SECURWARE 2013 - The 7th International Conference on Emerging Security Information, Systems and Technologies

# Identifying Suitable Attributes for Security and Dependability Metrication

Erland Jonsson, Laleh Pirzadeh
Department of Computer Science and Engineering
Chalmers University of Technology
Göteborg, Sweden
{erland.jonsson, laleh.pirzadeh}@chalmers.se

***Abstract*— In this paper, we suggest a framework for security and dependability metrics that is based on a number of non-functional system attributes. The attributes are the traditional security attributes (the "CIA") and a set of dependability attributes. Based on a system model, we group those attributes into protective attributes and behavioural attributes and propose that metrication should be done in accordance. We also discuss the dependence between these two sets of attributes and how it affects the corresponding metrics. The metrics themselves are only defined to a limited degree. The concepts of security and dependability largely reflect the same basic system meta-property and are partly overlapping. We claim that the suggested approach will facilitate making quantitative assessment of the integrated concept of security and dependability as reflected by those attributes.**

***Keywords - security and dependability metrics; security and dependability modelling; protective metrics; behavioural metrics***

## I. INTRODUCTION

There exists a large number of suggestions for how to measure (or metricate) security, with different goals and objectives. The application areas range from business management and organizational systems to large software systems. The approaches may be theoretical, technical, administrative or practical. 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. In this paper, we suggest a restricted view on security [29] as being only the integrity attribute of the dependability-security concept. Thus, we start out from a conceptual system model that integrates security and dependability. Other approaches have been suggested, e.g., by emphasizing the uncertainty dimension [11] or using ontologies [25]. Further, an excellent overview and classification is given in [33]. Our model is an input-output model in the sense that it describes a system's interaction with its environment via the system boundaries [15, 38]. The model identifies the main attributes of security and dependability. It clarifies the relation between malicious environmental influence on the input side and the service output to the users of the system. Based on the model we regroup the traditional security and dependability attributes into protective attributes and behavioural attributes. We argue that metrics for dependability and security attributes can be defined in accordance. Thus, protective attributes can be metricated by protective metrics and the behavioural attributes by behavioural metrics as originally proposed in a short paper [31]. Here, we extend and detail this original proposal. Also, we apply a metrication process perspective and discuss the system-related dependencies between different types of metrics. This approach is different from existing approaches to clearly relate the metrics to system input and output attributes and to address the impact of latency aspects.

In the following, Section II gives a brief summary of traditional security and dependability attributes. Section III describes the security model. The three defence lines in the model are described in Section IV as well as the causal relationship between the impairments in the system model. In Section V, security metrication according to the model is suggested. Section VI discusses the dependence between protective and behavioural metrics and Section VII briefly describes some benefits with our approach. Finally, we conclude the paper in Section VIII.

## II. TRADITIONAL DEFINITIONS OF SECURITY AND DEPENDABILITY

In this section, we briefly summarize the traditional security and dependability terminology. Security is normally decomposed into three different aspects: *confidentiality, integrity* and *availability* [8], loosely called "the CIA". Confidentiality is the ability of the computing system to prevent disclosure of information to unauthorized parties. Integrity is the ability of the computer system to prevent unauthorized withholding, modification or deletion. Availability is the ability of the system to in fact deliver its service. More formally, it can be described as the probability that the system will be available, or ready for use, at a certain instant in time. Sometimes other characteristics are also suggested as security aspects, e.g., authentication and non-repudation, e.g., see [6, 9].

Dependability, on the other hand, is decomposed into the attributes: *availability*, *reliability*, *safety*, *integrity* and *maintainability* [2]. Here, reliability is a characteristic that reflects the probability that the system will deliver its service under specified conditions for a stated period of

 ISBN: 978-1-61208-298-1

time. Safety denotes the system's ability to fail in such a way that catastrophic consequences are avoided. Thus, safety is reliability with respect to catastrophic failures. (Please note that there exist several other definitions of safety, e.g., in the software development area [2, 39].) Availability and integrity are defined as above. Finally, the maintainability attribute denotes the system's ability to undergo modifications and repairs.

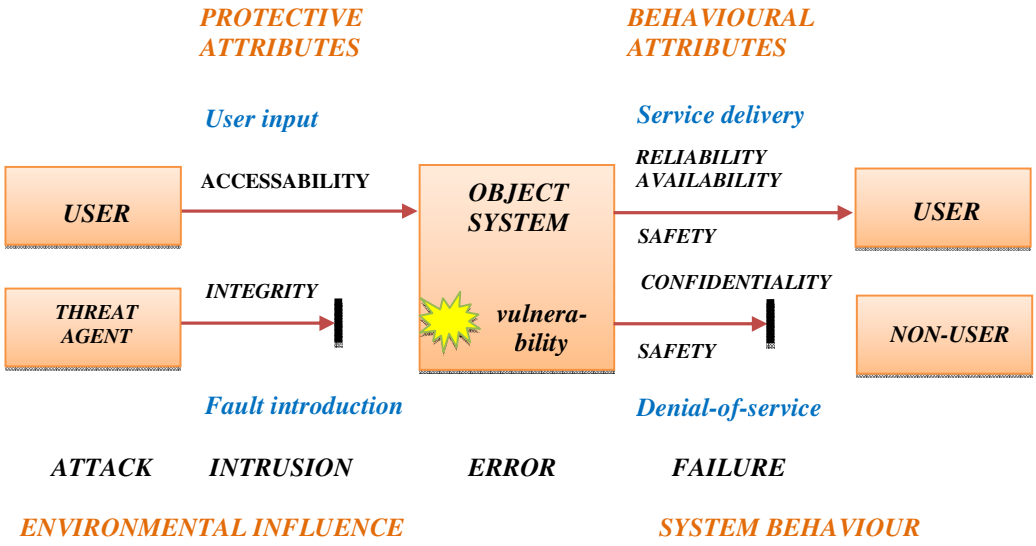


Fig. 1. An integrated model of security and dependability

It must be noted that the original dependability fault assumption was that of non-malicious, "stochastic" or "random" faults, such as those resulting from a component failure, rather than deliberate, malicious security faults (attacks). Such arbitrary faults might be internal faults, occurring (seemingly) spontaneously within the system, as well as external faults. Nowadays, both non-malicious and malicious faults are considered in existing models. However, because of the difficulty of making a formal or mathematical treatment of deliberate, malicious faults, most research so far has been done on dependability with a random fault assumption.

## III. A CONCEPTUAL SYSTEM MODEL

### A. *Interaction between the system and the environment*

This section gives a brief description of the system model for security and dependability attributes originally proposed by Jonsson [15]. Once again, for simplicity, we use the term *security* to denote the combined concept of security and dependability.

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. 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. The type of interaction we are interested in here is that which involves fault introduction. Malicious, external faults, i.e., attacks, are particularly interesting. Such faults originate from a ***threat*** (or ***threat agent***) in the environment. The threat may be a human being, a natural phenomenon or another computer system, among other things. The threat agent 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 result 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 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***: fault/attack, error/intrusion and failure. Further details on impairments and their interaction can be found in [2, 14].

 ISBN: 978-1-61208-298-1

### B. Defining the system attributes

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. (This is marked as a bold "stop-bar" in Figure 1.) We denote this ability ***integrity***. It is thus a ***protective attribute*** of security. The conceptual output from the object system is the ***system behaviour***. The system behaviour includes the notion of the degree of service delivery to the *authorized user* of the system, in the following denoted USER, and to the *non-authorized user,* denoted NON-USER.

Thus, the required system behaviour is different for USERs and NON-USERs. The desired ***service delivery*** to the USER is described by the ***availability*** and ***reliability*** attribute. The other desired quality is that the system shall have an ability to deny service, denoted ***denial-of-service***, to the NON-USER. (Marked by a "stop-bar".) Note the duality of these concepts. The normal and preferred situation with respect to 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*** [18]. Thus, exclusivity is the ability of the system to deny unauthorized use of system service.

Finally, the ***safety*** attribute introduces another aspect of system behaviour. It models the severity of a failure in the sense that it maps failures into catastrophic and non-catastrophic failures. All failures that are regarded as catastrophic, whether they represent a failure of service delivery or a failure of denial-of-service, are represented by the safety attribute. Thus, 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. Maintainability rather represents the efficiency of the implementation of a security mechanism that is aimed at making the system security design better (more secure, reliable, safe, etc).

### C. A limitation: The binary assumption for impairments

It must be noted that throughout this paper we have implicitly applied a binary model of our impairments. For example, we have assumed that the system is functioning or non-functioning, i.e., that there is a failure or there is no failure. Is is obvious that in many cases this is an over-simplification. In reality, the system will not fail completely, but only to a certain degree. It may continue to work, but with degraded service delivery or degraded performance. This aspect is encompassed by the attribute *performability.* See [34] and references therein.

There have been a few studies on behavioural metrics considering the degradation approach. In [12], a practical dependability metric for degradable computer systems with non-exponential degradation was proposed. The dependability attributes covered by this approach were: reliability, safety and performability. Markov modelling with phase-type assumption to enhance assessment of systems with non-exponential and time-dependent degradation was used. These types of studies have a good potential of being applied in behavioural security metrication.

We have also used the binary assumption on the input side in that we say that there is an intrusion or there is no intrusion. This assumption is also a significant simplification. We all know that intrusions are in many cases something that happens gradually, maybe starting with a session of port-scanning and continuing with increasing degrees of penetration. Thus, it may not be evident exactly when it happens. Further, an intrusion is not always a single event, but the combined effect of two or several events that cooperate.

## IV. IMPLICATIONS OF THE MODEL

### A. The causality perspective

A benefit of the model is that it clearly exhibits the causal chain of impairments, from attack to system failure. The attack is launched by a threat agent. If successful, there is an intrusion, which produces an unwanted system state, i.e., an error. There are three different outcomes of the system error. First, it may be immediately removed by some recovery mechanism. Second, it may be latent in the system for some time, before it propagates to the output. The latency time may be short. It may also last for very long time periods, e.g., many years, whether for operational reasons or because this was the intention of the attacker [1]. Third, the error may propagate through the system without any noticeable delay and directly cause a system failure.

The above reasoning shows how an attack may cause an error that propagates to cause a failure. On the other hand, it also shows that a successful attack may cause an error but that this error will not lead to a failure, i.e., it will not affect the system service. Therefore, insufficient integrity could lead to a behavioural failure, whether reflected in reduced reliability, availability, safety or confidentiality. Thus, the service delivered may be impaired by attacks on the system, but the relation between the attacks and the service is complicated and dependent on system internal factors among other things.

In another situation, the service delivered by the system may fail as a result of some (apparently) random error within the system, e.g., a component failure.

In summary, a system failure may be caused by an attack, but may also be due to some random event. Or,

 ISBN: 978-1-61208-298-1

taking the opposite view, a successful attack may or may not lead to a failure. If it leads to a failure, there may be considerable delay between the attack and the resulting failure.

### B. Three basic methods to avoid failures ("defence lines")

Considering the above causal relation between impairments, we can see that there are three basic ways to break the causal chain of unwanted events and to counter the propagation of impairments; see Figure 1. The basic causal chain is attack - error - failure. We observe that the attack, i.e., external fault, originates from the environmental threat. The error is the result of insufficient protection against the attack. Finally, the failure occurs since the error was permitted to propagate to the system output. The obvious conclusion is that defence methods could be applied accordingly. We name them ***threat reduction***, ***boundary protection*** and ***recovery***. Threat reduction methods focus on the threat. These methods aim to reduce or eliminate the threat, i.e., make it less probable that an attack is launched towards the system. An example of threat reduction would be legal measures. If the threat agent is a human attacker the prospect of facing a jail sentence would most probably decrease her motivation to launch attacks as compared to if the act was legal.

Boundary protection is the set of methods that protect the system from malicious external influence. An example would be authentication, which aims at refusing access for unauthorized entities.

Recovery methods aim at eliminating errors inside system boundaries before they produce a failure. For internal faults this is the only available defence methodology. An anti-virus tool is an obvious example of a recovery mechanism. A virus that has entered the system represents an error. It is well known that many viruses will not become visible to the USER until at some later occasion. If they can be found and deleted before they have caused a failure, a successful recovery has taken place.

In order to counter an attack, i.e., to avoid a system failure, only one of these methods needs to be effective. On the other hand careful security work requires that all three types of methods are used and are continuously active.

## V. SECURITY METRICS BASED ON THE SYSTEM MODEL

### A. Previous Research on Security Metrication

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 [27]. A generic concept for Information-Security *, denoted (IS)* was defined in the workshop to avoid confusion in terminology. IS* was intended to cover all different terms in the area, e.g., metric, measure, score, rating, rank, or assessment result. A significant outcome of the workshop was its proposal for the three main tracks for security metrication, i.e., *Technical, Organizational and Operational* metrics. Following this proposal, other researchers tried to add more categories with respect to various metrication applications, objectives and goals. Vaughn et al. [17] proposed two main categories for Information Assurance measurement: *Technical Target of Assessment* and *Organizational security*. From the Organizational perspective, NIST 800-26 [21] and Savola [3] proposed three main tracks for security metrication: *Technical, Operational* and *Management*. NIST 800-55 [19, 20] offered another categorization for metrication suggesting Implementation, Effectiveness and Efficiency as well as Business Impact as the main metrication categories. Other well-known security metrics approaches have been suggested by Savola [4], Pironti [7], CISWG [10] and NISTIR 7564 [22], ISO/IEC 27004 [26] and Payne [30], each of them for different systems and applications. There have not been many attempts to model-based security metrication. However, Savola [5] proposed a Security Metrics Objective Segment model, which is a taxonomy model including five levels for the main security metrics objective segments.

### B. Different Approaches to the Security Metrication Process

The process to find a metric for a concept such as security involves several steps. First, you must define the concept that you intend to metricate, i.e., you make a model of it. Second, you must decide which logical attributes of the model that could serve as carriers for the metric that you are interested of. Third, you must select a suitable method for assessing the "magnitude" of these attributes. Such a method could very often be based on some tangible feature of the system, such as a protection mechanism or a vulnerability. Finally, you must find a way to carry out the metrication in a practical way. Practical ways may involve data gathering, electrical measurement or inquiries.

The discussion in this paper mainly covers the two first steps above. However, for the integrity attribute we also have suggestion for the following steps.

### C. Metrication of Security and Dependability Based on Protective and Behavioural Attributes

In our approach, metrication is based on the attributes defined in the system model presented in section III. The attributes suitable for metrication are those defined according to the suggested two types of system-environment interaction, i.e., input from the environment and output to the environment. Thus, it should be possible to define ***protective metrics*** and ***behavioural metrics***, related to the system input and output respectively.

 ISBN: 978-1-61208-298-1

### D. Protective Security Metrics

#### 1) Protective security is integrity

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. According to our system model, it is the ***integrity*** attribute, that embodies ***(protective) security*** and in our opinion it is the integrity attribute that captures the essence of security.

#### 2) Protective metrics based on protection mechanisms

There may be several ways to measure the protective ability. One way could be based upon the strength of the (protective) security mechanisms of the system, under the assumption that the stronger the mechanisms are, the better the system is protected. In this situation, the measure would be based on the combined strength of all involved security mechanisms. For example, the ISO 27004 standard assesses the effectiveness of the implemented information security controls [26]. The problem with this approach is that the security (i.e., integrity) 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. However, it is a non-trivial task to find a method for such a combination of the effect of a number of protective mechanisms.

A similar approach is to base the metric on the three fundamental defence methods ("defence lines") described in IV.B: threat reduction, boundary protection and recovery. We realize that there are available mechanisms for the defence against intrusions for each of these methods and in this case the metric would assess the combined strength of the corresponding mechanisms.

#### 3) Using attacker effort as a protective security metric

Another way could be 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., compromise integrity). This idea was first proposed by Littlewood et al. [35] and their work has been extended in [16, 23, 36]. The idea is that an effort-based metric should be representative of all environment factors having effect on the attacker's ability 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.

#### 4) How to find an effort metric in practice

In the above section, we discussed which environmental parameters that an effort metric should reflect and in particular the attacker behaviour. However, it is probably infeasible to really measure all those parameters in practice. Instead we have to rely upon representative samples. An attempt to make a real measurement by performing supervised attack experiments was reported in [16, 28]. 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 (MTTI), or Mean Time To Compromise, 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 a single 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 could serve to make predictions of the security of other similar systems.

### E. Behavioural Security Metrics

As suggested by the model, the behavioural security attributes (or more accurately: security and dependability related attributes) 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.

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

***Availability*** 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].

***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*** quantifies the ability of the system to keep sensitive information confidential with respect to NON-USERs.

One of the approaches to confidentiality metrication is to derive behavioural measures from traditional reliability methods, such as Markov modelling. Jonsson et al. [13] proposed performance measures on user-specified service levels. They discussed that certain levels could be related to confidentiality degradation or confidentiality failures. Hence, Mean Time To Degradation was suggested both as a reliability metric (w.r.t the USERs) and a confidentiality metric (w.r.t. NON-USERs). We proposed a vectorized measure reflecting the status of the service levels defined for the system. Other approaches to confidentiality metrication are found in [38, 24].

 ISBN: 978-1-61208-298-1

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.

## VI. THE RELATION BETWEEN PROTECTIVE AND BEHAVIOURAL METRICS

### A. *Implication of the chain of impairments on behavioural metrics*

In "The causality perspective", Section (IV.A), we identified a causal chain of impairments from the attack phase to the system failure. In this section, we discuss the effect of the chain of impairments in security metrication.

We realize that the behavioural attributes of the system are dependent upon the environmental threats, protection mechanisms and the internal recovery mechanisms. The stronger a threat reduction mechanism is, the less becomes the threat towards the system and consequently the number and/or strength of potential attacks. Further, the better a boundary protection mechanism is, and the higher the integrity is, the lesser would the number of errors in the system be. Finally, the better a recovery mechanism is, the less probable is a system failure. As a conclusion, the behavioural attributes (and metrics), depend on 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. In conclusion, higher integrity will lead to higher reliability and the integrity metric will potentially affect the reliability metric as well as metrics for all other behavioural attributes.

### B. *Implications of latency on behavioural metrics*

In the preceding section, we noted that there is a coupling between protective and behavioural attributes (mechanisms, metrics). In this section, we will deal with the latency aspect. Error latency is the delay between the introduction of an error into the system, as a consequence of an intrusion, and the resulting failure. The latency is mainly a function of system operation and/or of recovery mechanisms. The latency may be short or long. In the case of infinite latency there will be no failure and the system behaviour will never be affected. Now, by applying the same reasoning as in the previous section we realize that latency will also affect behavioural attributes and metrics. The longer the error latency, the better is the system behaviour, i.e., the better the reliability, etc. The conclusion of this is that integrity "failures" are related to behavioural failures, but that there is no deterministic correspondence.

## VII. DISCUSSION

It is well known that security is a multi-faceted and complex concept. Further, there are several definitions of security, in the sense of which attributes should be included, on top of the traditional "CIA" ones. Some of these attributes may also be in contradiction to each other, for example integrity vs availability. Despite these facts many (if not most) authors suggest metrics for security without making a proper definition of it. We believe that the advantage of our approach is that it suggests a *model* of the integrated security-dependability meta-concept, in which it is split into a number of attributes. Our message is that metrication must focus on these attributes and that metrication of the meta-concept is not feasible or even possible. Thus, we have defined these attributes and the relation between them. There are several advantages with this approach: 1) It clarifies the relation between security "failures" and system (behvioural) failures. A security failure does not necessarily affect the service delivered. If it does indeed lead to a failure, this may take considerable time. 2) It becomes clear how preventive and protective actions, as well as recovery, may have beneficial consequences on the behavioural attributes. 3) The distinction between safety and security (integrity), which is sometimes an issue of controversy, becomes well defined. And in all of the three cases mentioned above there is an implication for the related metrics. For example, it clarifies why increased security leads to better safety. This is typically applicable for the "connected car", i.e., for virtually all modern cars. Another example, which shows that the model is very general can be taken from social sciences: by addressing problems with young people in metropolitan problem areas, we can mitigate criminality and its consequences many years later.

## VIII. CONCLUSION

We have described an approach for the meta-concept of security and dependability. The approach is based on a system model that re-groups its attributes into protective ("input") and behavioural ("output") ones. We have outlined how metrics could be defined in accordance: protective metrics and behavioural metrics. There are already some metrics for behavioural attributes, but less so for the protective attribute, integrity. We have argued that the integrity attribute captures the essence of security and could indeed serve as a definition of security, in a restricted sense. We have outlined two methods for metricating security and shown how behavioural metrics depend on security metrics.

## REFERENCES

[1] E. N. Adams, "Optimizing preventive service of software products", IBM Journal of Research and Development, vol. 28, no. 1, pp. 2-14, 1984.

[2] 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, pp. 11-33.

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

 ISBN: 978-1-61208-298-1

[4] R. Savola, “A novel security metrics taxonomy for R&D organisations”, ISSA 2008, July 2008, Johannesburg, South Africa, pp. 1-12.

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

[6] Common Criteria. ISO/IEC 15408-1, Information Technology - Security Techniques - Evaluation Criteria for IT Security, Part 1: Introduction and General Model, 1999.

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

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

[9] C. Irvine, T. Levin, “Toward a taxonomy and costing method for security services”, Computer Security Applications Conference, 1999. (ACSAC ’99) Proceedings. 15th Annual, 6-10 Dec. 1999, pp.183 – 188.

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

[11] Y. Asnar and P. Giorgini, “Uncertainty dimensions of risks in secure and dependable domain”, Technical Report # DISI-08-058, Univ. of Trento, 2008.

[12] E. Jonsson, M. Andersson, S. Asmussen, “A practical dependability measure for degradable computer systems with non-degradation”, Proc. IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS’94, Espoo, Finland, 1994, pp. 231-237.

[13] 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).

[14] 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), pp. 104-111.

[15] E. Jonsson, "Towards an integrated conceptual model of security and dependability," The First International Conference on Availability, Reliability and Security, (ARES 2006), 20-22 April 2006, pp. 8-16.

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

[17] 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 2003), Vol. 9. IEEE Computer Society, Washington, DC, USA, pp. 10-16.

[18] C. Meadows, “An outline of a taxonomy of computer security research and development”, New Security Paradigms Workshop, (NSPW 1993). ACM O-89791-635-2, pp. 33-35.

[19] 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.

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

[21] NIST 800-26, Swanson M., “Security Metrics Guide for Information Technology Systems”, National Institute of Standards and Technology Special Publication #800-26, November 2001.

[22] NISTIR 7564, W. Jansen, “Directions in security metrics research”, National Institute of Standards and Technology, April 2009.

[23] S. Brocklehurst, B. Littlewood, T. Olovsson and E. Jonsson, “On measurement of operational security”, Aerospace and Electronic Systems Magazine, IEEE, Vol. 9, Issue 10, Oct. 1994, pp. 7-16.

[24] L. Blasi, R. Savola, H. Abie and D. Rotondi, “Applicability of security metrics for adaptive security management in a universal banking hub system”, ECSA companion volume, August 23–26, 2010, Copenhagen, Denmark, pp. 197-204.

[25] S. Fenz and A. Ekelhart, “Formalizing information security knowledge”, ASIACCS’09, March 10-12, 2009, Sydney, NSW, Australia, pp. 183 – 194.

[26] ISO/IEC 27004:2009 Information technology — Security techniques — Information security management – Measurement.

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

[28] U. Gustafson and E. Jonsson, “Security Evaluation of a PC Network based on Intrusion Experiments”, Proc. 14th International l Congress on Computer and Communications Security, SECURICOM '96, Paris, France, pp. 187-203.

[29] A. Hecker, “On system security metrics and the definition approaches”, The Second International Conference on Emerging Security Information, Systems and Technologies, SECURWARE 2008, 25-31 Aug. 2008, pp. 412-419.

[30] S. C. Payne, “A guide to security metrics”, SANS Security Essentials.

[31] E. Jonsson and L. Pirzadeh, “A framework for security metrics based on operational system attributes”, International workshop on Security Measurements and Metrics (MetriSec 2011), Bannf, Alberta, Canada, 2011-09-21, pp. 58-65

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

[33] K.S. Trivedi, D. S. Kim, A. Roy and D. Meedhi, “Dependability and security models”, Proceedings of 7th International Workshop on the Design of Reliable Communication Networks (DRCN 2009), Washington, DC, October 2009, pp. 11-20.

[34] J. F. Meyer, “Performability: A retrospective and some pointers to the future”, Performance Evaluation, Vol. 14, No. 3-4, Elsevier, 1992, p. 139-156.

[35] B. Littlewood et al, “Towards operational measures of computer security”, Journal of Computer Security, Vol.2, 1993, pp.211-229.

[36] T. Olovsson, E. Jonsson, S. Brocklehurst, and B. Littlewood, “Towards operational measures of computer security: Experimentation and modelling”, Predictably Dependable Computing Systems, B. Randell et al., eds., ISBN 3-540-59334-9, Springer-Verlag, 1995, pp. 555-572.

[37] E. Jonsson, “An integrated framework for security and dependability”. Proceedings of the New Security Paradigms Workshop 1998, Charlottesville, VA, USA, September 22-25, 1998, pp. 22-29.

[38] R. Savola and H. Abie, ”Development of measurable security for a distributed messaging system”, International Journal on Advances in Security, vol. 2, no. 4, 2009, pp. 358-380.

[39] D. G. Firesmith, “Common Concepts Underlying Safety, Security, and Survivability Engineering”, CMU/SEI-2003-TN-033, Carnegie-Mellon University, Pittsburg, USA.

 ISBN: 978-1-61208-298-1