[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*, 1(1):11-33, Jan-March 2004. [bib | DOI]

This paper gives the main definitions relating to dependability, a generic concept including a special case of such attributes as reliability, availability, safety, integrity, maintainability, etc. Security brings in concerns for confidentiality, in addition to availability and integrity. Basic definitions are given first. They are then commented upon, and supplemented by additional definitions, which address the threats to dependability and security (faults, errors, failures), their attributes, and the means for their achievement (fault prevention, fault tolerance, fault removal, fault forecasting). The aim is to explicate a set of general concepts, of relevance across a wide range of situations and, therefore, helping communication and cooperation among a number of scientific and technical communities, including ones that are concentrating on particular types of system, of system failures, or of causes of system failures.

Keywords: data privacy, fault tolerant computing, security of data, software reliability, system recovery dependable computing, fault forecasting, fault prevention, fault removal, fault tolerance, secure computing, system attacks, system availability, system failures, system integrity, system maintainability, system reliability, system safety, system security, system vulnerabilities, taxonomy

[2] A. Bond and N. Pahlsson. A quantitative evaluation framework for component security in distributed information systems. Undergraduate thesis y-level (information theory), Linkoping University, Department of Electrical Engineering, 2004. [bib | http]

The Heimdal Framework presented in this thesis is a step towards an unambiguous framework that reveals the objective strength and weaknesses of the security of components. It provides a way to combine different aspects affecting the security of components - such as category requirements, implemented security functionality and the environment in which it operates - in a modular way, making each module replaceable in the event that a more accurate module is developed.

The environment is assessed and quantified through a methodology presented as a part of the Heimdal Framework. The result of the evaluation is quantitative data, which can be presented with varying degrees of detail, reflecting the needs of the evaluator.

The framework is flexible and divides the problem space into smaller, more accomplishable subtasks with the means to focus on specific problems, aspects or system scopes. The evaluation method is focusing on technological components and is based on, but not limited to, the Security Functional Requirements (SFR) of the Common Criteria.

Keywords: Quantitative, Security Evaluation, Threat Assessment, Distributed Information Systems, Common Criteria, Evaluation Framework, Component Security

[3] L. T. Heberlein, G. V. Dias, K. N. Levitt, B. Mukherjee, J. Wood, and D. Wolber. A network security monitor. In *IEEE Symposium on Security and Privacy*, pages 296-304, May 1990. [bib | DOI]

The study of security in computer networks is a rapidly growing area of interest because of the proliferation of networks and the paucity of security measures in most current networks. Since most networks consist of a collection of inter-connected local area networks (LANs), this paper concentrates on the security-related issues in a single broadcast LAN such as Ethernet. We formalize various possible network attacks. Our basic strategy is to develop profiles of usage of network resources and then compare current usage patterns with the historical profile to determine possible security violations. Thus, our work is similar to the host-based intrusion-detection systems such as SRI's IDES [9]. Different from such systems, however, is our use of a hierarchical model to refine the focus of the intrusion-detection mechanism. We also report on the development of our experimental LAN monitor currently under implementation. Several network attacks have been simulated and results on how the monitor has been able to detect these attacks are also analyzed. Initial results demonstrate that many network attacks are detectable with our monitor, although it can surely be defeated. Current work is focusing on the integration of network monitoring with host-based techniques.

Keywords: local area networks, security of dataEthernet, hierarchical model, host-based intrusion-

detection systems, local area network, network resources, network security monitor, single broadcast LAN

[4] E. Jonsson and T. Olovsson. A quantitative model of the security intrusion process based on attacker behavior. *IEEE Transactions on Software Engineering*, 23(4):235-245, April 1997. [bib | DOI]

This paper is based on a conceptual framework in which security can be split into two generic types of characteristics, behavioral and preventive. Here, preventive security denotes the system's ability to protect itself from external attacks. One way to describe the preventive security of a system is in terms of its interaction with the alleged attacker, i.e., by describing the intrusion process. To our knowledge, very little is done to model this process in quantitative terms. Therefore, based on empirical data collected from intrusion experiments, we have worked out a hypothesis on typical attacker behavior. The hypothesis suggests that the attacking process can be split into three phases: the learning phase, the standard attack phase, and the innovative attack phase. The probability for successful attacks during the learning and innovative phases is expected to be small, although for different reasons. During the standard attack phase it is expected to be considerably higher. The collected data indicates that the breaches during the standard attack phase are statistically equivalent and that the times between breaches are exponentially distributed. This would actually imply that traditional methods for reliability modeling could be applicable.

Keywords: authorisation, computer crime, message authentication, social aspects of automationalleged attacker, attacker behavior, attacking process, computer security, conceptual framework, empirical data, external attacks, innovative attack phase, intrusion experiments, learning phase, operational security, preventive security, quantitative model, quantitative terms, reliability modeling, security intrusion process, standard attack phase

[5] C. Ma and A. Concepcion. *Technologies for Business Information Systems*, chapter A Security Evaluation Model for Multi-Agent Distributed Systems, pages 403-415. Springer Netherlands, May 2007. [bib | DOI]

[6] R. Ortalo, Y. Deswarte, and M. Kaaniche. Experimenting with quantitative evaluation tools for monitoring operational security. *IEEE Transactions on Software Engineering*, 25(5):633-650, 1999. [bib | DOI]

This paper presents the results of an experiment in security evaluation. The system is modeled as a privilege graph that exhibits its security vulnerabilities. Quantitative measures that estimate the effort an attacker might expend to exploit these vulnerabilities to defeat the system security objectives are proposed. A set of tools has been developed to compute such measures and has been used in an experiment to monitor a large real system for nearly two years. The experimental results are presented and the validity of the measures is discussed. Finally, the practical usefulness of such tools for operational security monitoring is shown and a comparison with other existing approaches is given.

Keywords: Security assessment, operational vulnerabilities, privilege graph, quantitative evaluation

[7] R. Savola. Towards security evaluation based on evidence collection. In *Proceedings of the 3rd International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, volume 4223 of *Lecture Notes in Computer Science*, pages 1178-1181. Springer, 2006. [bib | DOI]

Information security evaluation of software-intensive systems typically relies heavily on the experience of the security professionals. Obviously, automated approaches are needed in this field. Unfortunately, there is no practical approach to carrying out security evaluation in a systematic way. We introduce a general-level holistic framework for security evaluation based on security behavior modeling and security evidence collection, and discuss its applicability to the design of security evaluation experimentation set-ups in real-world systems.
