# Security Assessment of Computer Networks Based on Attack Graphs and Security Events

Igor Kotenko, Elena Doynikova

# Security Assessment of Computer Networks based on Attack Graphs and Security Events

Igor Kotenko[1] and Elena Doynikova[1]

[1] Laboratory of Computer Security Problems
St. Petersburg Institute for Informatics and Automation (SPIIRAS)
39, 14 Liniya, St. Petersburg, Russia
{ivkote, doynikova}@comsec.spb.ru

**Abstract.** Security assessment is an important task for operation of modern computer networks. The paper suggests the security assessment technique based on attack graphs which can be implemented in contemporary SIEM systems. It is based on the security metrics taxonomy and different techniques for calculation of security metrics according to the data about current events. Proposed metrics form the basis for security awareness and reflect current security situation, including development of attacks, attacks sources and targets, attackers' characteristics. The technique suggested is demonstrated on a case study.

**Keywords:** cyber situational awareness, security metrics, security metrics taxonomy, attack graphs, SIEM-systems.

## 1 Introduction

Analysis and enhancement of the information security of the computer networks and systems is widely researched area. One of the essential aspects in this area is security evaluation that includes calculation of different security metrics. Calculation of security metrics is most relevant when it is solved in real-time (or near real-time) mode, which is specific to Security Information and Event Management (SIEM) systems [13]. Obviously these metrics should be clear and valuable for security decisions.

Currently there is a lot of investigations that consider different security assessment techniques and security metrics [1-6, etc.]. In the paper we aim to develop an approach intended for near real-time security metrics calculation. This approach should allow taking into account new security information and events that appear in the network operation process and fulfilling appropriate recalculation of security metrics. For this goal we developed the metrics taxonomy that considers the following aspects: recent research in the security metrics area; modeling of attacker steps as attack graphs; goals and characteristics of SIEM systems. For calculation of security metrics we use known and adopted techniques. On the base of these metrics, we determine current security situation, including existence of attacks, attacker skills and position, possible previous and future attacker steps and attack target. The main contribution of the paper is the developed metrics taxonomy and its application for security assess-

ment of computer networks based on attack graphs. The key feature of the technique suggested is taking into account current security information and events.

The paper is organized as follows. *Section 2* outlines main related works. *Section 3* describes the common idea of the assessment technique and its stages. *Section 4* presents case study and experiments for evaluating the security assessment technique. Conclusion analyzes the paper results and provides insight into the future research.

## 2 Related Work

Currently there is a multitude of security metrics taxonomies. We analyzed some of them and concluded that these taxonomies are defined according to the goals of the security assessment. For example, in [9] three categories are outlined: technical, operational and organizational. In [22] two categories are considered: organizational and technical. Taxonomy suggested by NIST [21] includes three categories: management, technical and organizational, and 17 sub-categories. In [20] the information assurance metrics taxonomy is defined. It includes three categories (security, quality of service, availability) and technical, organizational and operational metrics.

From another hand, there are classifications of security metrics according to the way of their measurement and computation. In [6] the metrics are divided on primary and secondary. In [11] metrics are classified on the metrics that are calculated for the attack graph (used to define, for example, attacker skill level, attack potentiality) and for the service dependencies graph (implemented to determine, for instance, attack/response impact or response benefit). The Center for Internet Security divides metrics according to six business functions [4]: incident management, vulnerability management, patch management, application security, configuration management, and financial metrics. In [2] eight categories of metrics are differentiated according to the value type: existence (indicator of whether something exists); ordinal (subjective qualitative measure); score (numeric values for qualitative measure); cardinal (number); percentage; holistic (based on external data sources); value (consider value loss); uncertainty (include stochastic or probabilistic aspect).

Nevertheless, we have not found an appropriate taxonomy of metrics based on attack graphs applicable for security assessment in SIEM systems. Thus, we aimed to develop the appropriate taxonomy taking into account the next aspects: contemporary research in the security metrics area [9, 10, 16, etc.]; characteristics of the architecture of the security analysis component in the scope of the SIEM system (modeling of the attack sequences on the base of attack graphs [8, 12, 17, 19] and service dependencies [10, 11]); different stages of security analysis (static and dynamic). We outlined the following categories: topological, attack, attacker, integral (system).

Topological characteristics can be defined from the network topology and the description of hosts [4, 15]. They involve host parameters [15], application characteristics [4], features about service dependencies [10, 11], characteristics that consider information about the vulnerabilities and possible attacks [4]. Attack characteristics (such as attack potentiality/probability) are defined on the base of attack graphs [10]. Attacker parameters are related to possible attackers and are considered in [3, 5, 10, 18]. Integral (system) characteristics involve features that define common security

estimations [5, 7, 13, 14]. From another hand, important aspects in our classification are cost-benefit analysis and analysis of zero-day attacks. Cost-benefit analysis is usually used for decision support and involves cost metrics that define costs of impacts and responses [8, 11]. For zero day attacks analysis, the metrics reflecting possible zero day attacks are used [1].

## 3 Security Assessment Technique

The component that implements the suggested security assessment technique is the part of the security evaluation system based on attack graphs [12]. The architecture of the component is presented in Fig. 1.

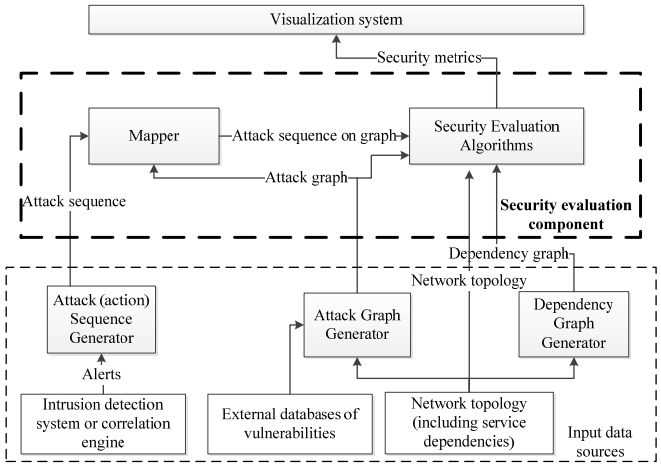


**Fig. 1 –** Architecture of the security evaluation component

The core of the component is the set of security evaluation algorithms for calculation of metrics. Other important subcomponent - Mapper - allows detecting attacker position on the base of security events and attack graph structure. Security evaluation component gets input data from different sources including: attack graph generator that builds attack graphs for the analyzed network; dependency graph generator that provides graph of the dependencies between the network services; and attack sequences generator that generates steps of the current attack on the base of the security alerts. Output data includes different security metrics according to the suggested taxonomy. Further output data is provided to the visualization system.

To describe the security assessment technique the following *input details* are used: (1) Test network with host characteristics and values of the topological metrics: *Business Value*, *Criticality* (including propagated criticality via service dependencies), etc.; (2) Attack graph that contains system vulnerabilities as vertexes and transitions between the vulnerabilities as arcs (these paths constitute threats). Possibility of transition from one vulnerability to another is defined by pre- and post-conditions of the vulnerabilities exploitation according CVSS [16]; (3) Calculated unconditional prob-

abilities for each node (in consideration that the attacker can implement all attack actions). Unconditional probabilities are defined on the base of the local conditional distributions for each node $S_i$, $i\epsilon[1,n]$: $Pr(S_1,\dots,S_n)=\prod_{i=1}^{n} Pr\,(S_i|Pa[S_i])$, where $Pa[S_i]$ - set of all parents of $S_i$. Conditional probabilities of the transitions between nodes are defined on the base of CVSS access complexity of the vulnerability; (4) Calculated risk values for each critical host for attack graph level (considering attack probability and possible impact); (5) Security events that include information about the attacked host, privileges and/or impact on the host.

The *security assessment technique* includes the following stages:

1. Definition of the attacker position on the attack graph on the base of the information from the security event. It can be done on the base of the next steps: Define the list of the vulnerabilities for the host which is described in the security event; Select the vulnerabilities that lead to the privileges and\or impact described in the event; If only one vulnerability was selected, the next steps of the technique should be performed for the node that corresponds to the exploitation of this vulnerability; If multiple vulnerabilities were selected, the next steps of the technique should be performed for all possible nodes; If a vulnerability was not selected, then the event is defined as exploitation of the zero-day.
2. Determination of the attacker skill level on the base of information from the security event. The next steps should be performed for all nodes selected on the previous stage: Define the most probable path of the attacker to the current node (on the base of the Bayes theorem); In case of multiple paths with the same probabilities, consider them all in further calculations; Select vulnerabilities with the maximum CVSS access complexity [16] for this path; Define the attacker skill level according to the access complexity as “High”/”Medium”/”Low”. Quantitative values are defined: 0.7 - “High”, 0.5 - “Medium”, 0.3 - “Low” *Attacker Skill Level*; Define the probability of skills as *(number of nodes with vulnerability with this access complexity)/(total number of steps in the path)*.
3. Calculation of the probabilities of the paths that go through the node that corresponds to the attacker position. On this step the next features should be considered: defined attacker skill level and that the probability of the compromise of this node is equal to 1.
4. Definition of the risks for the attack paths that go through the compromised node (based on the target asset criticality, attack impact and attack path probability).
5. Selection of the path with maximum value of risk. This path is selected as the most probable attack path and its end point should be selected as attacker goal.

As the result of the technique, we get the next output data: attacker skill level, attack path and attackers goal. Further this information is used for the decision support.

# 4 Case Study

## 4.1 Input Data Gathering

Let us consider the following input data used for the security assessment: topology of the test network (Fig. 2), values of the topological metrics, especially *Criticality* of the hosts (calculated on the previous assessment stage), attack graph, security events.

Host-1 and Host-2 are web-servers with critical web applications. External users of the local network are directed to the web-applications through Router-1 and Firewall-1 to Host-1 or Host-2. Authentication is needed to work with these applications. Authentication data is stored on the Authentication server. Critical data that the user get or add when working with applications is stored on Database server. Requests from Host-1 and Host-2 are handled by Web-server first. Internal users have access to Web-server via Router-2 and Firewall-3. The parameters of the hosts for the test network are as follows: (a) *External users* - Microsoft Windows 7 64-bit, Apple ITunes 9.0.3, Microsoft Office 2007 SP1, Microsoft Internet Explorer 7; (b) *Web-server* - Windows Ftp Server 2.3.0, Windows Server 2008 for 32-bit Systems; (c) *Database server* - Apache Software Foundation Derby 10.1.3.1, phpMYAdmin 3.5.2.2, Oracle MySQL 5.5.25, Linux Kernel 2.6.27.33; (d) *Host-1 u Host-2* - Red Hat JBoss Community Application Server 5.0.1, Windows Server 2008 R2 for x64-based Systems; (e) *Firewall-1, Firewall-3* - Linux Kernel 2.6.27.33, Citrix ICA Client; (f) *Firewall-2* - Novell SUSE Linux Enterprise Server 11 Service Pack 1 (with Netfilter),; (g) *Authentication server* - Novell SUSE Linux Enterprise Server 11 Service Pack 1, Novell eDirectory 8.8.1; *Internal users* - Apple Mac OS X Server 10.6.1, Apple iTunes 9.0.2 for Mac OS X, Microsoft Office 2008 Mac.

Fig. 2 depicts the values of the host *Criticality*. It is calculated on the base of the *Business Value* of the hosts for the system and the dependencies between the network services. *Criticality* is a vector that includes three scores <*Criticality of Confidentiality*, *Criticality of Integrity*, *Criticality of Availability*>.

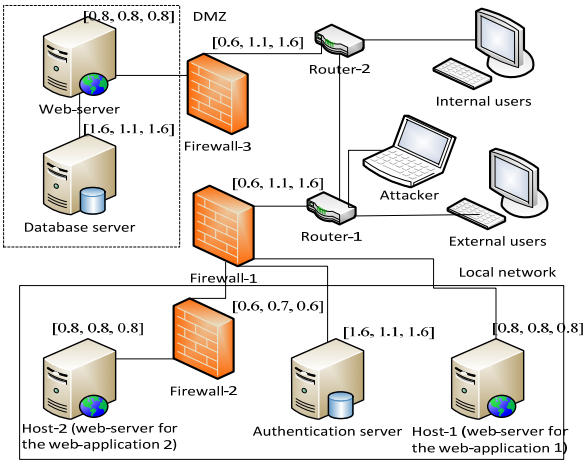


**Fig. 2.** Topology of the test network and *Criticality* values

The example of the user interface for the security evaluation system, which outlines the metrics values, is shown in Fig. 3 [12]. Common attack graph for the considered test case is presented in Fig. 4. Nodes of the attack graphs are defined as triple <Exploited vulnerability, Pre-conditions, Post-conditions>. Pre-conditions include privileges that are needed to exploit the vulnerability, Post-conditions are acquired

privileges and impact. For each node of the attack graph the appropriate vulnerabilities (according to the NVD database) are represented. Color of the node is defined with vulnerability BaseScore according to the CVSS [16] (yellow color - for the Medium score, red color - for the High score). For each node the probabilities that attacker can reach the node are calculated.

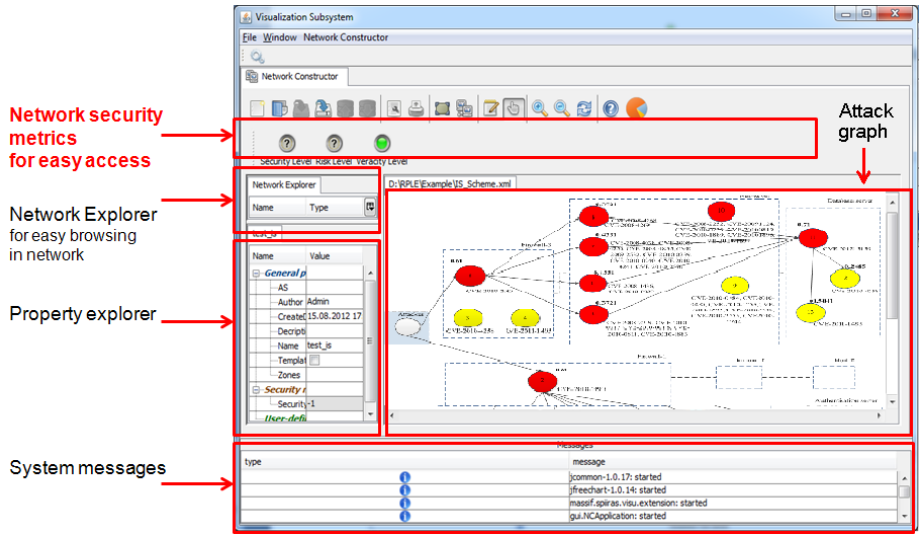


**Fig. 3.** Example of the user interface

For example, conditional probability on the node 1 in case of successful initialization of attack is equal to 0,61 (the access complexity of the CVE-2010-2990 is 0,61). Conditional probability on the node 6 in case of the success on the node 1 is equal to 0,71 (the access complexity of the CVE-2008-1436 is 0,71). Unconditional probability for the node 6 is defined as product of probabilities of successful states: $1 \cdot 0{,}61 \cdot 0{,}71 = 0{,}4331$.

As was defined above the description of the security event should include information about the attacked host and acquired privileges and/or impact.

To illustrate the experiments in the paper, two types of attackers were defined:

1. *Attacker with "Medium" attacker skill level*. He (she) has external access and some information on the network topology. This attacker can use exploits of known vulnerabilities with "Medium" access complexity. His (her) goal is to get data from the database. The sequence of such actions is represented with yellow color. We define the following events for this case as example: **event1** – malicious activity is detected on step 1, it contains the information on illegitimate admin access on the Firewall-3; **event2** – malicious activity on step 2, it contains the information on illegitimate admin access on the Web-server.
2. *Attacker with "High" attacker skill level*. He (she) has external access and no information about network topology. This attacker can exploit a zero-day vulnerability. His (her) goal is to compromise web-application on Host-2. The sequence

of such actions is outlined with red color. We define the following events for this case as example: **event1** - malicious activity is detected on step 1, it contains the information about illegitimate admin access on the Firewall-1; **event2** - malicious activity on step 2, it contains the information about illegitimate admin access on the Firewall-2; **event3** - malicious activity is detected on step 3, it contains the information about illegitimate admin access on the Host-2; **event4** - malicious activity is detected on step 4, it contains the information about violation of confidentiality, integrity or availability on the Host-2.

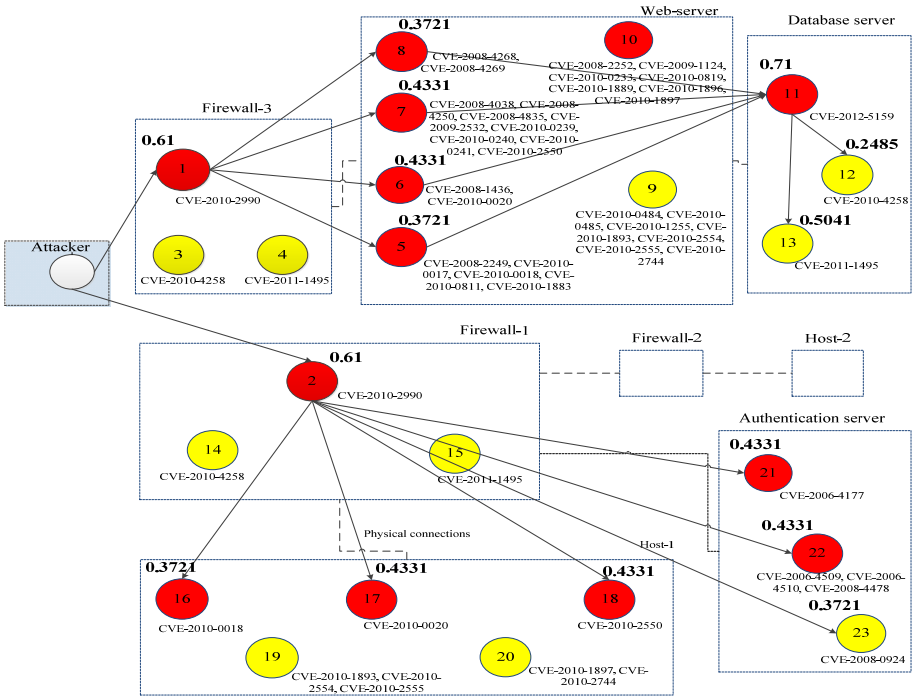


**Fig. 4.** Attack graph with calculated probabilities

## 4.2 Security Assessment Implementation

Let us go through the steps of the technique suggested for the described test case:

1. Definition of the node of the graph which corresponds to the attacker position. For example, for the first scenario to detect the attacked node after event1 we determine all vulnerabilities on the Firewall-3 defined in the event and then select vulnerabilities that provide privileges/impact described in the event. For the first scenario it is still node '1'.
2. Calculation of the attacker skill level on the base of the security event. For the nodes defined on the previous stage, the previous attacker steps are defined, i.e. the attack sequence on the attack graph with the maximum probability value. For the first scenario after event1 there is only one possible previous node – external

network, and only one exploited vulnerability – 1. On the base of the performed steps the attacker skill level is a maximum access complexity of them.

3. Determination of the probabilities of the attack sequences that go through the node with attacker and definition of the attacker goal. For the first scenario, according to event1, new probabilities are calculated: the probabilities on the nodes 5-8 are decreased, as from the one hand they were influenced by the new knowledge about the attacker position, but from another - by new knowledge about attacker skills. Also probabilities of the attacks on the nodes 2, 16-81, 21-23 are decreased, because of the new knowledge about attacker skills. Thus, after the first security event we can suppose that attack goal is Database Server, but additional information is needed. Fig. 5 depicts appropriate probabilities after each defined security event for the first scenario. Fig. 6 outlines the same calculations made for the second scenario.
4. Definition of the risks of the attack sequences. On this step the *Criticality* values are considered. Cumulative risk values for the graph nodes are represented in Fig. 6 (with new events the risk on the attacker goal node increases).

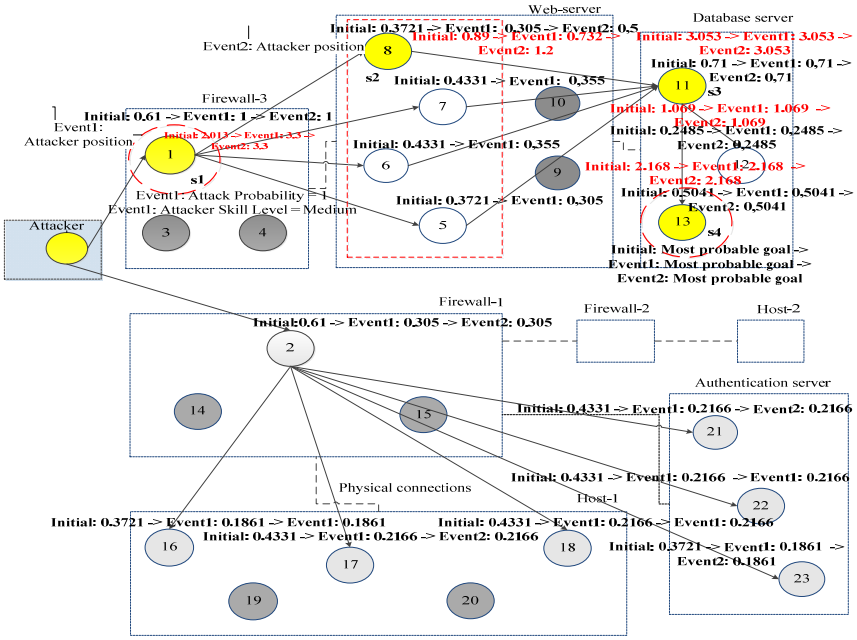


**Fig. 5.** Changes of attack probabilities after security events for the scenario 1

Output of the security assessment technique contains the following data: attack path with maximum risk value that defines the most probable attack sequence and attackers goal; the most probable previous attacker steps; attacker skills. These results allow making decision about the most efficient countermeasures. These experiments demonstrate the main possibilities of the suggested security evaluation system on security metrics calculation.

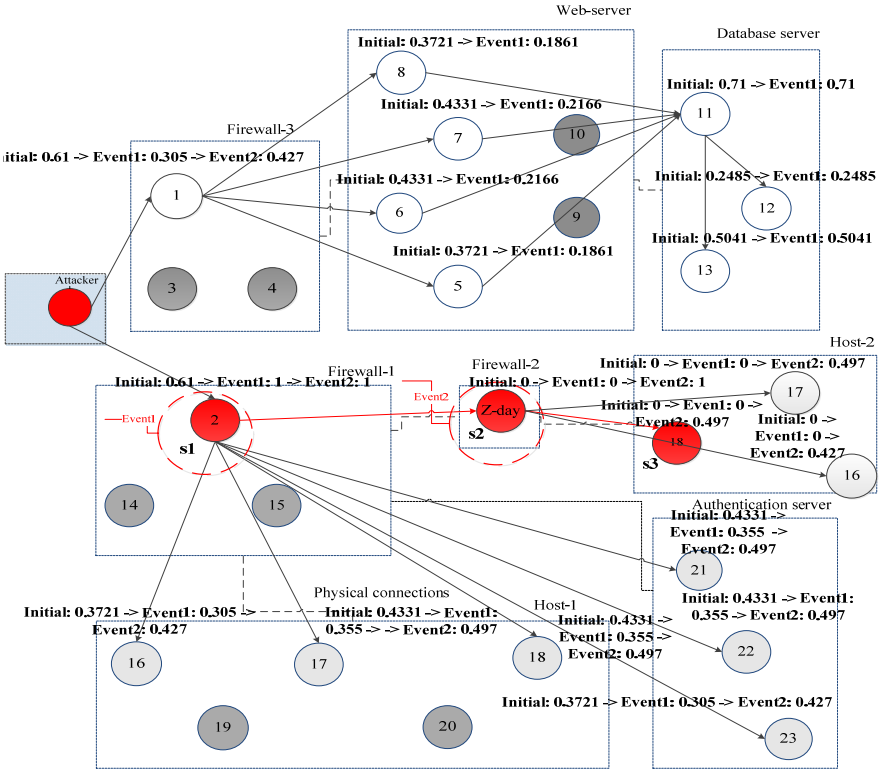


**Fig. 6.** Changes of attack probabilities after security events for the scenario 2

## 5 Conclusion

In the paper we suggested and analyzed the application of the security assessment technique for computer networks. It is oriented on near real time situation assessment, when we can monitor the current attacker position and his (her) path in the network, but have hard time limitations for calculations.

We defined the set of security metrics and traced their changes after appearance of security events. On the example of the case study it was shown that probability and risk of the attacker path increases with new data and allows defining the track of the attacker in the system. The limitations of the paper volume do not allow discussing proposed system of security metrics and techniques of their calculation in details.

The future research will be devoted to further specification of the technique and extension of the experiments.

**Acknowledgements.** This research is being supported by grants of the Russian Foundation of Basic Research (13-01-00843, 13-07-13159, 14-07-00697, 14-07-00417) and the Program of fundamental research of the Department for Nanotechnologies and Informational Technologies of the Russian Academy of Sciences (contract #2.2).

## References


1. Ahmed, M. S., Al-Shaer, E., Khan, L.: A Novel Quantitative Approach for Measuring Network Security. INFOCOM'08, pp.1957-1965 (2008)
2. Axelrod, C. W.: Accounting for Value and Uncertainty in Security Metrics. Information Systems Control Journal, vol.6, pp.1-6 (2008)
3. Blakely, B. A.: Cyberprints Identifying Cyber Attackers by Feature Analysis. Doctoral Dissertation: Iowa State University (2012)
4. The Center for Internet Security, The CIS Security Metrics (2009)
5. Dantu, R., Kolan, P., Cangussu, J.: Network Risk Management Using Attacker Profiling. Security and Communication Networks, vol.2, No.1, pp. 83-96 (2009)
6. Idika, N.C.: Characterizing and Aggregating Attack Graph-Based Security Metric. PhD Thesis, Purdue University, pp.1-131 (2010)
7. ISO/IEC 27005:2008, Information technology — Security techniques — Information security risk management (2008)
8. Jahnke, M., Thul, C., Martini, P.: Graph-based Metrics for Intrusion Response Measures in Computer Networks. IEEE Workshop on Network Security (2007)
9. Henning, R. et al.: Workshop on Information Security System, Scoring and Ranking ("Security Metrics"), MITRE, Williamsburg, Virginia (2002)
10. Kanoun, W., Cuppens-Boulahia, N., Cuppens, F., Araujo, J.: Automated Reaction Based on Risk Analysis and Attackers Skills in Intrusion Detection Systems. CRiSIS'08. Toezer, Tunisia, pp.117-124 (2008)
11. Kheir, N., Cuppens-Boulahia, N., Cuppens, F., Debar, H.: A Service Dependency Model for Cost-Sensitive Intrusion Response. ESORICS'10, pp.626-642 (2010)
12. Kotenko, I., Chechulin, A.: A Cyber Attack Modeling and Impact Assessment Framework. CyCon'2013. IEEE and NATO COE Publications, pp. 119-142 (2013)
13. Kotenko, I., Saenko, I., Polubelova, O., Doynikova, E.: The Ontology of Metrics for Security Evaluation and Decision Support in SIEM Systems. RaSIEM 2013 (2013)
14. Manadhata, P. K., Wing, J. M: An Attack Surface Metric. IEEE Transactions on Software Engineering, pp.371-386 (2010)
15. Mayer, A.: Operational Security Risk Metrics: Definitions, Calculations, Visualizations. Metricon 2.0. CTO RedSeal Systems (2007)
16. Mell, P., Scarfone, K., Romanosky, S.: A Complete Guide to the Common Vulnerability Scoring System Version 2.0 (2007)
17. Moore, A. P., Ellison, R. J., Linger, R. C.: Attack Modeling for Information Security and Survivability. Technical Note CMU/SEI-2001-TN-001. Survivable Systems (2001).
18. NMap reference guide http://nmap.org/book/man.html
19. Poolsappasit, N., Dewri, R., Ray, I.: Dynamic Security Risk Management Using Bayesian Attack Graphs. IEEE Transactions on Dependable and Security Computing, vol.9, No.1, pp.61-74 (2012)
20. Seddigh, N., Pieda, P., Matrawy, A., Nandy, B., Lambadaris, I., Hatfield, A.: Current Trends and Advances in Information Assurance Metrics. Proc. of the 2nd Annual Conference on Privacy, Security and Trust (PST 2004), Fredericton, NB, Oct. (2004)
21. Swanson, M., Bartol, N., Sabato, J., Hash, J., Graffo, L.: Security Metrics Guide for Information Technology Systems. NIST Special Publication 800-55, Jul. (2003)
22. Vaughn, R., Henning, R. and Siraj, A.: Information Assurance Measures and Metrics: State of Practice and Proposed Taxonomy. Proc. of 36th Hawaii Int. Conf. on System Sciences HICSS 03 (2003)