An Integrated Framework for Security and Dependability

Erland Jonsson
Department of Computer Engineering
Chalmers University of Technology
SE-412 96 Göteborg, SWEDEN
+46 31 772 1698
email: erland.jonsson@ce.chalmers.se

1. ABSTRACT

This paper deals with the problem of interpreting security and dependability in such a way that they can be incorporated into the same framework. This calls for a modified understanding of some of the traditional concepts. Thus, a system-related conceptual model is suggested in which the various aspects of security and dependability are analyzed and regrouped into a new "input-output"-related system model. The input characteristics of this new model are interpreted in *preventive* terms, whereas the output characteristics are interpreted in *behavioural* terms with respect to the *user* of the system. One of the benefits of the model is that it can form a basis for composite measures of security and dependability. Thus, it is possible to define *preventive measures* and *behavioural measures*. The behavioural measures are measures that relate to the behaviour of the system, or, put informally, relate to the "output" of the system. Behavioural measures deal with *system failures*, e.g., the probability for and magnitude of such failures. Well-known reliability methods, such as Markov modelling, can be used for deriving behavioural measures of security. A preventive measure, on the other hand, would describe the system's ability to avoid detrimental influence from the environment, in particular influence originating from security breaches into the system.

1.1 Keywords

Computer Security, Dependability, Concepts, Modelling, Confidentiality, Measure.

2. INTRODUCTION

Informally, we want for our computer systems to "work as intended" or "to function correctly". This means that they should be secure and dependable (including reliable, available, etc.) at the same time. Historically, the two research fields of security and dependability have evolved separately. In short, security has emerged from the viewpoint of intentional and hostile interaction with a system, an interaction that would lead to unauthorized disclosure or modification of information. Dependability has evolved from reliability and availability considerations. Security and dependability have traditionally been treated separately. Lately, however, attempts have been made to integrate these two, e.g., as suggested in [33], where dependability is defined as the overall concept of which security is simply one attribute among others or in [12], who is taking the opposite approach. The consequences of this proposed integration have not yet been fully realized. This paper brings this work one step further. It presents an integrated framework for security and dependability, that covers most aspects of "required functionality" as experienced by the user. It also outlines how the framework could be used for composite measures.

Section 3 of this paper gives a note on terminology and section 4 gives the present status of the disciplines of security and dependability. There are many different opinions as to the status of discussion of concepts and terminology used. The versions given below are believed to have widespread acceptance. Dependability is given in its "classical" form, with the traditional way of integrating security. Security is described by its different aspects and some alternatives are mentioned. In section 5 a novel conceptual framework and system model is suggested. Section 6 gives a survey of existing measures for security/dependability and outlines how novel measures could be defined based on the system model. Section 7 summarizes the paper.

3. A NOTE ON TERMINOLOGY

We urge the reader of this paper to *forget about his/her present understanding of the words* used in this area! Otherwise he/she will most probably not understand this paper. The reason for this is the following:

The work presented in this paper is about new concepts, and

it also uses old concepts in a new way. In general, new concepts call for the invention of new terms or re-definition of old terms, since it is essential that the concepts can be properly addressed and understood. It would be expected that the person who suggests a new conceptual framework would also suggest a corresponding terminology, and that he clarifies the relations with the established usage of the terms. It has not been possible to do so at this time. Still, please note the words in the paper may be used with a meaning that differs from normal usage. Unfortunately, the same word may also be used in its "normal" sense. We hope that it should be clear from the context which interpretation is correct.

Therefore, we do not wish to strongly defend any part of the *terminology* in this paper. The underlying *concepts*, on the other hand, have our full support, and we believe that once these concepts become commonly accepted, the issue of proper terminology will find its solution.

4. PRESENT STATUS

4.1 Dependability vs security

Dependability was first introduced as a generic term encompassing concepts such as *reliability, availability, maintainability* and *safety*, as well as related measures. It was defined in terms of "task accomplishment" and "provision of expected service" [32]. A number of versions of this original definition has since been published. Finally, as a result of several years of work in IFIP Working Group 10.4, a comprehensive summary of dependability concepts and terminology was presented [33]. Here, the attributes of dependability were defined as *reliability, availability, safety* and *security* (figure 1).

Thus, security is treated as an attribute of dependability,

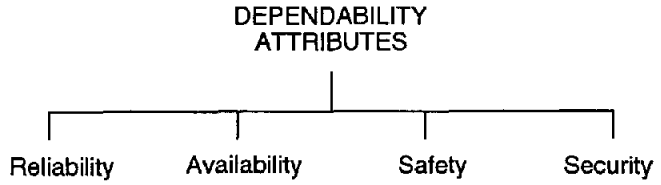

Figure 1: Dependability and its attributes

among others. Except for security, these attributes all refer to the system behaviour, i.e. the service that the system delivers to the environment. Therefore, they form an adequate basis for a behavioural approach. For security, however, the situation is different: It is normally defined by three different aspects: *confidentiality, integrity* and *availability* [46], [21]. See figure 2.

Therefore, security concept describes not only the system behaviour, i.e. the service that the system delivers to the environment (e.g. availability), but also the system's ability to resist external attacks (e.g. integrity).

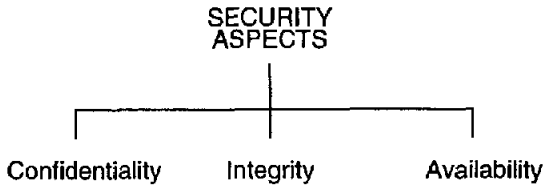

Figure 2: Security and its aspects

4.2 Generalized concepts

It is interesting to note that, as early as in 1978, [37] suggested the term system *defensiveness* as a generalized notion of security, to imply security, reliability, availability and auditability. However, the author does not really elaborate his extended notion in his analysis of operating systems. He also discusses in terms of *preventive* approaches as opposed to *remedial* ones. Here, preventive refers to measures taken during the design phase to attain a secure design by means of e.g. specific design methodologies and formal specifications, whereas the remedial involves the assessment of security when the system is in operation, followed by attempts to patch around vulnerabilities that might be uncovered. Therefore, his viewpoint is temporal with respect to the design phase.

In [15] the concept of *trustworthiness* is suggested as an extension of dependability, giving a judgement of the acceptability of the system rather than being a property of the system. This concept is especially appropriate for large and complex systems with rich human interaction for which the specifications are likely to be incomplete, ambiguous or inconsistent.

The problem of ensuring *secure fault-tolerance*, i.e., improved reliability (by fault-tolerance) and a preserved security policy at the same time, is discussed by [28]. The author points out the danger that fault-tolerance mechanisms can undermine the security of a system, and discusses possible solutions to this problem. One such technique is the so-called FRS (Fragmentation-Redundancy-Scattering) technique [10], which can be employed to achieve *intrusion-tolerance* [14].

A generalized view of the ideas underlying the "Orange Book" [46] is presented in [45]. The paper refers to the general problem of drawing a boundary between security and other critical requirements, and argues that ensuring maximum confidentiality, integrity and availability (called "assured service") does not address the problem of ensuring security satisfactorily. It proposes a solution based on three different security policy concepts, whereby he establishes a more precise view of security. He also notes that many integrity and availability requirements can not be directly

addressed by security policies and are more properly treated as requirements of a different nature, which are thoughts that are very much in line with those proposed in this paper.

The relation between security and safety is specifically discussed in [6]. The authors analyse several examples in which both safety and security are of concern. The terms *safety critical* and *security critical* are defined and are used to encompass *absolute* and *relative* harm, respectively. A simple formal definition of the concepts is also given. It is noted that some of the ideas, and especially the concept of "causal indirection" for security, agree with those presented in this paper.

Finally, we want to point out that there are striking similarities between the dependability concept discussed and the concept of *quality* as proposed by [29]. To him, quality means "fitness for use" and includes product satisfaction and freedom from deficiencies. The parameters of "fitness for use" include availability, reliability and maintainability.

4.3 Security concepts

Various versions of the established definition of security presented in paragraph 4.1 exist. For example, in some cases one or two extra aspects are added, such as *denial-of-service* and *authenticity*. In other cases, a different grouping is preferred, see e.g. [20], [36].

In database systems, *integrity* refers to the validity and consistency of data as defined by some integrity constraints, thus primarily actions taken by an *authorized* party, whereas *security* refers to protection of data against *unauthorized* disclosure, alternation and destruction [11]. However, the "traditional" definition is also used in parallel, see e.g., [7].

There also exists a wide range of *formal models*. Among the most important of these we find [3], who introduced a formal model for confidentiality, i.e., a description of information flow in a secure system, aimed at identifying paths that could lead to inappropriate disclosure of information. A corresponding model for integrity was suggested by [4]. A formal system of protection rules based on an access control matrix was introduced by [30] and [17]. The matrix is used to define the *rights R* of a *subject S* with respect to an *object O*. A very good overview and classification of formal models is presented in [31].

There is also the "Orange Book" security concept as described in the Trusted Computer System Evaluation Criteria [46], which primarily deals with confidentiality aspects. It was originally developed for military purposes as a result of the *DoD Computer Security Initiative* launched in 1978, with the intention to match the security policy of the United States Department of Defence. The security policy is understood as a set of laws, rules and practices that regulates how an organization manages, protects and distributes sensitive information. However, it has also been widely used for commercial operating systems. Based on the development procedure and the presence (or absence) of security mechanisms and methods, a protection level is evaluated and the system is classified into one of seven classes. A similar but more general criteria, which permits selection of arbitrary security functions, has been developed in Europe: the Information Technology Security Evaluation Criteria [21]. Still other alternatives exist in other counties [8], [22]. In a first attempt to achieve an international harmonization, the United States and Canada commonly proposed the "Federal Criteria" [16], which was never published in a final version. The present work is concentrated on the "Common Criteria", with the express intention of reaching an international standard.

5. THE SUGGESTED CONCEPTUAL FRAMEWORK

5.1 Interpreting the security attribute

We shall now detail how the three security aspects (confidentiality, integrity and availability) can be interpreted in behavioural and preventive terms. See figure 3, which describes the situation for information security.

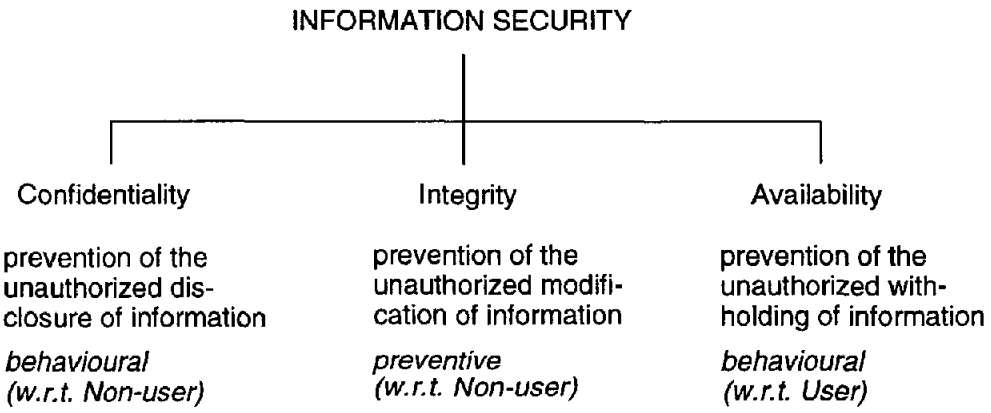

Figure 3: Information security and its aspects

Availability is primarily defined as the ability of the system to deliver its service to the authorized user. It is thus a behavioural concept. The authorized users are the users that are the intended receivers of the service that the system delivers, as specified in the system specification. In the following we shall call the authorized user(s) the **User**. This may be a human or an object: a person, a computer, a program etc. We have chosen to regard all potential users except the authorized users as unauthorized users. Unauthorized users are called **Non-users**. Therefore, availability as a security aspect has the same meaning as the availability attribute of dependability.

Integrity is the prevention of unauthorized modification or the deletion or destruction of system assets. Integrity is violated by means of an attack, which is normally performed by a Non-user, but may also be performed by a User who is abusing his/her authority. Thus, integrity is a preventive quality of a system and characterizes the system's ability to withstand attacks.

Confidentiality is the ability of the system to deny the Non-user access to confidential information. It is thus a behavioural concept but, unlike other attributes, it defines system behaviour *with respect to a Non-user*. It actually defines to what extent information should be accessible, or rather not accessible, to Non-users. Therefore, confidentiality is behavioural concept, parallel to reliability, availability and safety. Confidentiality can also be understood in a broader sense, i.e., the prevention of the delivery of service to the Non-user, even if this service delivery would not include harm to the User or disclosure of secret information. The term *exclusivity* has been proposed for this broader concept [13].

The conclusion of the discussion above leads to a modified understanding of security as two concepts: preventive security and behavioural security[1]. **Preventive security** is simply regarded as a form of fault prevention, namely fault prevention with respect to intentional faults and attacks. **Behavioural security** is an integrated part of (the traditional "behavioural") dependability and can not readily be distinguished from it.

In view of this discussion, we arrive at two generic types of behavioural attributes: *reliability/availability* and *confidentiality*. See figure 4.

Confidentiality relates to the denial-of-service to Non-users, i.e. unauthorized users shall not be able to obtain information from the system, nor be able to use it in any other way. Reliability and availability have been merged, since they both refer to delivery-of-service to the User. This does not mean that they are the same. They are merged as they both reflect delivery-of-service to the authorized user, even if different aspects of this delivery. The *safety* attribute characterizes a certain failure mode of the system: it denotes the non-occurrence of catastrophic failures. Note that failures can be of both a "reliability" type, i.e., related to the User, as well as a "confidentiality" type, i.e., related to the Non-user.

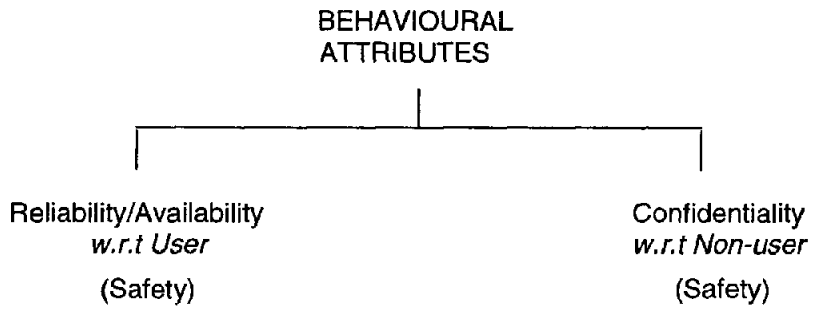

Figure 4: Behavioural dependability attributes

5.2 The System Model

The discussion above can be summarized into the following system model. The total system that we consider consists of the *object system* and the *environment*. In general, there are two basic types of interaction between the system and its environment, see figure 5

First, the system interacts with the environment or is *delivering an output or service* to the environment. We call this the system behaviour. There is also an environmental influence on the system, which means that the system *receives an input* from the environment. The input consists of many different types of interaction. The type of interaction we are interested in here is that which involves a *fault introduction* into the system, in particular intentional, and often malicious faults, i.e., *security breaches*. 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 encompasses the preventive aspect of security/dependability.

There are two different types of receivers of the output delivered by the system: the User and the Non-user. The desired (and preferably specified) delivery-of-service to the User can be described by the behavioural attributes reliability, availability and safety. Less often specified, but still desired, is that

[1] Here, we could just as well have used the terms preventive dependability and behavioural dependability, since we have merged these two concepts and split them in a new way. Another alternative would be to call the preventive aspects "security" and the behavioural "dependability"

the system shall have an ability to *deny service* to the Non-user. This is described by the behavioural attributes confidentiality (for information delivery) and exclusivity (for use) as well as safety.

5.3 An example: A Trojan Horse

One of the benefits of this model is that it clarifies the relation between traditional security/integrity and reliability. In general, it treats preventive and behavioural characteristics separately and gives a clue for a better understanding of the relation between them. Let's take an example, that is normally regarded as hard to model: a Trojan Horse.

The introduction of a Trojan Horse into the system constitutes a failure of the preventive characteristics ("integrity failure", "security failure" or simply "intrusion"). When the Horse is in the system the system is "incorrect". However, the Horse may remain latent for ever, and may thus never lead to a failure of the behavioural characteristics, e.g., a reliability failure or a confidentiality failure. Thus, the preventive characteristics have been impaired, but not the behavioural. The user would never notice the "incorrectness" if he/she did not actively search for it.

On the other hand, the Horse may be activated after some time, e.g., leading to a disruption of service to the user. In this case, the "security failure" has propagated and caused a "reliability failure". The coupling between these two is normally complicated, depending on the operation of the system etc.

We also realize that the very same "disruption of service to the user" that was caused by the Horse could have been the result of e.g., some (apparently spontaneous) hardware or software failure in the system. This clearly shows that input and output characteristics may or may not be related to each other. It also shows that the preventive and behavioural characteristics are only partly coupled to each other, and that the coupling seems to be complicated.

6. MEASURES OF SECURITY

This section presents some existing approaches to measuring security and composite security/dependability concepts. Commonly accepted and used reliability or availability measures, such as Mean Time To Failure or probability of a successful mission etc., are not covered. Finally, it is outlined how measures based on the suggested system model could be derived.

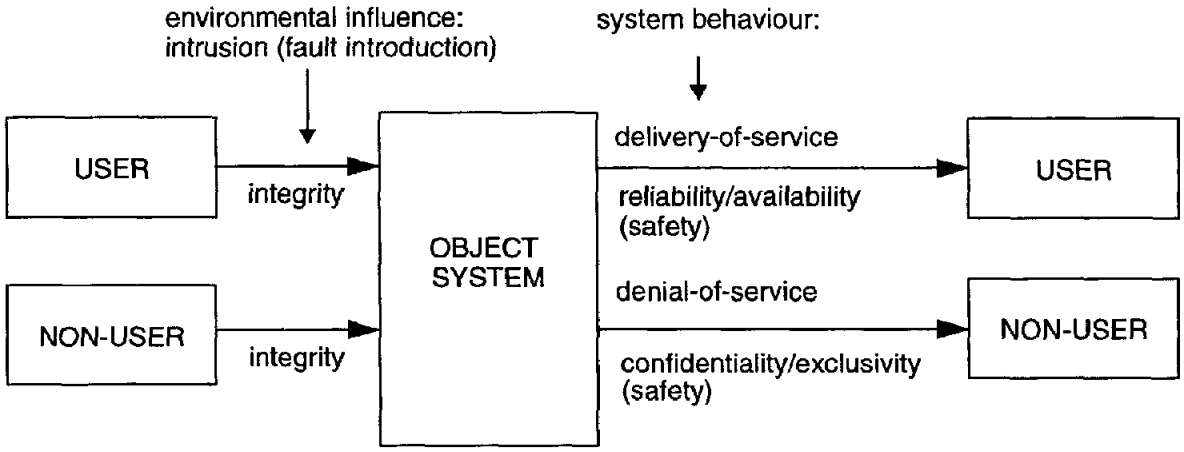

Figure 5: The system model

6.1 Existing measures of security

Today, the common way to "measure" security is to use the classes or rankings of the Orange Book or other evaluation criteria [46], [21]. These classes primarily reflect static design properties of the system and do not incorporate the uncertainty and dependence of the operational environment in a probabilistic way, similar to the way in which reliability is commonly expressed. These issues are discussed in the following.

To our knowledge, there are not many other practical measures, and the ones that are indeed suggested are focused mainly on intrusions and vulnerabilities. A "Security Computation Index" (SCI) was proposed by [44]. This index is calculated by means of using Markov chains and its aim is to quantify the total security aspect of an intrusion-tolerant system. However, the rationale for using Markov modelling is not discussed and the breaches are considered to be exponentially distributed, which in general is not true.

The concept of "intrusion coverage" is introduced to denote the effectiveness of the intrusion-detection mechanisms. However, a higher intrusion coverage does not necessarily lead to a higher Security Computation Index, which defies the intuitive expectations of such an index.

Another similar index, the "Security Vulnerability Index" (SVI), was proposed by [1]. The index is derived by evaluating a number of factors from three areas. The factors are such that the presence (or absence) of them is likely to influence the overall vulnerability of the system. In this way, an SVI between 0 and 1 is calculated. There are several problems with this approach. The main objection is that it may not be possible to make estimates of the influence of the initial factors. In general, neither all "physical vulnerabilities" nor all "unpatched OS bugs" are known, and can therefore not be estimated, let alone quantified. The quantification of "potentially malevolent acts" seems even more difficult. Finally, it is not evident how an index of a certain level should be interpreted, and the authors end by merging the levels into four different classes: "low", "moderate", "high" and "extremely high". It seems plausible that such a classification could more easily be attained by means of a purely subjective estimation of the system features.

A completely different approach is taken in [9]. The author suggests a method for quantitative evaluation of operational security based on a new concept called "privilege graph". This concept is an extension and elaboration of Stochastic Petri Nets and the Typed Access Matrix Model proposed by [43].

6.2 Existing composite measures

An alternative measure for dependability including security was suggested by [35]. He started with a view of dependability in which loss and risk are the unifying concepts for its definition. This definition permits a context-sensitive assessment of dependability, reflecting different perceptions of risk exposure. Furthermore, risk and loss (per unit time) are suggested as measures of dependability. Risk can be used in early design phases to handle the inherent uncertainty of the design, i.e., the fact that we have incomplete knowledge of the final system realization. Thus, conventional risk-analysis techniques can be employed. A loss-based measure is more appropriate during the operational phase. The advantage of such a measure is that it can readily be translated into economic terms.

Finally, there is a large class of papers that claim to address the problem of measuring dependability, but in which only two or three dependability aspects are addressed. In these, dependability is used in a more limited sense. Typically, the security aspect is totally neglected. Thus, in [19], reliability and availability are considered together with a new concept called "task completion" and, in [2], only reliability and safety are evaluated. A further example is found in [42]. Here, successive operational periods modelled by Markov processes are used as a measure of dependability. The whole analysis is based on the fact that there are three types of states: *up* (i.e., operational), *down* (i.e. recoverable failure) and *completely down* (i.e., non-recoverable failure). It is interesting to note that there is a certain resemblance with the behavioural modelling in this paper. However, the derived measure is rather a combined reliability-availability measure than one that would also reflect security and safety.

6.3 Measures of behavioural and preventive security

The conceptual framework presented in paragraph 5.2 suggests a way to integrate security-related and dependability-related aspects in such a way that the difference between detrimental influence on the system and failed system performance is clarified. Thus, there are attributes that describe the system's ability to avoid harmful impact from the environment, termed *preventive* attributes, and those describing the system's ability to fulfil its expected function, *behavioural* attributes.

In consequence, the measures defined for a system could be divided in a similar way into preventive and behavioural measures. It was shown that the confidentiality aspect of security can be incorporated into a behavioural measure once the distinction between delivery-of-service to the authorized user and denial-of-service to the non-authorized user is made, and that traditional reliability modelling techniques can be used to derive a **behavioural measure** [25], [26].

A **preventive measure** reflects the system's ability to prevent intrusions or any other detrimental impact on the system. Preventive measures are much less developed than behavioural ones. However, there has been some attempts to model the preventive attribute using the intrusion process. The rationale for this is that the system's protective ability should be correlated to the difficulty of succeeding with an attack, i.e., making an intrusion. A possible way to achieve this is to perform attacking campaigns, during which intruders are encouraged to attack a system, while as much relevant data as possible on the intrusion process are collected [5], [18], [27], [41].

It should also be noted that there is one remaining characteristic of a system, for which it could be interesting to make a quantitative assessment, namely the *correctness* of the system. We are not aware of any attempts to measure this aspect of a system, even if, in principle, this should not be impossible. Such a measure should be especially applicable to data base systems.

Finally, we want to point out that these three measures clearly are not independent of each other, even if they reflect different aspects of a system. Rather, a reduction in the preventive ability will normally, but not necessarily, result in the system being incorrect. Furthermore, an incorrectness would often, but not always, lead to an impaired behaviour.

7. SUMMARY

A novel approach to the integration of security and dependability has been proposed. It is based on the observation that a computer system could be described in behavioural and preventive terms. A behavioural viewpoint is related to the behaviour of the system, i.e. to how the system influences its environment, normally reflected by the reliability and availability aspects. A preventive viewpoint describes how to prevent unwanted environmental influence on the system. Using this approach, we have shown how the aspects of traditional security could be integrated with existing dependability concepts and interpreted as preventive or behavioural characteristics.

Confidentiality is different from the other behavioural aspects in that it describes the system's relation to an *unauthorized* user rather than to the authorized user. Safety is interpreted as a "sub-attribute" describing a special subset of (behavioural) failures, denoting the system's ability to avoid catastrophic consequences. Integrity is understood as a concept for fault prevention with respect to intentional external faults or attacks against the system. Finally, it was outlined how these novel concepts could be assessed quantitatively, i.e. measured.

8. REFERENCES

[1] J. Alves-Foss, S. Barbosa, "Assessing Computer Security Vulnerability", Operating Systems Review, Vol. 29, No. 3, July 1995. pp. 3-13.

[2] J. Arlat, K. Kanoun, J-C. Laprie, "Dependability Modeling and Evaluation of Software Fault-tolerant Systems" in *IEEE Transactions on Computers,* Vol. 39, No. 4, April 1990. pp. 504-513.

[3] D. Bell, L. LaPadula, "Secure Computer Systems: Mathematical Foundations and Model", MITRE Report MTR 2547, Vol. 2, Nov. 1973.

[4] K. J. Biba, "Integrity Considerations for Secure Computer Systems", Technical Report No. ESD-TR-76-372, Electronic Systems Division, US Air Force, Hanscom Field, Bedford, MA, 1977.

[5] S. Brocklehurst, B. Littlewood, T. Olovsson, E. Jonsson: *"On Measurement of Operational Security"*, in Proceedings of the Ninth Annual IEEE Conference on Computer Assurance, COMPASS'94, Gaithersburg, Maryland, USA, June 29-July 1, pp. 257-266. 1994.

[6] A. Burns, J. McDermid, J. Dobson, On the Meaning of Safety and Security, The Computer Journal, Vol. 35, No. 1, 1992. pp. 3-15.

[7] S. Castano, M. G. Fugini, G. Martella, P. Samarati, "Database Security", Addison-Wesley, 1995. ISBN 0-201-59375-0.

[8] Canadian Trusted Computer Product Evaluation Criteria, Version 3.0e, Canadian System Security center, Communications Security Establishment Government of Canada, 1993.

[9] M. Dacier: *Vers une evaluation quantitative de la securite informatique,* Doctoral thesis, LAAS Report No 94488, LAAS/CNRS, Toulouse, December 1994. (In French).

[10] J. da Silva Fraga, D. Powell, "A Fault- and Intrusion-Tolerant File System", Proc. of the 3rd International Conference on Computer Security, IFIP/SEC '85, Dublin, Ireland, Aug. 1985. pp. 203-218.

[11] C. J. Date, "An Introduction to Database Systems", Vol. 1, 5th edition, pp. 429ff, Addison-Wesley 1990, ISBN 0-201-51381-1.

[12] D. E. Denning: "Secure Databases and Safety: Some unexpected conflicts," pp. 101-111 in T. Anderson (editor): *Safe & Secure Computing Systems,* Blackwell Scientific Publications, ISBN 0-632-01819-4, 1989.

[13] D. E. Denning, "A New Paradigm for Trusted Systems", Proceedings of the IEEE New Paradigms Workshop, pp. 36-41. 1993.

[14] Y. Deswarte, L. Blain, J-C. Fabre, "Intrusion Tolerance in Distributed Computer Systems", IEEE Symposium on Security and Privacy, IEEE Computer Society Press, 1991. pp. 110-121.

[15] J. Dobson, J. McDermid, B. Randell: "On the Trustworthiness of Computer Systems", ESPRIT/BRA Project 3092 Technical Report Series No. 14, 1990.

[16] Federal Criteria for Information Security Technology, Draft, National Institute of Standards and technology (NIST) and National Security Agency (NSA), 1992.

[17] G. Graham, P. Denning, "Protection - Principles and Practice", Proc. 1972 AFIPS Spring Joint Computer Conference, AFIPS Press. pp. 417-429.

[18] U. Gustafson, E. Jonsson, T. Olovsson: *"On the Modelling of Preventive Security Based on a PC Network Intrusion Experiment"*. Proceedings of the Australasian Conference on Information Security and Privacy, ACISP'96, Wollongong, Australia, June 24-26, 1996.

[19] D. Heimann, N. Mittal, K. Trivedi, "Dependability Modeling for Computer Systems" in *Proc. of the Annual Reliability and Maintainability Symposium,* 1991. pp. 120-127.

[20] International Standards Organization: *Information Processing Systems - Open Systems Interconnection - Basic Reference Model, part 2: Security Architecture 7498/2.*

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

[22] Japanese Computer Security Evaluation Criteria - Functionality Requirements, Draft version 1.0, Ministry of International Trade and Industry (MITI), 1992.

[23] E. Jonsson, T. Olovsson, "On the Integration of Security and Dependability in Computer Systems", IASTED International Conference on Reliability, Quality Control and Risk Assessment, Washington, Nov. 4-6, 1992. ISBN 0-88986-171-4, pp. 93-97.

[24] E. Jonsson, "A Unified Approach to Dependability Impairments in Computer Systems", IASTED International Conference on Reliability, Quality Control and Risk Assessment, Cambridge, MA, Oct. 18-20 1993, ISBN 0-88986-181-1, pp. 173-178.

[25] E. Jonsson, M. Andersson, S. Asmussen, "A Practical Dependability Measure for Degradable Computer Systems with Non-exponential Degradation", Proceedings of the IFAC Symposium on Fault Detection, Supervision and Safety for Technical Processes, SAFEPROCESS'94, Espoo, Finland, vol. 2, June 13-15, 1994. pp. 227-233.

[26] E. Jonsson, M. Andersson, "On the Quantitative Assessment of Behavioural Security". Proc. of the First Australasian Conference on Information Security and Privacy, ACISP'96, 24-26 june 1996, Wollongong, Australia. In Lecture Notes in Computer Science 1172, Springer-Verlag 1996. ISBN 3-540-61991-7. pp. 228-241.

[27] 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, April 1997.

[28] M.K. Joseph: "Integration Problems in Fault-Tolerant, Secure Computer Design," pp. 347-364 in A.Avizienis. J.C. Laprie (editors): *Dependable Computing for Critical Applications,* Springer-Verlag, N.Y., ISBN 3-211-82249-6, 1991.

[29] J. M. Juran, "Juran's Quality Control Handbook" 4th ed., McGraw-Hill, N.Y., 1988. ISBN 0-07-033176-6. pp. 2.8ff.

[30] B. Lampson, "Protection", Proc. 5th Princeton Symposium in Operating Systems Review, Vol. 8, No. 1, Nov. 1974. pp. 18.24.

[31] C. E. Landwehr, "Formal Models for Computer Security", ACM Computing Surveys, Vol. 13, No. 3, 1981. pp. 247-278.

[32] J. C. Laprie, A. Costes: "Dependability: A unifying concept for reliable computing", in *Proc. 12th IEEE International Symposium on Fault-Tolerant Computing (FTCS-12),* June 1982, pp 18-21.

[33] J. C. Laprie et al.: *Dependability: Basic Concepts and Terminology,* Springer-Verlag, ISBN 3-211-82296-8, 1992.

[34] B. Littlewood, S. Brocklehurst, N.E. Fenton, P. Mellor, S. Page, D. Wright, J.E. Dobson, J.A. McDermid and D. Gollmann, "Towards Operational Measures of Computer Security", Journal of Computer Security, vol. 2, no. 3. 1994.

[35] J. McDermid, "On Dependability, Its Measurement and Its Management", in *High Integrity Systems,* Vol. 1, No. 1, 1994, Oxford University Press, pp. 17-26.

[36] S. Muftic: *Security Mechanisms for Computer Networks,* Ellis Horwood Ltd, England, ISBN 0-7458-0613-9, 1989.

[37] Peter G Neumann: "Computer system security evaluation", in 1978 National Computer Conference, AFIPS Conf. Proceedings 47, Arlington, VA, pp 1087-1095.

[38] National Institute of Standards and Technology: Glossary of Computer Security Terms, *NSC-TG-004 version. 1,* ("Aqua Book"), Oct. 21, 1988.

[39] G. J. Myers: The Art of Software Testing, John Wiley & Sons, Inc, ISBN 0-471-04328-1, 1979.

[40] T. Olovsson, E. Jonsson, S. Brocklehurst, B. Littlewood: "Data Collection for Security Fault Forecasting: Pilot Experiment", Technical Report No 167, Department of Computer Engineering, Chalmers University of Technology, 1992 and ESPRIT/BRA Project No 6362 (PDCS2) First Year Report, Toulouse Sept. 1993, pp 515-540.

[41] T. Olovsson, E. Jonsson, S. Brocklehurst, B. Littlewood: "Towards Operational Measures of Computer Security: Experimentation and Modelling", Technical Report No 236, Department of Computer Engineering, Chalmers University of Technology, 1995 and in B. Randell et al. (editors.): *Predictably Dependable Computing Systems*, ESPRIT Basic Research Series, Springer Verlag, 1995, ISBN 3-540-59334-9, pp 555-572.

[42] G. Rubino, B. Sericola, "Successive Operational Periods as Measures of Dependability" in Dependable Computing for Critical Applications (editors A. Avizieniz et al.), Springer Verlag, ISBN 3-211-82249-6, 1991, pp. 239-254.

[43] R. S. Sandhu: "The Typed Access Matrix Model", *IEEE Symposium on Security & Privacy,* 1992, pp. 122-136.

[44] B. C. Soh, T. S. Dillon," System Intrusion Detection: Model, Design and Analysis", Pacific Rim International Symposium on Fault-Tolerant Computing, Dec. 16-17, 1993, (PRFTS'93), Melbourne, Australia, CRT Publishing Ltd, London. pp. 85-90.

[45] D.F. Sterne, "On the Buzzword Security Policy", *IEEE Symposium on Security & Privacy,* 1991, pp. 219 - 230.

[46] *Trusted Computer System Evaluation Criteria* ("orange book"), National Computer Security Center, Department of Defense, No DOD 5200.28.STD, 1985.