible, even if not trivial, to define what is meant by correct data, for example in a database, but it seems harder to define correctness for the system itself. If we could find a good correctness definition, the next step would be to find the degree of incorrectness, i.e. the deviation from the correct state. We are not aware of any research attempts to address this problem and we will not make any such suggestions in this paper. We limit ourselves to observe that a correctness metric will be needed to make the set of system-related metrics complete.

IV. DISCUSSION

We realize that the behavioural attributes of the system are dependent upon the environmental threats, protection mechanisms and the internal recovery mechanisms. As a conclusion, the behavioural attributes, e.g. reliability, vary with respect to the strength of the three defence lines in the system in such a way that a better defence will lead to increased reliability. Thus, the better the defence mechanisms are the higher becomes the reliability of the system. Therefore, higher integrity ("security") will lead to higher reliability. The same reasoning is of course also valid for availability, safety, confidentiality and exclusivity. It should be noted that this effect will apply even if the defence mechanisms only present a delay of impairments' propagation, a *latency effect.*

V. CONCLUSIONS

We have suggested a framework for security metrication that is based on an input-output-related system model for security and dependability. The model describes the attributes of these two concepts and how they interact with the system's environment. This leads us to the conclusion that there are at least two possible sets of security metrics: protective security metrics, related to the system input, and behavioural security metrics, related to the system output. We have no firm opinion on how to treat correctness at this stage. As behavioural security metrics we incorporate those already defined from the dependability discipline. We suggest that protective security, i.e. integrity, is the one that is nearest to the essence of traditional security concept and could possibly be adopted as a new, more limited definition of security. We suggest two methods for the metrication of protective security.

REFERENCES

[1] A. Avizienis, J-C. Laprie, B. Randell and C. Landwehr, "Basic Concepts and Taxonomy of Dependable and Secure Computing", IEEE Transactions on Dependable and Secure Computing, Vol.1, No.1, Jan-Mar 2004.

[2] R. Savola. 2007, "Towards a taxonomy for information security metrics", In Proceedings of the 2007 ACM workshop on Quality of protection (QoP '07), pp. 28-30, 2007.

[3] R. Savola, "A Novel Security Metrics Taxonomy for R&D Organisations", ISSA 2008, July 2008, Johannesburg, South Africa.

[4] R. Savola, "A security metrics taxonomization model for software-intensive systems", Journal of Information Processing Systems, vol. 5, No. 4, pp. 197-206, 2009.

[5] Pironti, J. P, "Information security governance: Motivations, benefits and outcomes", Information Systems Control Journal, vol. 4, pp. 45-48, 2006.

[6] Information Technology Security Evaluation Criteria (ITSEC): Provisional Harmonized Criteria, December 1993. ISBN 92-826-7024-4.

[7] CISWG, "Report of the best practices and metrics teams" (Revised), Government Reform Committee, United States House of Representatives, 2005.

[8] E. Jonsson, T. Olovsson, "A quantitative model of the security intrusion process based on attacker behavior", IEEE Transactions on Software Engineering,, vol.23, no.4, pp.235-245, Apr 1997.

[9] E. Jonsson, M.Andersson, S.Asmussen, "An attempt to quantitative modeling of behavioural security", Proc. 11th International Information Security Conference, Cape Town, Sout Africa, May 1995 (IFIP/SEC'95).

[10] E. Jonsson, L. Strömberg, S. Lindskog, "On the Functional Relation Between Security and Dependbility Impairments", ACM New Security Paradigms Workshop, Caledon Hills, Canada, 23-25, September 1999 (NSPW 1999).

[11] E.Jonsson, "Towards an integrated conceptual model of security and dependability," Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on , vol., no., pp. 8 pp., 20-22 April 2006.

[12] R. Vaughn, R. Henning,A. Siraj., "Information Assurance Measures and Metrics", State of Practice and Proposed Taxonomy, Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03) - Track 9 - Volume 9(HICSS '03), Vol. 9. IEEE Computer Society, Washington, DC, USA, pp. 331.3--, 2003.

[13] NIST 800-55 Rev1, E.Chew, M. Swanson,K. Stine, N. Bartol, A.Brown,W. Robinson, "Performance measurement guide for information security", National Institute of Standards and Technology Special Publication #800-55-rev1, 2008.

[14] NIST 800-55, Swanson M., Nadya B., Sabato J., Hash J., Graffo L., "Security Metrics Guide for Information Technology Systems", National Institute of Standards and Technology Special Publication #800-55, 2003.

[15] NIST 800-26, Swanson M., "Security Metrics Guide for Information Technology Systems", National Institute of Standards and Technology Special Publication #800-26, Novembre 2001.

[16] NISTIR 7564, W. Jansen, "Directions in Security Metrics Research", National Institute of Standards and Technology, April 2009.

[17] ISO/IEC 27004:2009. 2009. "Information Technology — Security Techniques ʊ Information Security Management — Measurement," ISO/IECWISSRR. 2001.

[18] Workshop on Information-Security-System Rating and Ranking (ISSRR) held in Williamsburg, VA, May 21-23, 2001.

[19] B. Littlewood, S. Brocklehurst, N. Fenton, P. Mellor, D. Wright, J. Dobson, J. Mcdermid, D. Gollmann, and E. T. Ex. "Towards operational measures of computer security". Journal of Computer Security, Vol.2, pp.211-229, 1993

[20] S.C. Payne, "A Guide to Security Metrics", SANS Security Essentials

[21] C. Meadows, "An Outline of a Taxonomy of Computer Security Research and Development", 1993. ACM O-89791-635-2.

[22] D.M. Nicol, W.H. Sanders, K.S. Trivedi, "Model-based evaluation: from dependability to security", Dependable and Secure Computing, IEEE Transactions on , vol.1, no.1, pp. 48-65, Jan.-March 2004.