Towards Quantitative Risk Management for Next Generation Networks

Iztok Starc and Denis Trček

Faculty of Computer and Information Science, University of Ljubljana, Slovenia
{iztok.starc,denis.trcek}@fri.uni-lj.si

Abstract. While user dependence on ICT is rising and the information security situation is worsening at an alarming rate, IT industry is not able to answer accurately and in time questions like "How secure is our information system?" Consequently, information security risk management is reactive and is lagging behind incidents. To overcome this problem, risk management paradigm has to change from reactive to active and from qualitative to quantitative. In this section, we present a computerized risk management approach that enables active risk management and is aligned with the leading initiative to make security measurable and manageable. Furthermore, we point out qualitative methods deficiencies and argue about the importance of use of quantitative over qualitative methods in order to improve accuracy of information security feedback information. Finally, we present two quantitative metrics, used together in the model, and enabling a quantitative risk assessment and support risk treatment decision making.

Keywords: computer security, economics of security, risk management, security metrics, security measurement.

1 Introduction

Information security risk management is still in its early stages with regards to measuring and quantitative assessment. Currently, risk assessment is normally based on qualitative measurement and metrics. The consequent undesirable side-effect is that risk assessment cannot provide answer to questions like "How safe is my information system (IS)?" and "How much safer is my IS then my competitors' IS? Decision making under such uncertainty is not effective. Currently, decision makers react on incidents rather than be proactive. This lagging reaction results in notable losses. Risk management paradigm has to change from reactive to proactive, where risks are identified, assessed and treated in time, before incident takes place. Furthermore, risk management is also about financial investment into security safeguards. Therefore, their spending should be justified as much as possible. This is possible only when decision makers have adequate information to evaluate discrepancy between desired and actual risk. Based on this information, appropriate and economically sound safeguards are implemented to reduce risk to a level acceptable for organization and stakeholders.

A.M. Hadjiantonis and B. Stiller (Eds.): Telecommunication Economics, LNCS 7216, pp. 229–239, 2012.

New research steps are presented in this subsection and are aiming towards computerized quantitative risk management for decision making support. First, we will present basic definitions and open problems in this area. Next, we will focus on risk assessment methodology and will address measurement and metrics issues. Finally, we will present technological architecture that enables reactive and proactive risk management in modern IS.

2 Basic Definitions

The normative reference, which is most relevant for risk management in IS, is ISO/IEC 27000-series standards for information security management systems. According to ISO/IEC 27000 [9] information security means preservation of confidentiality, integrity and availability of information.

- "Confidentiality is a property of system that information is not made available or disclosed to unauthorized individuals, entities or socio- and/or technical processes".
- "Integrity is a property of protecting accuracy and completeness of assets. There are many types of assets, tangible assets like (i) information, (ii) software, (iii) hardware, (iv) services, (v) people and also intangible assets like (vi) reputation".
- "Availability is a property of being accessible and usable upon demand by an authorized entity".
- Furthermore, and according to ISO/IEC 27000, information security may include preservation of other properties, such as authenticity, accountability, non-repudiation and reliability.

Concepts defined above are only meaningful in practice when they are linked to organization's assets and selected as operational requirements. Assets are valuable to organization and other stakeholders as well as to various threat agents. Therefore, an appropriate security assurance method has to be chosen in order to achieve organization's and stakeholders' confidence that assets satisfy the stated information security requirements and consequently its security policy and/or applicable law like [6]. For example, when organization provides service to its customers, a process security assurance method is chosen, like ISO/IEC 27001 [10]. Next, the method is applied to ensure that assets (including IS and IS services) conform to security requirements. In this way, correct, efficient and economically sound safeguards are implemented that protect assets from threat agents in such way that risk is reduced to a level acceptable for both organization and stakeholders. Risks have to be constantly monitored and when any risk factor changes then the process has to be repeated again in timely manner. This continuous activity is called information security risk management (risk management for short). Before we advance with risk management and its activities some additional basic terms have to be defined.

According to ISO/IEC 27000 information security risk (risk for short) means potential that a threat will exploit a vulnerability of an asset or group of assets and thereby cause harm to an organization and consequently cause harm to stakeholders. Vulnerability is a weakness of an asset or safeguard that can be exploited by a threat. Threat is a potential cause of an information security incident (incident for short).

We can now focus on risk management, which is, according to ISO/IEC 27005 [12], comprised of coordinated activities that aim to direct and control an organization with regard to risk. First, organization's business context has to be established that is foundation for further activities. Within this context, risks have to be identified. Next, risk assessment takes place where risk are qualitatively or better quantitatively described and prioritized against organization's risk evaluation criteria. Subsequently, risks have to be treated to achieve security requirements and correct, efficient and economically sound means of managing risk have to be implemented[1]. These means are called safeguards[2] which include policies, processes, procedures, organizational structures, and software and hardware functions. Depending upon safeguards objectives risk treatment can be accomplished in four different ways: (i) risk reduction, (ii) risk retention, (iii) risk avoidance and/or (iv) risk transfer. Finally, if risk treatment is satisfactory then any residual risk is accepted. Risk management is continuous "Plan-Do-Check-Act" process, because risk factors may change abruptly and this may lead to undesirable consequences. Thus, risk and safeguards need to be monitored, reviewed and improved, when necessary.

3 Open Problems

Information security researches are facing challenge, because current risk management practice is reactive and it is lagging behind incidents. This practice has adverse impact to the level of business objectives achieved and results in huge damages due to following reasons.

- **Plan and Do Problems.** Safeguards may be not correct and/or effective enough to protect assets from harm. Software (including security software) is buggy and single attack can disable safeguards and expose assets. In addition, threat landscape is constantly changing and future threats are not anticipated in time, because (i) business contexts of organizations are changing, (ii) user dependence on ICT is rising and (iii) ICT grows in size and complexity and (iv) ICT interdependencies is increasing.
- **Check and Act Problems.** Incapability to provide answers to security and risk related questions in time means that security cannot be managed efficiently, e.g., "How secure is the organization?" or "What is the degree of information security risk?". Logical consequence of this incapability is wider window of vulnerability [16] and increased duration of asset exposure. Thus, probability of information security incident is greater on average. Eventually, answer to two questions above is provided when risk manifests itself as incident and assets are damaged. Finally, risk management reacts on this lagging (human perceptible) indication. At this (too late) point, organizations as well as stakeholders perceive that security requirement are not fulfilled and risk level is unacceptable.

[1] Other product assurance methods such as Systems Security Engineering – Capability maturity Model [8] and/or process assurance methods such as Common Criteria [7] are used to ensure safeguard correctness and efficiency. ISO/IEC TR 15443-2 [13] lists a comprehensive list of assurance frameworks.

[2] Safeguards are also known as controls or countermeasures. Standard ISO/IEC 27002 [11] provides a comprehensive list of safeguards.

How are these problems addressed in information security research? On one hand, new security mechanisms [1] are studied to overcome brittleness of software and to safeguard IS more effectively. In parallel with this effort, new product security assurance methods are developed to evaluated security mechanism's strength as well as process assurance method to evaluate correctness of security mechanism's design, implementation, integration with the IS and deployment.

On the other hand, no security mechanism or security assurance method seems to be perfect to this point. Risk factors may change abruptly and ISs are changing, so statistically relevant long-term data is not available to enable security forecasting and information security insurance practical. Therefore, risk has to be reduced and this means safeguards have to be constantly monitored, reviewed and last but not least, improved, when necessary. This is possible only if information security feedback is accurate and is provided in real-time. Only then, decision makers have adequate information.

Detection of security precursor before incident takes place and risk forecasting ability is a research priority. In order to accomplish this, better security measurements methods have to be defined that are (i) accurate, (ii) real-time, (iii) economically sound, and (iv) measure security attributes according to business requirements. Security attribute measurement takes place on various IS objects, e.g., on routers, workstations, personal computer, etc. Acquired raw data can be then interpreted using metrics/indicators that are in fact analytical models, which take basic measurements as an input and return organization's information security state. This feedback information should be provided to decision maker as soon as possible in order to enable pro-active risk management rather than reactive. Thus, leading indicators should be chosen over lagging indicators, to prevent incident rather than to detect and manage incidents.

The indicator output is manually or computationally compared to organization's own risk evaluation criteria and risk management action is taken if necessary. Using described measurement and metrics as a foundation, security research aims to create also self-adapting security information and event management systems (SIEM) [2] that take actions based upon indicators values and measurements.

Before we advance towards computerized risk assessment for proactive risk management, we will analyze current risk assessment practices as well as address security metrics and measurement issues and provide some problem solutions.

4 Current Risk Assessment Methodology

The most elementary approach to risk assessment starts with identification of a set of assets $A = \{a_1, a_1, ..., a_n\}$ and threats $T = \{t_1, t_2, ..., t_n\}$. Next, a Cartesian product is formed $A \times T = \{(a_1, t_1), (a_2, t_1), ..., (a_n, t_m)\}$. The value of each asset $v(a_n)$ is determined and, for each threat, the probability of interaction with asset during certain period is assessed $Ea_n(t_m)$. An interaction is problematic only if asset is exposed to vulnerability $Vt_m(a_n) \in [0,1]$. Taking this into account, an appropriate risk estimate is obtained as following.

$$R(a_n, t_m) = v(a_n) * Ea_n(t_m) * Vt_m(a_n) \quad (1)$$

The real problem with this procedure is obtaining exact quantitative values for the above variables in real-time for the following reasons.

- Old statistical data are not available, because the technological landscape and IS change quickly to meet evolving business requirements. Within these changes, new vulnerabilities are created. In addition, different threats are attracted at different time, because business context and assets change over time. Consequently, likelihood of attack and number of vulnerabilities and exposures change over time.
- Furthermore, a substantial proportion of an organization's assets are intangible assets, such as information and goodwill. Identification and valuation of these assets remains a difficult issue [4]. Even worse, the most important asset is personnel. Due to the specifics of this type of assets their valuation is very hard. For example, none of them are recorded and valued in balance sheets.

Therefore, it is hard to derive the exact value of risk. The above facts lead to the current view that the logical alternative to quantitative IS risk assessment is a qualitative approach at the level of aggregates. Here, assets, threats, and vulnerabilities are each categorized intro certain classes. By using tables, such as one below, risks are assessed and estimated, and priorities are set by rank-ordering data on an ordinal scale.

Table 1. The ISO/IEC 27005 risk assessment matrix measures risk on a scale of 0 to 8 and takes two qualitative inputs: (i) likelihood of an incident scenario and (ii) the estimated business impact. For example, if the estimated likelihood of incident scenario is low and the corresponding business impact is high, then the risk is described by the value 4.

		Likelihood of Incident Scenario				
		Very Low	Low	Medium	High	Very High
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

This is also a legitimate approach according to standards, such as ISO/IEC 27005. However qualitative risk assessment approaches have significant shortcomings and suffer from the following two major disadvantages [3].

- Reversed rankings, i.e., assigning higher qualitative risk ratings to situations that have lower quantitative risks.
- Uninformative ratings, i.e., (i) frequently assigning the most severe qualitative risk label (such as "high") to scenarios with arbitrarily small quantitative risks and (ii) assigning the same ratings to risk that differ by many orders of magnitude.

Therefore, the value of information that qualitative risk assessment approaches provide for improving risk management decision making can be close to zero and misleading in many cases of many small risks and a few large ones, where qualitative ratings often do not distinguish the large risk from the small. This is further justification that quantitative risk treatment has always to be the preferred option, if metrics and measurement methods are available.

5 Metrics and Measurement Problems

The very first activity for successful risk assessment is data collection. These data should include new threats, identified vulnerabilities, exposure times and the available safeguards. This collection and dissemination of data should be in real time to ensure a proactive approach to risk management and also self-adapting security systems. In order to accomplish this, acquisition and distribution process have to be automated.

It needs to be emphasized that, although security in IS has been an important issue for a few decades, there is a lack of appropriate metrics and measurement methods. During measurement activity, numerals are assigned to measures under different rules that lead to different kinds of scales.

Qualitative scale types are nowadays used predominantly for information security measurements. Under Steven's taxonomy [23], they are classified as nominal (categorical) and ordinal. Ordinal scales determine only greater or lesser operation between two measurements. The difference operation between two measurements is not allowed and has no meaning, because successive intervals on the scale are generally unequal in size. Nevertheless, statistical operations such as mean and standard deviation are frequently performed on rank-ordering data, but conclusions drawn from these operations can be misleading.

Instead, quantitative scale types, such as interval and ration scales, should be used to outcome shortcomings described above and consequently, to provide more accurate feedback information. Some important advances have been achieved towards quantitative vulnerability metrics recently. The first such advances are constituted by two databases, the MITRE Corporation Common Vulnerabilities and Exposures [18] and U.S. National Vulnerability Database [19]. These are closely related efforts in which online acquisition and distribution of related data have been enabled by the security content automation protocol SCAP [21]. The main procedure with the first of the databases is as follows.

- The basis is the ID vulnerability, which is an 11-digit number, in which the first three digits are assigned as a candidate value (CAN), the next four denote the year of assignment, and the last four denote the serial number of vulnerability or exposure in that year.
- Once vulnerability is identified in this way, the CAN value is converted to common vulnerability and exposure (CVE).

The data contained in this database are in one of two states. In the first state there are weaknesses with no available patch and in the second state are those variables for which a publicly available patch exists.

This is the basis for the metric called daily vulnerability exposure DVE [14]. DVE is conditional summation formula to calculate how many asset vulnerabilities were public at given date with no corresponding patch and thus possibly leaving a calculated number of assets exposed to threat. DVE values are obtained as follows.

$$DVE(date) = \sum_{vu\ln s} (DATE_{disclosed} < date) \wedge (DATE_{patched} > date) \tag{2}$$

DVE is useful to show whether an asset is vulnerable and how many vulnerabilities contribute to asset's exposure. In addition, derived DVE trend metric is useful in risk

management process to adjust security resources to keep up with rate of disclosed vulnerabilities. Also, additional filtering can be used with DVE such as Common Vulnerability Scoring System (CVSS) [17] to focus on more severe vulnerabilities and exposures. But extra care should be taken when interpreting filtered results, because CVSS filter takes qualitative inputs for quantitative impact evaluation and suffers from same deficiencies as similar qualitative risk assessment approaches.

Another useful metric for our purpose has been proposed by Harriri et al., called the vulnerability index VI [5]. This index is based on categorical assessments of the state of a system: normal, uncertain, or vulnerable. Each network node has an agent that measures the impact factors in real time and sends its reports to a vulnerability analysis engine. The vulnerability analysis engine VAE statistically correlates received data and computes component or system vulnerability and impact metrics. Impact metrics can be used in conjunction with risk evaluation criteria to assess and prioritize risks.

More precise description of VI calculation will be demonstrated for the following fault scenario FS_k. During normal network operation, node's transfer rate is TR_{norm}. Transfer rate may deviate around this value but should not fall below TR_{min}. For each node, CIF is calculated using $TR_{measurement}$.

$$CIF\left(node_j, FS_k\right) = \frac{\left|TR_{norm} - TR_{measuremen\ t}\right|}{\left|TR_{norm} - TR_{\min}\right|} \tag{3}$$

Having all CIF values, the component operating state COS can be computed. For each fault scenario FS_k, a operational threshold $d(FS_k)$ is set according to organization's risk acceptance criteria. Next, CIF value is compared to the operational threshold $d(FS_k)$. The resulting COS value equals 1 when the component operates in an abnormal state and 0 when it operates in a normal state.

$$COS\left(node_j, FS_k\right) = \begin{cases} 1, CIF\left(node_j\right) \geq d\left(FS_k\right) \\ 0, CIF\left(node_j\right) < d\left(FS_k\right) \end{cases} \tag{4}$$

Finally, a system impact factor SIF can be computed that identifies how a fault affects the whole network and shows the percentage of components operating in abnormal states, i.e., where CIF exceeds normal operational threshold $d(FS_k)$, in relation to the total number of component. The obtained SIF value can be used can be used in conjunction with risk evaluation criteria to assess and prioritize risks.

$$SIF_{nodes}\left(FS_k\right) = \frac{\sum_{\forall j} COS\left(node_j, FS_k\right)}{totaNumber\ OfNodes} \tag{5}$$

At the end of this sub-section, graph based methods need to be mentioned, which are often used in IS risk assessment and management. One well-established technique in this field is suggested by Schneier [22] and is called attack trees. Attack trees model security of system and subsystems. They support decision making about how to improve security, or evaluate impacts of new attacks. Rote nodes are the principal goals of an attacker and leaf nodes at the bottom represent different attack options.

Intermediate nodes are placed to further refine attacks towards the root node. Nodes can be classified into two categories. When attack can be mounted in many different ways, an "OR" node is used. When attack precondition exists, an "AND" node is used. After the tree is constructed, various metrics can be applied, e.g., cost in time and resources to attack or defend, likelihood of attack and probability of success, or statements about attack such as "Cheapest attack with the highest probability of success".

6 Towards a Computerized Risk Management Architecture

The basis towards computerized risk management is MITRE's initiative called "Making Security Measurable and Manageable" [15]. This initiative has the following structural elements: (i) standardized enumeration of common information security concepts that need to be shared such as vulnerabilities, (ii) languages for encoding and communicating information on common information security concepts, (iii) repositories for sharing these concepts, and (iv) adoption of the above elements by the community through the use of defined program interfaces and their implementations. The initiative is focused on operational level of risk management. Many leading industry security products [20] are already SCAP standard validated, and utilize above described benefits.

Our approach [24] follows the above structure, builds on it (the implementation is still an on-going process), and can be used to improve risk management on strategic and/or tactical level with the development of business flight simulators. In addition, these simulators may be used for automated support of decision-making and could be thus self-adapting security information and event management systems enablers. The IS security environment is complex and it is comprised of information technology and human factor. Because analytical solutions in complex systems are exceptions, we have to rely on computer simulations. Based on this and on the measurement apparatus developed so far, our approach works as follows (see Fig 1).

With regard to achieve efficient risk management, simulations have to be as much realistic as possible. Thus, simulators use two real-time data-feeds.

The US National Vulnerability Database serves as a data-feed for detecting vulnerabilities and exposures of assets. The architecture communicates with the database (or tools provided in the footnote) via SCAP protocol. For example, DVE is calculated by querying the database for each organization's IS asset.

1. Another data-feed is provided through SIF infrastructure where agents monitor the status of nodes in the observed system. Agents and monitoring nodes communicate via SNMP protocol.

In order to successfully correlate organization's asset with newly discovered vulnerabilities and exposures, these have to be registered in NVD. Thus, this data-feed enables reactive risk management. Next data-feed enables proactive risk management, because likelihood and impact of attack is assessed in real-time, regardless if vulnerabilities or exposures are registered in NVD.

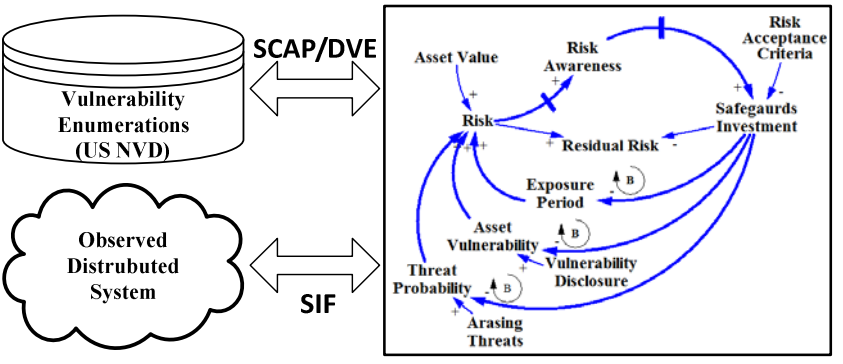

Fig. 1. General Information Technology Risk Management (GIT-RM) model

The numerical representation of acquired data is then used in the simulation model. The aim of simulation is determining dynamics of risk factors to derive information security risk dynamics. The causal dependency of risk factors can be explained in the following way. In the centre of the analysis are assets and threats. Assets are exposed to threats due to their various vulnerabilities. The interaction of threats with vulnerable assets leads to risks. The longer assets are exposed to threats, the higher is the probability of successful exploitation of these vulnerabilities, and therefore the higher the risk. In line with time delayed risk perception, it takes some time to implement appropriate safeguards to reduce exposure period, threat probability and/or asset's vulnerability. After implementation of safeguards according to organization's risk acceptance criteria, some portion of risk may remain effective and is referred to as residual risk.

The mathematical model that formalizes description above [25] is based on first-order differential calculus and is originally provided in Vensim syntax. We present its state-space representation to provide some insight into model characteristics. The internal states, like asset value, are represented by vector $\mathbf{x}(t)$. Vector $\mathbf{u}(t)$ describes inputs, such as arising threats or vulnerability disclosure and $\mathbf{y}(t)$ is output vector to derive residual risk. The system output is defined by functions $\mathbf{h}(t, \mathbf{x}(t), \mathbf{u}(t))$, while the system state can change with respect to current state and its inputs and it is modelled with functions $\mathbf{f}(t, \mathbf{x}(t), \mathbf{u}(t))$. Due to causal dependencies of risk factors and consequently their representation in equations, this system is classified as non-linear. For example, asset vulnerability and safeguard investment states are mutually depended. This system is also time-variant, because it can change in the simulation time, due to PDCA risk management process.

$$\begin{aligned} \frac{d\mathbf{x}}{dt} &= \mathbf{f}\left(t, \mathbf{x}\left(t\right), \mathbf{u}\left(t\right)\right), \\ \mathbf{y} &= \mathbf{h}\left(t, \mathbf{x}\left(t\right), \mathbf{u}\left(t\right)\right) \end{aligned} \tag{6}$$

7 Conclusion

User dependence on ICT is rising, primarily because of ever-increasing number of customers that use and rely on electronic services. The value of electronic business is also rising with it and the amount of personal information on Internet is nowadays greater than ever before. Secondarily, the complexity of ICT is increasing. As a consequence, it is more and more difficult to assure security requirements for such systems. Furthermore, some traditional risk assessment techniques are no longer satisfactory for efficient risk management.

These factors together with the fact that exposed assets can be exploited automatically, remotely and with low risk, increasingly attract threat agents in cyberspace. Recent attacks on industrial infrastructure in 2010-2011 revealed that the attacks are becoming more advanced and targeted. Attackers also make great profits because risk management is reactive rather proactive. Thus, risk management paradigm has to change in order to increase odds of a timely risk identification and incident prevention.

In this section, we present a computerized risk management approach that supports active risk management and is architecturally aligned with MITRE's initiative. We argue that quantitative methods should be always preferred over qualitative in order to improve accuracy of risk assessment and efficiency of risk management. Thus, our approach is based on quantitative methods (DVE and SIF) and uses quantitative measurements provided by NVD and monitoring agents in observed system. Self-adapting security information and event management systems will be successful only if accurate information security feedback is provided.

References

1. Bellovin, S.M.: On the Brittleness of Software and the Infeasibility of Security Metrics. IEEE Security & Privacy Magazine 4(4), 96–96 (2006)
2. Centre for Secure Information Technologies: The World Cyber Security Technology Research Summit Report. Belfast (2011)
3. Cox, L.A.T., Babayev, D., Huber, W.: Some limitations of qualitative risk rating systems. Risk Analysis: An Official Publication of the Society for Risk Analysis 25(3), 651–662 (2005)
4. Gerber, M., von Solms, R.: Management of risk in the information age. Computers & Security 24(1), 16–30 (2005)
5. Hariri, S., Dharmagadda, T., Ramkishore, M., Raghavendra, C.S.: Impact analysis of faults and attacks in large-scale networks. IEEE Security & Privacy Magazine 1(5), 49–54 (2003)
6. HIPAA, Basics of Risk Analysis and Risk Management. Washington, USA (2005)
7. ISO/IEC 15408-1:2009, Information technology - Security techniques - Evaluation criteria for IT security - Part 1: Introduction and general model. ISO/IEC (2009)

8. ISO/IEC 21827:2008, Information technology - Security techniques - Systems Security Engineering - Capability Maturity Model (SSE-CMM). ISO/IEC (2008)
9. ISO/IEC 27000:2009, Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC (2009)
10. ISO/IEC 27001:2005, Information technology - Security techniques - Information security management systems - Requirements. ISO/IEC (2005)
11. ISO/IEC 27002:2005, Information technology - Security techniques - Code of practice for information security management. ISO/IEC (2005)
12. ISO/IEC 27005:2008, Information technology - Security techniques - Information security risk management. ISO/IEC (2008)
13. ISO/IEC TR 15443-2:2005, Information technology - Security techniques - A framework for IT security assurance - Part 2: Assurance methods (2005)
14. Jones, J.R.: Estimating Software Vulnerabilities. IEEE Security & Privacy Magazine 5(4), 28–32 (2007)
15. Martin, R.A.: Making security measurable and manageable. In: MILCOM 2008 - 2008 IEEE Military Communications Conference, pp. 1–9 (2008)
16. McHugh, J., Fithen, W.L., Arbaugh, W.A.: Windows of vulnerability: a case study analysis. Computer 33(12), 52–59 (2000)
17. Mell, P., Scarfone, K., Romanosky, S.: Common Vulnerability Scoring System. IEEE Security & Privacy Magazine 4(6), 85–89 (2006)
18. MITRE Corp., Common Vulnerabilities and Exposures: The Standard for Information Security Vulnerabilities Names, `http://cve.mitre.org/` (accessed: November 19, 2011)
19. NIST, National Vulnerability Database: automating vulnerability management, security measurement, and complience checking, `http://nvd.nist.gov/` (accessed: November 19, 2011)
20. NIST, Security Content Automation Protocol Validated Products (2011), `http://nvd.nist.gov/scapproducts.cfm` (accessed: November 27, 2011)
21. NIST SP 800-126, The Technical Specification for the Security Content Automation Protocol (SCAP): SCAP Version 1.1 (DRAFT), NIST (2010)
22. Schneier, B.: Attack trees. Dr. Dobb's Journal (12), 21–29 (1999)
23. Stevens, S.S.: On the Theory of Scales of Measurement. Science 103(2684), 677–680 (1946)
24. Trček, D.: Security Metrics Foundations for Computer Security. The Computer Journal 53(7), 1106–1112 (2009)
25. Trček, D.: Computationally Supported Quantitative Risk Management for Information Systems. In: Gülpnar, N., Harrison, P., Rüstem, B. (eds.) Performance Models and Risk Management in Communications Systems (Springer Optimization and Its Applications), p. 258. Springer (2010)