computing@computingonline.net
www.computingonline.net

ISSN 1727-6209
International Journal of Computing

COMPREHENSIVE MULTILEVEL SECURITY RISK ASSESSMENT OF DISTRIBUTED INFORMATION SYSTEMS

Igor Kotenko and Elena Doynikova

St. Petersburg Institute for Informatics and Automation of Russian Academy of Sciences (SPIIRAS)
39, 14 Liniya, St. Petersburg, Russia
ivkote@comsec.spb.ru, http://www.comsec.spb.ru/kotenko/
doynikova@comsec.spb.ru, http://www.comsec.spb.ru/doynikova/

Abstract: The paper suggests the multilevel approach to the risk assessment that is based on the system of security metrics and techniques for their calculation. Proposed techniques are based on attack graphs and service dependencies. They allow evaluating security of network topologies, malefactors and attack characteristics, and integral security properties and characteristics calculated on the basis of the cost-benefit and zero-day vulnerability analysis. Classification of these characteristics and separation of the security information on static, dynamic and historical allows defining different assessment levels. The paper considers the main issues and recommendations for using the risk assessment techniques based on the suggested approach. *Copyright © Research Institute for Intelligent Computer Systems, 2013. All rights reserved.*

Keywords: Cyber security, security metrics, risk assessment, attack graphs, service dependencies.

1. INTRODUCTION

Information risk management is an important aspect of operation of modern complex distributed information systems.

For effective security decisions it is necessary to get accurate and actual information about security state of the system.

Different security metrics can provide this information. Calculation and analysis of security metrics are involved in the risk assessment process as part of the risk management process.

There are a lot of security metrics that are related to the different aspects of the security of the distributed systems [1, 3, 4, 7, 11, 12, etc.]. This paper proposes the integrated system of security metrics and techniques for their calculation.

Main elements of the suggested approach include analysis of the static, dynamic and historical security information, calculation of security metrics on the base of attack graphs and service dependencies, usage of the standards of the Security Content Automation Protocol (SCAP) to represent data about system platforms, applications and configurations in unified form and to assess vulnerabilities.

The approach is based on taking into account the current research in the area of security metrics.

Proposed metrics allow evaluating a set of parameters: the security level of network topologies, malefactors and attack characteristics, and integral security properties calculated on the basis of the cost-benefit and zero-day vulnerability analysis.

We define several assessment levels according to the type of the analyzed characteristics and used data – a topological, an attack graph, a malefactor, events and the whole system. Each of the level contains risk assessment metrics that we propose to calculate. Such approach allows assessing risk on different stages of the system operation and getting time-dependent results. Also the paper discusses the most characteristic techniques that allow evaluating the proposed metrics with different accuracy: express risk assessment static technique, performance-based technique and technique based on historical data.

The express risk assessment technique allows simple and quick assessment of the security level of the system in the static operation mode. The performance-based technique permits assessment of the security level in the operation mode according to the detected security events. The technique based on the historical data allows detailed assessment with consideration of the data about previous security incidents.

One of the main problems in the risk assessment is the lack of data on the security incidents. We use Common Vulnerabilities Scoring System (CVSS) [29] scores as basis for calculations of the security metrics. But it is still heuristic assessments. To manage uncertainty we use Bayes techniques and consider possibility of zero-day vulnerabilities that are not included to the Common Vulnerabilities and Exposures (CVE) [9] database.

This paper is an extended version of the paper presented on IDAACS'2013 [21]. It structured as follows. *Section 2* reviews related works in the area of security metrics. On the base of the review we outline the classes of known security metrics (topology, malefactor, and attack characteristics), consider integral metrics, and also metrics calculated on the basis of the cost-benefit and zero-day vulnerability analysis. The proposed hierarchical security assessment framework allows to evaluate the considered system from different aspects and to specify the risk value according to the available data. *Section 3* describes requirements to the suggested approach and proposes the system of security metrics. *Section 4* considers the techniques that are suggested for evaluation of the proposed security metrics. *Conclusion* outlines main results of the work and directions of future research.

2. RELATED WORK

There is the number of different *classifications of the security metrics* according to their goals, way of computation or value types.

For example, The Center for Internet Security (CIS) divides metrics according to six business functions [7]: 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). In [14] metrics are divided according to the way of computation on primary (calculated on the base of the attack graphs or service dependencies graphs) and secondary (calculated on the base of the primary metrics).

In [18] metrics are distinguished according to the used model: logical dependencies graph (used to define, for example, attacker skill level, attack potentiality) and service dependencies graph (used to define, for instance, attack/response impact, response benefit).

Based on the current research in the area of security metrics we outline the following main groups of metrics: topology characteristics, malefactor characteristics, attack and response characteristics, system characteristics (integral metrics), cost characteristics and characteristics that are used in analysis of the zero-day vulnerabilities.

Topology characteristics are considered, for example, in [28] and [7].

In [28] the following metrics are outlined: *Host Criticality* (impact from loss of the host to the business), *Exposure* (it is defined by the reachability of the host and easiness to exploit the vulnerabilities on the host), *Business Value* (it is similar to *Criticality*, but expressed in monetary units), *Risk* (it is defined by *Exposure* and *Business Value*) and *Downstream Risk* (it is cumulative risk over the hosts attackable from the current host).

In [7] the topology metrics from the applications point of view are suggested – *Number of Applications*, *Percentage of Critical Applications*, and topology characteristics that consider information about vulnerabilities – *Percent of Systems Without Known Severe Vulnerabilities*, *Mean-Time to Mitigate Vulnerabilities*, *Number of Known Vulnerability Instances*, and topology characteristics that consider information about attacks – *Severity* of the vulnerability and its *Access Complexity*, that can be considered when the attack likelihood is calculated.

One of the most important *malefactor characteristics* is *Attacker Skill Level*, which is considered in [17] and [32]. It is valuable indicator about the attacker ability to carry-on an attack scenario and thus to attain his objectives.

In [10] calculation of the risk level on the base of the malefactor behavior is proposed. In some other papers, for example, in [5], attack attribution metrics are considered (the concrete actors involved, equipment and tools used, geographic position, motives, etc.).

Attack characteristics include *Attack Potentiality* (dynamic metric that is computed with respect to the attacker position in the attack graph).

In [35] *Attack Potentiality* is defined on the base of the *Confidence Level* metric – a confidence level in the fact that attack is in progress.

In [38] *Compromised Confidence Index* is suggested.

In [1, 16, 19, 36] another attack characteristic is proposed – *Attack Impact*. In [16, 19, 38] such *response metrics* as *Response Efficiency*, *Benefit of the Response* and *Response Collateral Damage* are considered.

Two main metrics should be outlined to consider the total *risk level* of the system (i.e. *integral metrics*): *Attack Surface* (it is defined on the base of the *Damage Potential-Effort Ratio* metric) [27] and *Security Level* [10, 15, 20, 22, 23, 35].

For the *cost-benefit analysis* the following metrics can be used: *Net Benefit* (total benefit in case of implementation of safeguard), *Annual Loss*

Expectancy (product of an incident's annual frequency times its total losses) [13], and *Return on Response Investment* [19].

Metrics that are used in the *analysis of zero-day vulnerabilities* involve *Probabilistic Vulnerability Measure* [1], which defines how likely the vulnerability will be released for a service over some period and the vulnerability's expected severity, and *k-zero day safety*, which defines network resistance to zero-day vulnerabilities [37].

3. THE SYSTEM OF SECURITY METRICS

We define the classification of security metrics on the base of the review above. Classification of security metrics is demonstrated in Fig. 1 and includes the following classes of security metrics:

(1) Host/topology characteristics;

(2) Malefactor characteristics (define malefactor skills, position etc.);

(3) Attack characteristics (define attack potential and possible impact);

(4) System characteristics (define integral security characteristics);

(5) Zero-days characteristics (define possibility of zero-day attacks);

(6) Cost-benefit characteristics (define cost of the attack and response).

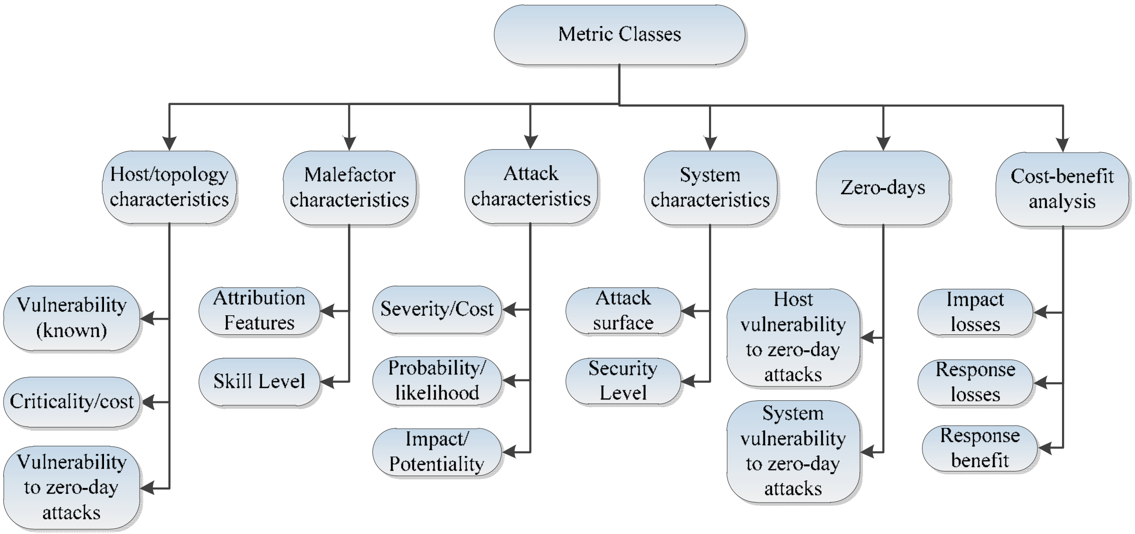

Fig. 1 – Classes of metrics

The system of security metrics as proposed in this paper is designed for the risk assessment approach that involves the next stages:

(1) generation of the attack and service dependency graphs on the base of the data about the network topology;

(2) consideration of the malefactor skills and position and generation of the profile attack graphs;

(3) analysis of the system events to monitor current security situation;

(4) calculation of security metrics on the base of this data.

This approach is implemented in the *Security Evaluator* [22-25].

We propose to use the SCAP protocol and particular standards included to this protocol [34] to present input security data for the *Security Evaluator*. SCAP, produced by the National Institute of Standards and Technologies (NIST) [30], includes a collection of specifications intended to standardize the way the security software solutions communicate software security flaw and configuration information.

SCAP contains the following standards: Common Configuration Enumeration (CCE) specifies features of the configurations that negatively influence the system security [6], Common Platform Enumeration (CPE) allows to create the list of the used platforms and applications [8], CVE allows to specify the list of the vulnerabilities, CVSS assesses negative influence of the configurations and vulnerabilities that allows the most critical vulnerabilities to be defined. CPE, CVE and CVSS are used for the attack graph generation.

Besides the configuration information, the list of used platforms and applications and the list of vulnerabilities, the input data includes software weaknesses represented by the Common Weakness Enumeration (CWE) standard, attack patterns specified using the Common Attack Pattern Enumeration and Classification (CAPEC) standard, security remediations in the format of the Common Remediation Enumeration (CRE) standard, security events in the Common Event Expression (CEE) format, the service dependencies (allow to define impact propagation), security policies, malefactor models, etc.

Results of the processing of *Security Evaluator* include: attack graphs; calculated security and exposure metrics (some of them are calculated on the base of the attack graph); countermeasures (are defined on the base of the calculated security and exposure metrics).

Input and output information for the suggested *Security Evaluator* is outlined in Fig. 2.

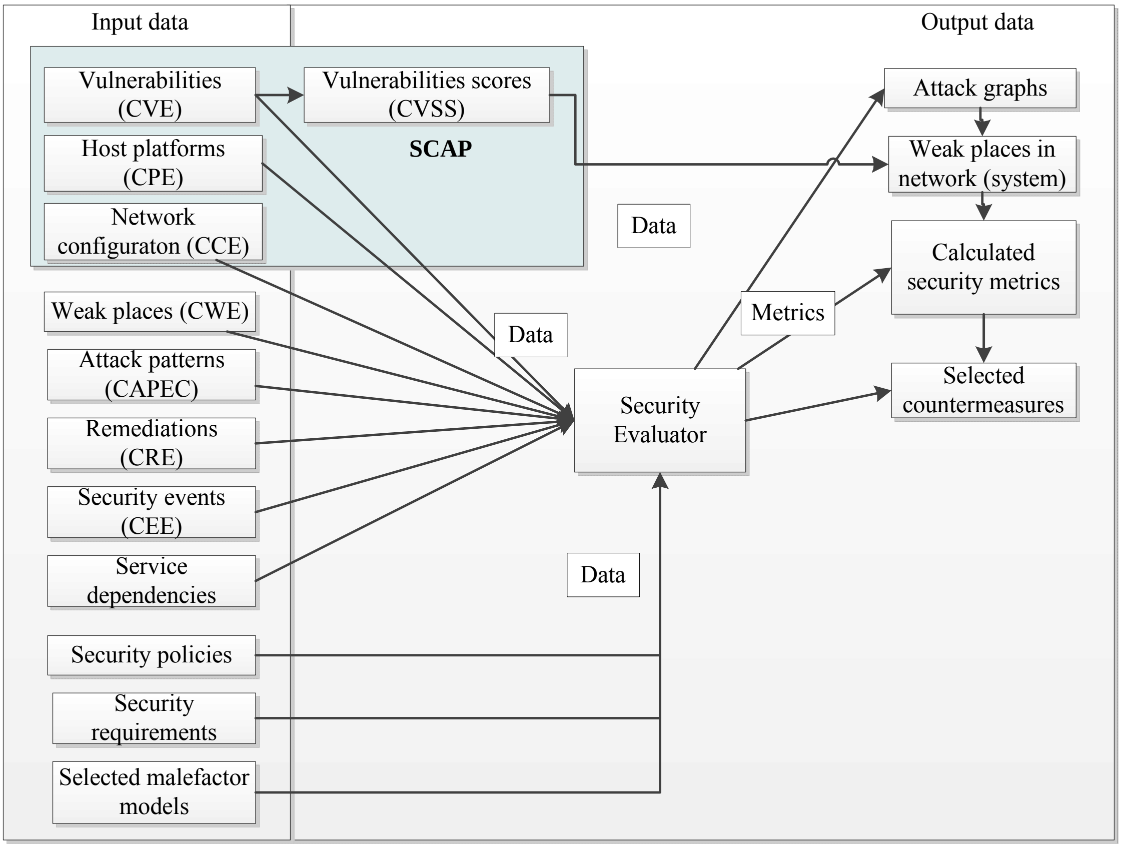

Fig. 2 – Data transformations in Security Evaluator

In process of security metrics development we considered the state-of-the-art in security metrics research as well as the architecture of the *Security Evaluator*.

Offered techniques cover two operation modes of the security evaluation system: online and offline.

The online mode stipulates limitations on the calculation time; however, it takes into account the current security situation (events, system configuration, etc.). So we can monitor position and skills of malefactor, and we can define the direction of the attack more carefully.

Off-line mode has no hard time limitations. In this case, historical data are used, and attack graphs are analyzed. This mode allows making a more profound and detailed risk assessment, as it applies more meaningful metrics that characterize the malefactor and attacks. Besides, computations of this level can be used as the base for the on-line mode.

On the base of the considered aspects we can arrange security metrics in our framework by levels, as it is shown in Fig. 3.

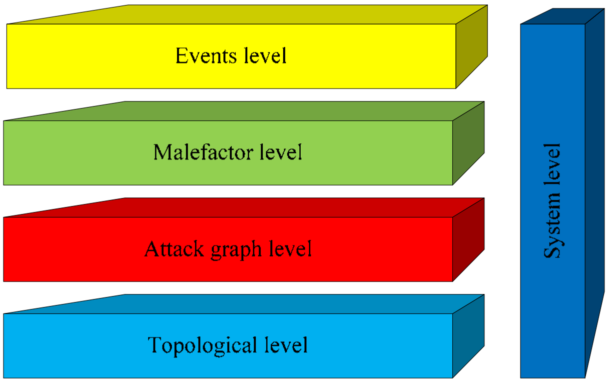

Fig. 3 – Levels of the suggested framework

Metrics of the higher levels are defined on the base of metrics of the lower levels, except for the system level metrics that are specified on each level via metrics of the appropriate level:

- *Topological level* – metrics of this level can be calculated by the administrator on the base of the system topology. We consider the following examples of metrics of this level: vulnerability level of host, criticality level of host and vulnerability of host to the zero-day attacks.

- *Attack graph level* – on this level we consider information from the attack graph for the metrics generation. The metrics of this level are *Attack Likelihood* and *Attack Impact* (in this case the impact is defined only by the target criticality and the attack severity). When presenting the attack graph to the user we can highlight the most critical attack paths (from the risk level point of view, i.e. combination of the attack probability and attack impact).
- *Malefactor level* – on the base of the metrics of this level the dependency from the malefactor profile is introduced (including his position and skills), this allows presenting the profile attack graph [10], which includes only attacks that can be implemented by the appropriate malefactor.
- *Events level* – this level is actual, when the Security Evaluator works in online mode (in real time), because on this level the security events are considered. It allows monitoring attack deployment and malefactor profile according to incoming events. When new events come, we can represent the current position of the malefactor (host and access rights) on the attack graph and possible attack paths (all possible paths and the most probable).
- *System level* – *Common Security Level* of the system and *Attack Surface* are defined on this level. One more common metric that can be used on this level is the resistance to zero day attacks. Approach to computation of these metrics depends on taken into consideration parameters, thus it differs for all upper levels.

The values of metrics calculated on the lower levels are specified with new data, for example, the probability of the attack becomes higher if we get a security event that confirms appropriate attack.

4. THE RISK ASSESSMENT TECHNIQUES

Fig. 4 depicts all levels described above and their relation to the appropriate security metrics.

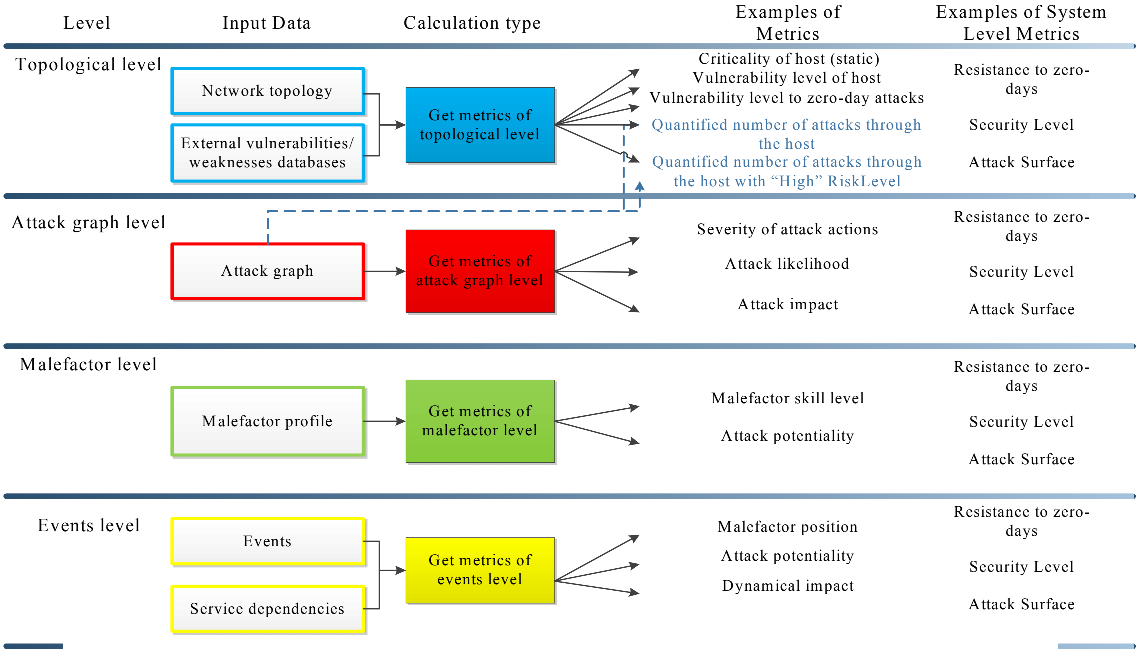

Fig. 4 – Security metrics and assessment levels

For the *topological level* we outline several host/system metrics that can be useful for the administrator and can be applied as base metrics (metrics that are used in calculations of another metrics) on the other levels. The examples of these metrics are as follows:

- *Criticality of Host* (or *Host Criticality*) gives information about the host criticality, can be defined for example on the base of CVSS (High, Medium or Low);
- *Vulnerability Level of Host* (or *Host Vulnerability*) (this metric can consist of the several values, for example, number of known vulnerabilities for the host, number of vulnerabilities with "High" CVSS *BaseScore*, etc. These values can be determined on the base of the CIS metric *Number of Known Vulnerability Instances* (*NKVI*), CVE and NVD);
- *Vulnerability Level to Zero-day Attacks* (for example, number of weaknesses, number of weaknesses with "High" CWSS *BaseScore*, etc.

These values can be determined on the base of CWE). For this metric we can use two calculation techniques: (1) considering vulnerability to zero-days only for single host (*Host Weakness*), and (2) detecting integrated system resistance to zero-days (*Vulnerability to Zero-day Attacks*), as, for example, in [37];

- *Percent of Systems (hosts) Without Known Severe Vulnerabilities (PSWKSV)* or number of hosts with “High” criticality in the system, etc.

The following two metrics can be calculated after adding information about the attack graph:

- *Quantified Number of Attacks through the Host*, which is equal to (Number of attacks that go through the host)/(Total number of attacks in the graph);
- *Quantified Number of Attacks through the Host with “High” RiskLevel*, which is equal to (Number of attacks with “High” *RiskLevel* through the host)/(Total number of attacks with “High” *RiskLevel* in the graph).

For techniques of the *attack graph level* we outline the metrics that consider paths in the attack graph. Such type of techniques allows us to define the security level of the system rather simply without considering attacker skills and likelihood of ongoing attack. The following metrics can be used here:

- *Severity of Attack Actions* (“base” metric);
- *Attack Severity*;
- *Attack Complexity*;
- *Attack Likelihood* (here we consider static and statistical approaches);
- *Attack Impact* (as static impact).

Here we should note that on the base of these metrics the express risk assessment technique is suggested. This technique does not consider attacker skills and attack changes in time and dynamic impact, but has low computational complexity. It can be improved by using the metrics of malefactor and events levels.

Techniques of the *malefactor level* deal with attacker skills (static/ statistical/ historical) and attack probability.

Here we suggest using the following *techniques and their modifications*:

- *Assessment where a malefactor profile is set statically by an administrator*. On the base of the malefactor skill level it is possible to create the profile attack graphs and evaluate the system security for each group of malefactors;
- *Probability assessment that uses the attack graphs for attacks representation and the Bayesian inference for risk analysis* (to get probability of attacks on the base of the probability of malefactor skills) [10];
- *Historical data assessment* that considers historical data to get the posterior probability of the attacks [32].

At the *events level* the risk assessment techniques take into account the dynamic aspect of risk assessment, using information (from sensors, correlation or intrusion detection components) on new events, probability of false and missed alarms, etc. We suppose the techniques of this level should be based on the following metrics:

- Malefactor position and compromised hosts;
- *Attacker Skill Level* (dynamic metric) [16];
- *Attack Potentiality* (here the event-based [35] and historical data-based [38] techniques can be used);
- *Dynamical Attack Impact* on the base of service dependencies [19, 37] (here we also can add such metric for the host as availability);
- The risk of the event can be evaluated, for example, as in [26].

On the base of the considerations above we outlined *three risk assessment techniques*:

- Express risk assessment technique;
- Performance-based (dynamic) technique;
- Technique based on historical data.

The *express risk assessment technique* is used for the express risk evaluation. It is a static technique that incorporates qualitative and quantitative approaches to the risk assessment and allows defining the common security level of the system.

This approach considers traditional understanding of the risk as the result of probability of the threat and its consequences for the system.

To assess risk we use CVSS (to define criticality of the attack action) and procedures of the FRAP (Facilitated Risk Analysis Process) technique [31].

Technique includes definition of the severity levels for hosts and attack actions, calculation of the impact from the attack actions, calculation of the impact from threats realization and complexity of threats realization, then on the base of this data the risk level for all threats is determined, and common security level of the system is calculated.

Main difference of the *performance-based technique* is that fact that it is oriented on the real time situation, when we can monitor the current attacker position and his (her) path in the network, but have hard time limitations for calculations.

Main modules of the *Security Evaluator* that are responsible for this technique, input data and links between them are represented in Fig. 5.

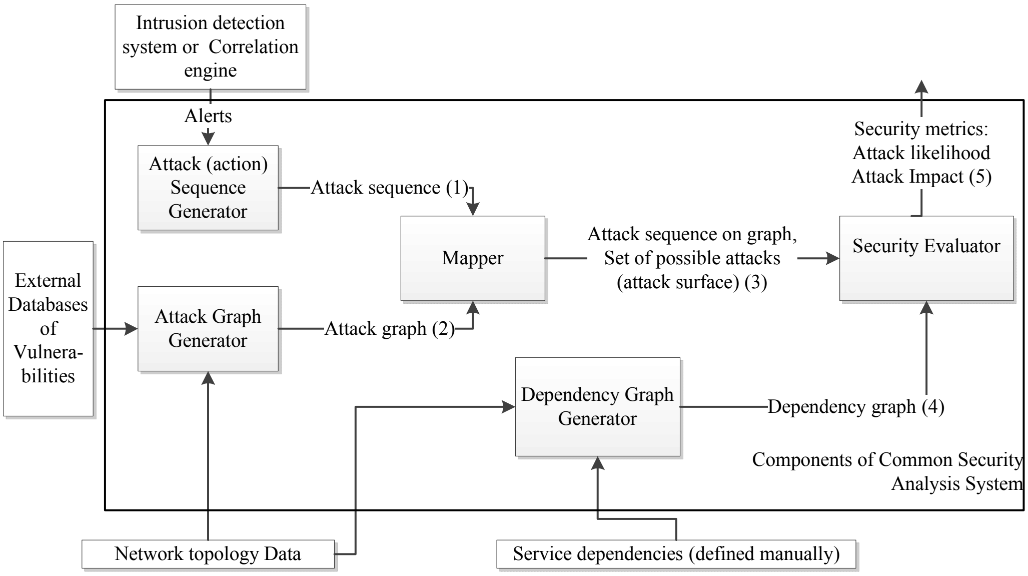
Intrusion detection system or Correlation engine
Alerts
Attack (action) Sequence Generator
Attack sequence (1)
Mapper
Attack sequence on graph, Set of possible attacks (attack surface) (3)
Security Evaluator
Security metrics: Attack likelihood Attack Impact (5)
External Databases of Vulnera-bilities
Attack Graph Generator
Attack graph (2)
Dependency Graph Generator
Dependency graph (4)
Components of Common Security Analysis System
Network topology Data
Service dependencies (defined manually)

Fig. 5 – Input data and main modules of Security Evaluator for performance-based risk assessment

Main stages of the technique are as follows:

(1) Attack (action) Sequence Generator builds the attack (action) sequence on the base of the alerts from correlation engine (CEP).

(2) Attack Graph Generator forms the graph of possible attacks on the base of the data about known vulnerabilities and the network topology.

(3) Mapper reflects the attack sequence (generated on stage 1) on the attack graph (generated on stage 2) to define realized attack sequence and the malefactor position on the attack graph.

(4) Dependency Graph Generator builds the service dependency graph on the base of the data about service dependencies in the analyzed network.

(5) Security Evaluator calculates the set of security metrics on the base of the attack graph, the defined malefactor position, the set of realized steps, and the service dependency graph.

This approach also defines the risk as the result of probability of the threat and its consequences for the system.

Probability of the threat is defined with the *Likelihood of Successful Attack* metric. In case of the ongoing attack it can be defined on the base of the following elements: *Severity* of the attack action (calculated on the base of the CVSS), *Attacker Skill Level* (calculated on the base of the *AccessComplexity* of the realized steps), *Attack Potentiality* (it is equal *number of realized attack steps*/*total number of attack steps*), *Reliability* coefficient (it is evaluated on the base of the *False Positive Rate*).

Consequences of the threat for the system are defined with the *Impact of Successful Attack* metric. It can be divided on the impact of the attack action (a *Native Impact*) and the *Propagated Attack Impact*. *Native Impact* is defined as vector {*Confidentiality Impact*, *Integrity Impact*, and *Availability Impact*} on the base of the CVSS indexes. *Propagated Impact* is defined via the service dependencies.

The *technique based on historical data* uses the same approach as performance-based technique, but when attack likelihood is defined we add additional weights that are related to historical data. It concerns such metrics as *Attack Potentiality* and *Attacker Skill Level*.

For the *Attack Potentiality* weight is defined by the relation of the number of cases when detected attack sequence led to the assessed attack to the total number of the occurrences of the detected attack sequence.

For the *Attacker Skill Level* statistical data is used to define probability that attacker with appropriate skills initialize assessed attack. The data is stored in the historical database.

5. CONCLUSION

The paper proposed the comprehensive multilevel system of security metrics and techniques for their calculation. We analyzed the state-of-the-art in the area of risk assessment.

On the base of this research we outlined different classes for known risk assessment metrics. The system of risk assessment metrics that we suggest to calculate in the *Security Evaluator* is proposed. The most characteristic techniques that allow evaluating the proposed metrics are discussed. Brief description of the security metrics for each level and techniques of their calculation is given. We implemented suggested techniques in the scope of the Common Security Analysis System [22- 25].

The suggested framework proposes structural organization of security metrics for the security analysis on the base of attack graphs. The metrics are defined on the base of the main elements of such analysis (system model, attacker model, attack model, events level). The framework allows to assess each element separately and to use it in the common risk assessment on the base of the suggested techniques. The techniques are selected according to the last research in the risk analysis area. In dynamic case information from the security events is considered. More information leads to the more accurate assessments.

On this moment we do not consider reliability of the data from the security events but we suppose to consider it in the future research. Techniques and metrics that are described in the paper will be considerably extended and detailed. Also we plan to test the *Security Evaluator* on real examples and analyze effectiveness of security assessment.

6. ACKNOWLEDGMENT

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

7. REFERENCES

[1] M. S. Ahmed, E. Al-Shaer, L. Khan, A novel quantitative approach for measuring network security, *Proceedings of the 27th Conference on Computer Communications* (*INFOCOM'08*), Phoenix, AZ, USA (April 13-18, 2008), pp. 1957-1965.

[2] C. W. Axelrod, Accounting for value and uncertainty in security metrics, *Information Systems Control Journal*, (6) (2008), pp. 1-6.

[3] R. Barabanov, S. Kowalski, L. Yngstrom, *Information Security Metrics. State of the Art*, DSV Report series, No. 11-007 (March 2011).

[4] N. Bartol, *Practical measurement framework for software assurance and information security (Version 1.0)*, Software Assurance Measurement Working Group (2008). Available at https://buildsecurityin.us-cert.gov/swa/downloads/SwA_Measurement.pdf.

[5] B. A. Blakely, *Cyberprints Identifying cyber attackers by feature analysis*, Doctoral Dissertation, Iowa State University, 2012.

[6] Common Configuration Enumeration (CCE) [Electronic resource]. Available at http://cce.mitre.org/.

[7] *The CIS Security Metrics*, The Center for Internet Security, 2009.

[8] Common Platform Enumeration (CPE) [Electronic resource]. Available at http://cpe.mitre.org/.

[9] Common Vulnerabilities and Exposures (CVE). [Electronic resource]. Available at http://cve.mitre.org/.

[10] R. Dantu, P. Kolan, J. Cangussu, Network risk management using attacker profiling, *Security and Communication Networks*, (1) (2009), pp. 83-96.

[11] L. Hayden, *IT Security Metrics: A Practical Framework for Measuring Security & Protecting Data*, McGraw-Hill, 2010, 396 p.

[12] D. S. Herrmann, *Complete Guide to Security and Privacy Metrics*, Auerbach Publications, 2007, 848 p.

[13] K. J. S. Hoo, *How much is enough? A risk-management approach to computer security*, PhD thesis, Stanford University, CA, 2000.

[14] N. C. Idika, *Characterizing and Aggregating Attack Graph-based Security Metrics*, CERIAS Tech Report 2010-23, Center for Education and Research Information Assurance and Security, Purdue University, August 2010.

[15] ISO/IEC 27005:2008, Information technology – Security techniques – Information security risk management, 2008.

[16] M. Jahnke, C. Thul and P. Martini, Graph-based metrics for intrusion response measures in computer networks, *Proceedings of the 3rd IEEE Workshop on Network Security, held in conjunction with 32nd IEEE Conference on Local Computer Networks*, Dublin (2007).

[17] W. Kanoun, N. Cuppens-Boulahia, F. Cuppens, J. Araujo, Automated reaction based on risk analysis and attackers skills in intrusion detection systems, *Proceedings of the third International Conference on Risks and Security of Internet and Systems* (*CRiSIS'08*), Toezer, Tunisia (2008), pp. 117-124.

[18] N. Kheir, *Response policies & counter-measures: Management of service dependencies and intrusion and reaction impacts*, PhD Thesis, Telecom Bretagne, 2010.

[19] N. Kheir, N. Cuppens-Boulahia, F. Cuppens, H. Debar, A service dependency model for cost-sensitive intrusion response, *Proceedings of the 15th European Symposium on Research in Computer Security* (*ESORICS'10*), Athens, Greece (2010), pp. 626-642.

[20] I. Kotenko, M. Stepashkin, Attack graph based evaluation of network security, *Proceedings of the 10th IFIP Conference on Communications*

and Multimedia Security (*CMS'2006*), Heraklion, Greece (2006), pp. 216-227.

[21] I. Kotenko, E. Doynikova, Security metrics for risk assessment of distributed information systems, *Proceedings of the IEEE 7th International Conference on "Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications" (IDAACS'2013)*, Berlin, Germany, pp. 646-650.

[22] I. Kotenko, A. Chechulin, and E. Novikova, Attack Modelling and Security Evaluation for Security Information and Event Management, *Proceedings of the International Conference on Security and Cryptography (SECRYPT 2012)*, Rome, Italy, pp. 391-394.

[23] I. Kotenko, A. Chechulin, Common Framework for Attack Modeling and Security Evaluation in SIEM Systems, *Proceedings of the 2012 IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing*, Besançon, France, *IEEE Computer Society*, Los Alamitos, California (2012), pp. 94-101.

[24] I. Kotenko and A. Chechulin, Attack Modeling and Security Evaluation in SIEM Systems, *International Transactions on Systems Science and Applications*, (8) 2012, pp. 129-147.

[25] I. Kotenko and A. Chechulin, A Cyber Attack Modeling and Impact Assessment Framework, *5th International Conference on Cyber Conflict 2013 (CyCon 2013)*, *Proceedings. IEEE and NATO COE Publications*, Tallinn, Estonia, pp. 119-142.

[26] J. M. Lorenzo, *AlienVault Users Manual. Version 1.0*, AlienVault, 2010-2011.

[27] P. K. Manadhata, J. M. Wing, An attack surface metric, *IEEE Transactions on Software Engineering*, (37) 3 (2011), pp. 371-386.

[28] A. Mayer, *Operational Security Risk Metrics: Definitions, Calculations, Visualizations*, Metricon 2.0. CTO RedSeal Systems, 2007.

[29] P. Mell, K. Scarfone, S. Romanosky, *A Complete Guide to the Common Vulnerability Scoring System Version 2.0*, June 2007.

[30] National Institute of Standard and Technologies. Available at http://www.nist.gov/.

[31] T. R. Peltier, *How to complete a risk assessment in 5 days or less*, Auerbach publications, 2008, 55 p.

[32] T. Olsson, Assessing security risk to a network using a statistical model of attacker community competence, *Proceedings of the 11th International Conference on Information and Communications Security (ICICS'2009)*, Beijing, China, pp. 308-324.

[33] N. Poolsappasit, R. Dewri, I. Ray, Dynamic security risk management using Bayesian attack graphs, *IEEE Transactions on Dependable and Security Computing*, (9) 1 (2012), pp. 61-74.

[34] S. Quinn, D. Waltermire, C. Johnson, K. Scarfone, J. Banghart, *The technical specification for the security content automation protocol (Version 1.0)*, Gaithersburg, MD: National Institute of Standards and Technology, 2009. Available at http://csrc.nist.gov/publications/nistpubs/800-126/sp800-126.pdf.

[35] N. Stakhanova, S. Basu, and J. Wong, A cost-sensitive model for preemptive intrusion response systems, *Proceedings of the 21st International Conference on Advanced Networking and Applications*, Washington, DC, USA, IEEE Computer Society (2007), pp. 428-435.

[36] T. Toth and C. Kruegel, Evaluating the impact of automated intrusion response mechanisms, *18th Annual Computer Security Applications Conference (ACSAC)*, 2002, pp.301-310.

[37] L. Wang, A. Singhal, S. Jajodia, and S. Noel, k-zero day safety: measuring the security risk of networks against unknown attacks, *Proceedings of the 15th European conference on Research in computer security*, Springer-Verlag Berlin, Heidelberg (2010), pp. 573-587.

[38] Y.-S. Wu, B. Foo, Y.-C. Mao, S. Bagchi, and E. H. Spafford, Automated adaptive intrusion containment in systems of interacting services, *Computer Networks: The International Journal of Computer and Telecommunications Networking*, (51) (2007), pp. 1334-1360.

***Igor Kotenko** graduated with honors from St. Petersburg Academy of Space Engineering and St. Petersburg Signal Academy. He obtained the Ph.D. degree in 1990 and the National degree of Doctor of Engineering Science in 1999. He is Professor of computer science and Head of the Laboratory of Computer Security Problems of St. Petersburg Institute for Informatics and Automation.*

***Elena Doynikova** graduated with honors from St. Petersburg Electrotechnical University "LETI". She is researcher of the Laboratory of Computer Security Problems of St. Petersburg Institute for Informatics and Automation.*