

Why to adopt a security metric? A brief survey *

Andrea Atzeni and Antonio Lioy

Politecnico di Torino
Dip di Automatica ed Informatica
Torino(Italy)
{shocked, lioy} @ polito.it

Abstract. No doubt that computer security is a hot topic nowadays: given the importance of computer-assisted activities, protection of computer system is of the utmost importance. However we have insofar failed to evaluate the actual security level of a system and thus to justify (either in technical or economical terms) the investments in security. This paper highlights the motivations to improve security measurement techniques, analyses the existing approaches, and discusses whether their are appropriate or some new directions should be explored.

Keywords: security metric, computer system security

1 Introduction

Intuitively, security evaluation of computer systems is an important task. But why is it so important? Why is it so urgent and why so many efforts are devoted to this aim? Obviously, it is so important because *electronic machines* surround us everytime and everywhere: for example, when we make a call, when we edit a document, when we write an e-mail, or when we schedule a meeting with our Personal Digital Assistant. So, in a certain way, computer systems bear on our life the same influence that atmospheric conditions and wild animals bore on our ancestors. Undeniably, computers surround us pervasively, and they will much more spread in the future, as last decades permit us to foresee.

Measurement is the way by which humans understand with more precision the rational world. *We measure to reveal a condition and possibly alert the user. We also measure to quantify the magnitude of phenomena. Probably most importantly, we measure to control processes* [1]. Paraphrasing Lord Kelvin, *when you can measure what you are speaking about and express it in numbers, you know something about it* [2]. Starting from this base, we will explore the scientific literature to gain more insight to the motivation of measuring the security of a computer system, recalling that measurement and metric adoption is almost always a tool to improve and manage developing process [3]. The rest of the paper is organised in following manner. Section 2 briefly describes general concepts related to metric and measurement systems, sections 3, 4 and 5 examine three main motivations justifying the improvement of security measures, respectively efficiency, economical gain and social management. Section 6 explores some

* This work is part of the POSITIF project, funded by the EC under contract IST-2002-002314.

actual work developed on measurement tools in security. This topic permits to understand if spending an effort in the definition of a security metric is worthwhile or not. Conclusions follow in section 7.

2 What is a measure

To understand the importance of measuring a system, it is first necessary to understand what a measure is. A measure is the result of a measurement, i.e. a process aiming to acquire quantitative or qualitative values of real world attributes. A “real-world attribute” is any property of an abstract or concrete existing entity. For example, my clock is an entity, and one attribute is its colour, which could be expressed in qualitative term (it is black) or in quantitative term (its Red-Green-Blue hexadecimal component values are 06-03-03).

A measurement system should exhibit some properties in order to be effective and useful:

- **Clarity** A measure should be easy to interpret, at least in its operative context. A measure without clear meaning will lead to discussions and different beliefs in the best case, to wrong conclusions in the worst. In both cases, the usefulness of the measure is reduced.
- **Objectiveness** The measure should not be influenced by the measurer will, or beliefs, or actual feeling. Otherwise, its value will retain the correct sense only for the original measurer, and the measure would lose in generality.
- **Repeatability** If repeated in the same context, with exactly the same conditions, the measure should return the same result. If this is not the case, as the uncertainty in the value increases so the measurement’s usefulness may decrease, and its treatment may become harder.
- **Easiness** The measure of an attribute should raise knowledge about the entity itself, sometimes with the purpose of improving the usefulness of the entity. However, if the measure is too difficult to be performed, or simply impossible to accomplish, the knowledge’s gain is not sufficient to motivate the measurement.
- **Succinctness** Only important parameters should be considered, letting aside aspects not important to the definition and/or the comprehension of the entity under measurement. Such property aims to reduce both measure’s complexity and uncertainty. In a few words, “don’t miss the forest for the trees”.

These properties are always desirable, but they are very difficult to achieve when dealing with measure of complex quantities – such as security (or goodness or any other not easily definable entity). Therefore, as the simple existence of statistics proves, many attempts successfully treat measures not clearly understood or prone to relevant uncertainty.

After this brief discussion of the desirable properties, we may now face the paper’s main question: *why would the adoption of a security metric be a profitable enhancement?*

3 Efficiency

A natural answer to the paper’s question is *because to work without measure is not efficient*, that is, the ratio of output to input of a system may be improved by employing better metrics. Blakley [4] claims that the *traditional approach to information security has failed*, and this is due to a number of reasons, that can be resumed by the tremendous complexity of large computer systems. Composing a large, secure system from little and simple secure components is a daunting purpose, due to the difficulty of the composition, rather than to building the single components, which may be easy. On the other hand, starting directly with the construction of huge secure system is worse. As previously stated, this is not surprising, because the complexity of general-purpose system permits billions of different operation types, hence it is quite difficult to foresee each of them in different possible scenarios. However, in spite of the problem difficulty, measurement systems can greatly help. As stated by Bush et al. [5] *the better one understands a phenomenon, the more concisely the phenomenon can be described*, so description’s efficiency improves. In fact, the simple act to measure can improve the efficiency, we could just recall the axiom, circulating in software engineering field, *when performance is measured, it improves* [6]

A metric is not only important for its own sake, but as part of a more wide schema. The measures permit to acquire knowledge and improve the system. As in the conceptual schema of Fig. 1, the *acquisitors* are means to gain knowledge of the external world, i.e. to measure some attributes. These *acquisitors* are the focus of the measurement’s system definition, they are the ones that should exhibit properties of “good measure”. The remaining part of the figure refers to the *treatment system* (for data manipulation to extract meaning) and *feedback system* (for the desirable feedback to the system under measurement, in terms of improving changes). It is noticeable that all the other system parts profit from a “good” measurement system.

If embedded in an overall evaluation schema, the power of the measurement can inspire awe. In the ongoing European project POSITIF [7] a holistic approach is proposed to face the security concern, restricted to the computer network environment.

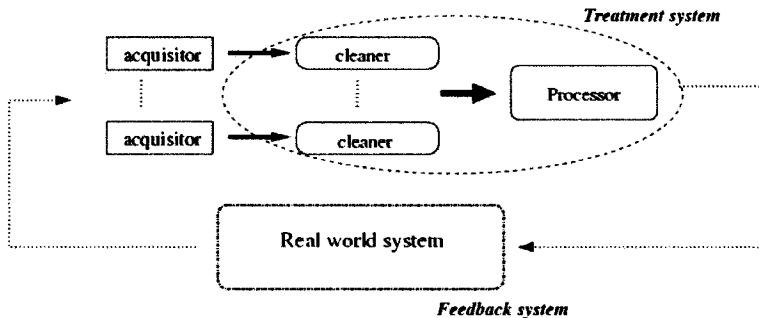


Fig. 1. The righteous improving schema

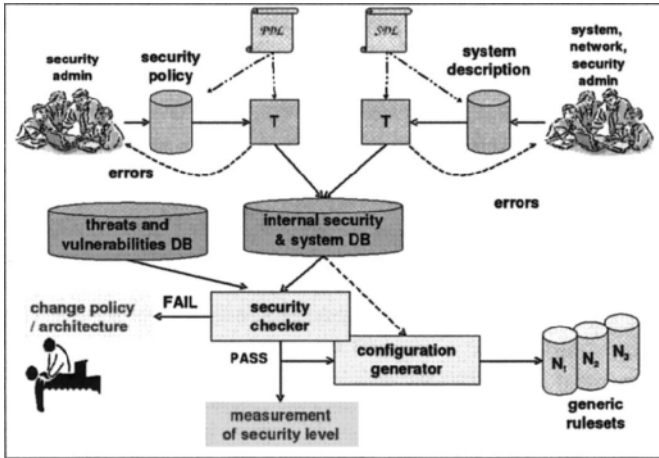


Fig. 2. The Positif framework

In the POSITIF framework (depicted in Fig. 2) the network will be described in formal terms by a formal *system description language*, the desired security level will be described by a formal *policy description language* and the security evaluation will be performed by a *security checker*, capable of evaluating the actual network security level.

4 Economical motivations

Without the conscious decision to agree on a way of measuring, cooperative activity could hardly take place. With it, marketplaces and increasingly sophisticated economies can develop, matching barter, cash, or credit to whatever is owned by one person and desired by another [8]

In our current society, economical reasons are the most common motivation for human actions¹, thus, many researches approach the metric definition problem from an economical perspective. An issue in metric establishment is that security is not described in “comprehensible terms” with respect to a business expert [4], and even more for “normal computer users”. This holds a great difference to other field, like medicine (for example, the effect of smoking on a human body is much more clear, also in “monetary” terms). This issue arises in security due to the difficulty of the evaluation of the benefits of adopting a security technology, which are hard to assess. It is difficult to know beforehand the impact of a security change, to compare alternative designs and

¹ We are really afraid that many people would agree upon this statement ... Anyway we don't want to linger in moral judgements in this (scientific) paper (and, however, other wide motivations, such as military supremacy, often are also worse).

to make the right choice with poorly-objective available data [9]. Furthermore, without an economical evaluation framework, the companies' tendency may be to not share security information, embracing a greedy strategy of short-period gain [10].

Another urgent point is the dramatical increment in the last few years of the attack frequency. Long ago, in the early Internet stage, only universities and "good guys" shared information by wide area networks, so security concerns has been far remoted from Internet developer's minds for long time². When Internet spread its influence and became commonplace to the majority of computer users, also "bad guys" came into play, and security threats multiplied as well. At the same time, the company's economic reliance on information and informatics grows more and more [11] and hence Internet (in)security has become an economic concern.

Nowadays, cyber-attacks cause huge losses. For example, a survey [12] estimates that *the stock price impact of cyber-attacks show that identified target firms suffer losses of 1%-5% in the days after an attack. For the average New York Stock Exchange corporation, price drops of these magnitudes translate into shareholder losses of between \$50 million and \$200 million.* The same survey also claims a worldwide overall loss, for all attack types, of about \$226 billion³. However, the fact remains: attacks on information systems influence the stock market, the extent of which depends on the firm's business type and on the attack type. Some partially contradictory studies exist on the topic, e.g. [13–16], summarized by [12]. The apparent trend is, in general, a loss in the short time period, and a smaller loss in the medium-long range. The extent of such losses is surely related to the type of company, for example B2C companies, such as Amazon and eBay, almost completely relying on Internet technology, can suffer very wide financial losses, as demonstrated in June 1999 when eBay's site was unavailable for 22 hours and the stock lost twenty-five percent of its value [17]. Possibly, the type of attack is an influencing factor, in particular attacks impacting confidentiality seem to cause a greater damage than others [14], but such result is probably related to the company type.

Other researches and surveys highlight the overall financial impact of virus and worm diffusion, and general economic damage imputable to any kind of cyber-attack. Costs are always many billion dollars. Moreover, cyber attacks can influence cost in more subtle terms, for example diminishing the adoption of informative infrastructure, hence decreasing the achievable productivity.

All these menaces are reduced by better security tools, and a meaningful and effective measurement system is propaedeutic to any security improvement .

5 National security motivations

Domination and leadership are one of the earliest and strongest motivations for knowledge acquisition among human beings. The capability to measure security enables strategic plans and appropriate counteracts to enemy's actions. Computer system attacks, depending on motivations, may be a concern of national and international rel-

² But for availability issues, that were studied since the very beginning of Internet development.

³ The survey also states that *the reliability of these estimates is often challenged; the underlying methodology is basically anecdotal.*

evance. Since metaphors and similitudes are a way to *give maximum meaning with a minimum of words* [18], they often illuminate on the real meaning of a concept in a particular context. Words like *cyber-terrorism* or *cyber-war*, used in many government and police documents, point out the great importance informatics attacks hold in such environments. We can just notice that rumours report that even the (in)famous head-terrorist Osama-Bin-Laden spread orders and informations to his followers by means of Internet and steganographic techniques [19]. Of course, a security measure able to measure both the attacking techniques and also the defending countermeasures, in a comparable fashion, would be of great help to understand if terrorists can by-pass the defences or if instead the situation is relatively safe.

A series of yearly USA CSI-FBI surveys gather data by interviewing a large number of computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities. Investigation concerns include, among others, the way organisations evaluate the performance of their investments in computer security, the portion of the IT budget devoted to computer security, the security training needs of organisations, the level of organisational spending on security investments, the impact of outsourcing on computer security activities. The most recent surveys [20] exhibit some good news, such as the decrease of financial losses related to security breaches, and the extensive adoption of security audits. On the other hands, virus and denial of service attacks increase to a value of \$55 million, and the sharing of intrusion information is in decline, due to the consequent bad publicity. However, the report does not highlight clear trends in computer crime and, by the way, its samples are probably not chosen in a statistically sound fashion [12]. These facts point out one more time the need of useful metrics to determine security and the consequence of security action. Such consequences should be determined both to analyse business interaction and to evaluate effectiveness of countermeasures.

6 Proposed solutions

The purpose of this section is to illustrate the proposes actually in the arena, in order to judge the opportunity to adopt or not a security metrics.

First of all, an advice always valid when dealing with measures and metrics is to *give meaning to measurement*, that is, to follow the principles explained in section 2, and some other practical principles, like visibility of the measure (the results should be close to the end-user), tail-to-the-audience (the results should be adapted to the end-user, for example eliminating non-relevant data), traceability (the tools and measures employed should refer to an explaining base, for example, the needed knowledge base to calibrate a sensor) [21]

The way to improve the world can be economic and/or technical, and it may come from one or more of the approaches considered in the next subsections.

6.1 Technical solutions

Several approaches to establish a technical security evaluation have been proposed. Maybe the most promising ones involve statistical research. The idea is the establish-

ment of a model capable of describing system behaviour. Starting from such a description, the aspired result is the acquisition of further knowledge on the (simulated) system, and hopefully the forecast of the system security evolution. This *modus operandi* mainly stems from the dependability field, not surprisingly however, since dependability and security share many common points, and security or dependability are sometimes considered one as a subset of the other, as expressed in [22]. An excellent paper [23] surveys many methodologies developed.

Reliability block diagrams, usually adopted in large network analysis [24, 25], represent a system as composed by many interconnected components. The components are modelled with statistical properties, like mean-time-between-failure, and the system behaviour is simulated starting from single-component characteristics and properties of the component linking connection.

Fault trees are acyclic graphs (trees), in which the root is the system of interest, leaves are single component and inner nodes, that is nodes between the root and the leaves, are “logic gates”, able to model the failure flow from the leaves to the root. If a flow from leaves to root is established, then a failure occurs. These systems are well understood and general enough to be applied in *hardware, software and humanware in complex computer-based systems* [26].

Attack trees are a natural security adaptation of fault trees, where a system failure (i.e. the root of the tree) is a security breach, the leaves are the menaces to which the system is exposed, and the flows between leaves and root are the possible ways of exploiting the basic weaknesses. The first mention of attack trees is in the Schneier’s milestone book *Secrets and Lies: Digital Security in a Networked World* [27].

Other modelling tools include model checking, in which the system is formally depicted by its possible operative states, and the evaluation is based on reachability analysis of the state space, and stochastic representation of the system evolution by Markov chains, as pointed out by Dacier’s notable work during his PhD studies and later [28–31].

We believe that several of these approaches are very promising, as witnessed by their many successful applications to the dependability field. At the present time the problem is the lack of a formal and validated model of security behaviour, which in rough words could be resumed by a challenging issue of statistical analysis: the study of non-independent statistical variables.

6.2 US Government solutions

Governments, first among all that of the United States of America, devote considerable efforts to analyse and implement efficient metrics and measurement systems. The National Institute of Standards and Technologies (NIST) [32] is the official standardisation organism in the USA, and its CSD division is devoted to computer security standardisation [33]. Inside CSD, three sections are involved in system evaluation and certification, both mansions strictly related with measurement; these sections are:

- Federal Information System Management Act (FISMA) implementation program
- Security Testing
- Security Management and Guidance

FISMA is the emanation of the US Congress that highlights the risks of aggressive cyber attacks at the heart of critical infrastructures, and that urges countermeasures in order to prevent such possibilities from becoming real. The FISMA implementation project is a NIST's CSD effort aiming at promoting standards and guidelines to reach goals like security categorisation of information and information systems, selection of appropriate security controls for information systems, verification of security control effectiveness and determination of information system vulnerabilities, operational authorisation for processing (security accreditation) of information systems, in order to make available more consistent, comparable, and repeatable evaluations of security controls applied to information systems, a better understanding of enterprise-wide mission risks resulting from the operation of information systems, more complete, reliable, and trustworthy information for authorising officials, facilitating more informed security accreditation decisions, or, synthetically, more secure information systems within federal agencies, which composes the critical computer infrastructure of the United States [34]. Roughly speaking, almost all activities relate to qualitative or quantitative measurements.

The Security Testing Unit approaches the problem of developing, managing and promoting assessment tools as means of secure system development. Under this Unit fall partnerships promoting the dissemination and use of evaluated IT products and systems and the growth of such products in U.S.A., like National Information Assurance Partnership [35] or Trust Technology Assessment Program [36]. Other aspects involve the development of an automatic testing toolset, in order to improve the economics of security functional testing [37], or the development and dissemination of cryptographic-modules validation program [38] against FIPS 140-2 Security Requirements for Cryptographic Modules [39].

The Security Management and Guidance Unit mainly gathers standards, best practices and guidelines adopted inside federal US agencies [40] aiming to export virtuous behaviour or to discuss and improve possible weak practices. Moreover, this division emits or collects publications related to all system security aspects, from system evaluation to information acquisition by means of questionnaires [41].

Other CSD duties include guidance to embed security development into the system life-cycle [42], to adhere to federal security requirements for federal agencies, a.k.a policies [43], helping program for security management [44], and economical framework evaluation method for IT security investment [45]. Also a software tool helping towards automating security self-assessment is freely available from the web site [46]

6.3 Economical solutions

Blakley [4] proposes the "monetisation" of security actions. In such a way, information loss and product effectiveness will be available in monetary terms, and may possibly become a usual insurance and trade instruments. He remarks how the publication of such monetary information would create an *effective information security market* and permit to allocate capitals in the right manner, and would stop the rewarding of ineffective solutions. However, such a solution appears really hard to achieve. Blakley's suggestion is to initially accept limited liabilities for security products, which will be adjusted by the

market with its usual demand-offer mechanism. Even if Blakley's position may make sense, a long and hard work appears essential to correctly price security.

Butler proposed an intriguing cost-benefit analysis, called Security Attribute Evaluation Method (SAEM) able to *bridge the communication gap between security managers and information technology (IT) managers* [9], that is, in simple term, to make clear the benefit and the cost of a security solution to a non-security adept. SAEM method involves four steps: 1) a security technology benefit assessment, 2) an evaluation of the effect of security technologies in mitigating risks, 3) a coverage assessment and 4) a cost analysis. Of course, the hard part is not to state but to accomplish such tasks. The first point is accomplished by supervised and extensive interviews of IT and security managers. The second point is achieved through statistical data, describing the frequency and the outcome of threats. The last two points can be developed in parallel, and relate to the evaluation of how large is the coverage of the countermeasure and what is its relative cost. Many problems arise with such evaluation systems. The initial data acquired in the first phase are not objective, so all the subsequent phases are potentially influenced by such errors. Moreover, the statistical data required for the second phase may be not available. With regard to this point, Butler proposes the multi-attribute analysis, a useful technique able to treat uncertainty when many attributes are involved. However, much of the multi-attribute approach is based on human subjective choices, hence the final result is often useful, but rarely objective.

Gordon et al [10] studied the topic of sharing security-breach information. Based on previous literature and on the experience of Trade Associations (TAs), Information Sharing Analysis Centres (ISACs)⁴ and Research Joint Ventures (RJVs), they conduct a deep analysis of pros and cons for information sharing, stating that the combination of literature regarding TAs and RJVs *provides theoretical underpinnings to develop a model for examining information sharing related to security breaches*. The work is very interesting, but not conclusive, leading to suggest further research for the development of such a model. An investment security model was carried out in a more recent work [11]. Many are the simplifying assumptions, nevertheless the model retains a sound economical sense, capable of evaluating the best trade-off between cost of security breaches and benefit of threat reduction.

7 Conclusion

Security is a complex matter, neither deeply understood nor easily measurable, therefore, in order to better understand and evaluate it, the actual measurement system has to improve and possibly new measurement schemes have to come into play. From the economical perspective, the huge amount of money loss is a natural engine towards improvement, therefore many economical researches are going toward some sort of econometric models, as shown by the last 5-6 years of literature. Unluckily, these studies are not at the present time conclusive nor widely proven, hence further studies and

⁴ ISACs are industrial based organisation, with federal participation and assistance, aiming to information sharing, for example offering confidential venue for sharing security vulnerabilities and solutions

researches are welcome. In spite of this, we believe the scenario to be promising and fruits near to be borne.

As said, security is a complex matter, but this seems to stimulate a vast enflowering of studies, improving the day-by-day knowledge on the topic and the capability of structured evaluation, as pointed out by the cited papers. This should not come as surprise, since security is both a matter of civilian concern and government concern; so, it is natural that stimulating action is taken by more sensitive states (like the USA).

Perhaps, a problem of the past approaches was a too stringent focus on the evaluation issue. Instead, we believe that in order to work out practically usable solutions, the problem has to be approached in a more holistic way, formalising the goal to be achieved, formalising the properties of the system, and then using formal and automatic tools to evaluate the security. Positive side-effects, letting aside the automation of the evaluation, should be highly customisable results, precisely suitable for the actual evaluated system.

References

1. K. Fowler and J. Schmalzel. Why do we care about measurement? *Instrumentation & Measurement Magazine, IEEE*, 7(1):38–46, March 2004.
2. William Thompson. Popular lectures and addresses, 1891–1894.
3. KnowledgeRoundtable. Metrics. <http://www.knowledgeroundtable.com/app/content/knowledgesource/section/149>.
4. B. Blakley. The measure of information security is dollars. In *The First Workshop on Economics and Information Security, Berkeley (CA, USA)*, 16–17 May 2002.
5. S.F. Bush and S.C. Evans. Complexity based information assurance. Technical report, General Electric's corporate research and development, October 2001.
6. S.J. Keene. Cost effective software quality. In *Proceedings of Annual Reliability and Maintainability Symposium, Orlando (FL, USA)*, pages 433–437, 29–31 January 1991.
7. Sixth Framework Programme IST-2002-002314. Policy-based security tools and framework. [Online] <http://www.positif.org/>.
8. A. Linklate. *Measuring America*. Walker & company, 2002.
9. S. A. Butler. Security attribute evaluation method, a cost-benefit approach. In *Proceedings of ICSE2002 International Conference on Software Engineering, Orlando (Florida, USA)*, pages 232–240, 19–25 May 2002.
10. L. A. Gordon, M. P. Loeb, and W. Lucyshyn. An economics perspective on the sharing of information related to security breaches: concepts and empirical evidence. In *The First Workshop on Economics and Information Security, Berkeley (CA, USA)*, 16–17 May 2002.
11. L. A. Gordon and M. P. Loeb. The economics of information security investment. *ACM Transactions on Information and System Security*, 5(4):438–457, 2002.
12. B. Cashell, W. D. Jackson, M. Jickling, and B. Webel. The economic impact of cyber attacks. Technical Report RL32331, U.S.A. Government and Finance Division, 1 April 2004.
13. H. Cavusoglu, B. Mishra, and S. Raghunathan. The effect of internet security breach announcements on market value: Capital market reactions for breached firms and internet security developers. *International Journal of Electronic Commerce*, 9(1):69, Fall 2004.
14. M.P. Loeb Campbell K, L.A. Gordon and L. Zhou. The economic cost of publicly announced information security breaches: Empirical evidence from the stock market. *Journal of Computer Security*, 11(3):431–448, 2003.

15. M. Ettredge and V. J. Richardson. Assessing the risk in e-commerce. In *Proceedings of the 35th Hawaii International Conference on System Sciences, Big Island (Hawaii)*, page 11, 7-10 January 2002.
16. A. Garg, J. Curtis, and H. Halper. Quantifying the financial impact of it security breaches. *Information Management & Computer Security*, 11(2):74–83, 2003.
17. S. Glover, S. Liddle, and D. Prawitt. *Ebusiness: principles & strategies for accountants*. Prentice Hall, 2001.
18. OnlineWritingLab. Using metaphors in creative writing - why use metaphors? http://owl.english.purdue.edu/handouts/general/gl_metaphor.html.
19. P. Swami. Failed intelligence. *Frontline*, 18, 7 December 2001.
20. L. A. Gordon, M. P. Loeb, W. Lucyshyn, and R. Richardson. Ninth CSI/FBI computer crime and security survey. Technical Report RL32331, C.S.I. Computer Security Institute, 2004.
21. K. Fowler. Giving meaning to measurement. *Instrumentation & Measurement Magazine, IEEE*, 4(3):41–45, September 2001.
22. A. Avizienis, J. Laprie, and B. Randell. Fundamental concepts of dependability. Technical Report N01145, LAAS-CNRS, April 2001.
23. D.M. Nicol, W.H. Sanders, and K.S. Trivedi. Model-based evaluation: from dependability to security. *IEEE Transactions on Dependable and Secure Computing*, 1(1):48–65, Jan.-March 2004.
24. M. Sahinoglu, C.V. Ramamoorthy, A.E. Smith, and B. Dengiz. A reliability block diagramming tool to describe networks. In *Proceedings of Reliability and Maintainability Annual Symposium, Los Angeles (CA, USA)*, pages 141–145, 26–29 January 2004.
25. W. Wang, J.M. Loman, R.G. Arno, P. Vassiliou, E.R. Furlong, and D. Ogden. Reliability block diagram simulation techniques applied to the ieee std. 493 standard network. *IEEE Transactions on Industry Applications*, 40(3):887–895, May-June 2004.
26. L.L. Pullum and J.B. Dugan. Fault tree models for the analysis of complex computer-based systems. In *Proceedings of Reliability and Maintainability Symposium, 'International Symposium on Product Quality and Integrity', Las Vegas (NV, USA)*, pages 200–207, 22–25 January 1996.
27. B. Schneier. *Secrets and Lies: Digital Security in a Networked World*. John Wiley & Sons, 2000.
28. M. Dacier. *Towards Quantitative Evaluation of Computer Security*. PhD thesis, Institute National Polytechnique de Toulouse, 1994.
29. M. Dacier and Y. Deswarte. The privilege graph: an extension to the typed access matrix model. In D. Gollman, editor, *European Symposium in Computer Security (ESORICS 94), (Brighton, UK), Lecture Notes in Computer Science, 875*, pages 319–334. Springer Verlag, 1994.
30. M. Dacier, Y. Deswarte, and M. Kaaniche. Models and tools for quantitative assessment of operational security. In *12th International Information Security Conference (IFIP/SEC 96), Samos (Greece)*, pages 177–186. Chapman & Hall, 1996.
31. M. Dacier, Y. Deswarte, and M. Kaaniche. Quantitative assessment of operational security: Models and tools, 1996.
32. National institute of standards and technologies. <http://www.nist.gov/>.
33. National institute of standards and technologies - computer security division. <http://csrc.nist.gov/>.
34. National institute of standards and technologies - security certification index. <http://csrc.nist.gov/sec-cert/index.html>.
35. National information assurance partnership. <http://niap.nist.gov/>.
36. Trust technology assessment program. <http://csrc.nist.gov/ttap/>.
37. NIST - automatic functional testing. <http://csrc.nist.gov/auto-func-test/index.html>.

38. Cryptographic-modules validation program. <http://csrc.nist.gov/cryptval/>.
39. Federal information processing standard 140-2. <http://csrc.nist.gov/cryptval/140-2.htm>.
40. Federal agencies security practice. <http://csrc.nist.gov/fasp/index.html>.
41. Computer security research center - publications. <http://csrc.nist.gov/publications/>.
42. NIST - system development life cycle. <http://csrc.nist.gov/SDLCinfosec/index.html>.
43. NIST - federal agencies policies. <http://csrc.nist.gov/policies/index.html>.
44. Program review for information security management assistance (PRISMA). <http://prisma.nist.gov/>.
45. Return on security investment and IT security capital investment planning. <http://csrc.nist.gov/roi/index.html>.
46. NIST - software assessment tool. <http://csrc.nist.gov/asset/index.html>.