Attack Modelling and Security Evaluation for Security Information and Event Management

Igor Kotenko, Andrey Chechulin and Evgenia Novikova
Laboratory of Computer Security Problems, St. Petersburg Institute for Informatics and Automation (SPIIRAS), 14th Liniya, Saint-Petersburg, Russia

Keywords: Attack Modelling, Security Evaluation, Security Information and Event Management Systems, Attack Graph, Service Dependences Graph, Zero Day Vulnerabilities.

Abstract: The paper considers an approach to attack modelling in Security Information and Event Management (SIEM) systems. The suggested approach incorporates usage of service dependency graphs and zero-day vulnerabilities to produce attack graph, calculation of security metrics based on attack graph and service dependencies and advanced any-time techniques for attack graph generation and security evaluation, etc.

1 INTRODUCTION

The complexity of computer network security management causes the necessity to develop powerful automated security analysis components which can be important components of Security Information and Event Management (SIEM) systems (Miller et al., 2011); (MASSIF, 2012). These components should allow finding and correcting errors in the network configuration, reveal possible assault actions for different security threats, determine critical network resources and choose an effective security policy and security mechanisms appropriate to current threats.

The paper considers attack modelling security evaluation processes, intended to be implemented for the security analysis in SIEM systems.

There are a lot of papers, which consider different approaches to attack modelling and security evaluation taking into account various classes of attacks. In (Huang and Wicks, 1998); (Moore et al., 2001); (Dawkins et al., 2002) attacks are described and modelled in a structured and reusable "tree"-based form. Different approaches, which use attack graphs and trees for security analysis, have been suggested. Hariri et al. (Hariri et al., 2003) calculate global metrics to analyze and proactively manage the effects of complex network faults and attacks. Noel et al. (Noel et al., 2003); (Wang et al., 2006) propose a risk based technique based on determining the minimum-cost network hardening via exploit dependency graphs. Kotenko and Stepashkin (Kotenko and Stepashkin, 2006); (Kotenko et al., 2011) are focused on security metrics computations based on attack graph representation of malefactor behaviour. Lippmann and Ingols (Lippmann and Ingols, 2006); (Ingols et al., 2009) propose to use attack graphs to detect firewall configuration defects and host critical vulnerabilities. Wang et al. (Wang et al., 2008); (Wang et al., 2011) propose an approach to calculate attack resistance metrics based on probabilistic scores by combining CVSS scores (CVSS, 2012). Kheir et al. (Kheir et al., 2010) suggest an implementation of confidentiality, integrity and availability metrics using the notion of privilege, which is inspired by access permissions within access control policies.

We suggest an approach based on the following main procedures: usage of comprehensive internal security repository and open security databases; generation of attack trees considering service dependency graphs and zero-day vulnerabilities; application of anytime algorithms to provide near real-time attack modelling; usage of attack graphs to predict possible malefactor's actions; calculation of a multitude of security metrics, attack and response impacts; interactive decision support to select the security solutions. The main difference of the offered approach from the already suggested ones is the integration of these functionalities in one component to achieve better results in near real time effective attack modelling and security evaluation.

Kotenko I., Chechulin A. and Novikova E..
Attack Modelling and Security Evaluation for Security Information and Event Management.
DOI: 10.5220/0004063403910394
In *Proceedings of the International Conference on Security and Cryptography* (SECRYPT-2012), pages 391-394
ISBN: 978-989-8565-24-2

In the paper we discuss the architectural solution of the proposed Attack Modelling and Security Evaluation Component (AMSEC) as one of the important SIEM subsystem and the techniques used to realize main AMSEC functionality. To illustrate these architecture and techniques we developed a software prototype and carried out experiments for different case-studies.

The rest of the paper is organized as follows. *Section 2* discusses the AMSEC framework. In *Section 3,* we describe the AMSEC implementation and an example of experiments. *Conclusion* analyzes the paper results and future research.

2 FRAMEWORK

According to the analysis of state-of-the-art in attack modelling we selected the following key elements to be included in the architectural solution of AMSEC as part of the SIEM-system:

- Comprehensive security data repository;
- Effective attack tree and service dependencies generation techniques based on TVA (Topological Vulnerability Analysis) approach which enumerates potential sequences of exploits of known vulnerabilities to build attack graphs;
- Attack graph generation considering both known and zero-day vulnerabilities;
- Usage of anytime algorithms for near-real time attack sub-graph (re)generation and analytical modelling;
- Stochastic analytical modelling;
- Combined usage of attack graphs and service dependency graphs;
- Security metric calculation, including attack impact, response efficiency, response collateral damages, attack potentiality, attacker skill level assessment, etc.;
- Interactive decision support to select the solutions on security measures/tools by defining their preferences regarding different types of requirements (risks, costs, benefits) and setting trade-offs between high-level security objectives.

To bind the key elements we developed the following generalized architecture of AMSEC. The brief descriptions of the AMSEC's modules and their functions are given below.

Network interface supports interaction with external environment (sending requests to external databases and communicating with data sources).

Interactive decision support module provides the user (decision maker) with the ability to select the solutions on countermeasures by defining their preferences regarding different types of requirements and setting trade-offs between objects. Decision support can include three phases: setting feasible security solutions (security measures/tools); identification of efficient (Pareto-optimal) security solutions; selection (generation) of the final solution.

Generator of system and security policy specification converts the information about network configuration and security policy received from the data collection and correlation components or user into internal representation. It is supposed, that at the design stage, this information is specified on special System Description Language and Security Policy Language. Used specifications of the analyzed network (system) and the security policy should describe network components with the necessary degree of detail, for example, the used software should be set in the form of names and versions.

Data repository updater downloads the open databases of vulnerabilities, attacks, configuration, weaknesses, platforms, countermeasures, etc., for example, National Vulnerability Database (NVD) (NVD, 2012), Common Vulnerabilities and Exposures (CVE) (CVE, 2012), Common Platform Enumeration (CPE) (CPE, 2012), and then translates them into the AMSEC security data repository.

Reports generator shows vulnerabilities detected by AMSEC, represents “weak” places, generates recommendations on strengthening the security level, etc.

Security repository is a hybrid (relational, XML-based and triplet-based) data storage which contains information necessary for attack graph generation and analysis. We suggest to use a set of MSM related standards (MSM, 2012) or other related standards for the common enumeration, expression and reporting of cyber-security-related information as the basis for the design of the common security repository.

Malefactor Modeller is responsible for malefactor modelling and is used on both design and exploitation stage of the AMSEC operation. On the first phase it is used to build the set of all possible attack graphs using preset characteristics of malefactor (the malefactor profile) which are determined by the user. Later on the second phase it allows predicting the possible characteristics of the malefactor according to the actions fulfilled.

Attack Graph Generator is responsible for attack graph building. In our approach we use hierarchical model of attack scenarios which consists of three levels: integrated, script and actions levels.

The algorithm of generating the common attack graph is based on the attack scenarios model. The result of the algorithm is attack graph which describes the possible routes of attack actions in the view of malefactor's initial position, skill level, network configuration and used security policy.

Attack Graph Generator operates in conjunction with *Manager of Service Dependencies* and *Generator of Attack Graph Based on Zero-day Vulnerabilities* to obtain more precise results in attack modelling. The usage of service dependency graphs makes it possible to exclude information about attack impacts from the attack graph and to use the dependency graph in order to simulate impacts and obtain a dynamic evaluation of an attack impact. In our approach we take to into account zero-day vulnerabilities to generate attack graph. To do this we modified the approach suggested in (Ingols et al., 2009) by adding additional characteristics which define probability of existence of the zero day vulnerability. The main idea is to automate process of selection of hosts which are likely to have zero day vulnerabilities then others (instead of manual search).

The attack graph is based on the network model and the probabilities of vulnerabilities defined as weight coefficients. The net of the connected information sensors that are able to detect attacks is formed in the real network. The monitoring system allows constructing general view about the events that take place in the network according to the information sensors.

Security Evaluator is responsible for qualitative and quantitative assessment of the system security. For qualitative express assessment of the network security we planning to use several approaches which are based on different security metrics, risk analysis and security evaluation techniques.

3 EXPERIMENTS

By now a prototype of AMSEC, which can generate possible attack trees for a predefined network and evaluate the network security level, was implemented. It contains three basic components: *VDBUpdater*, *Network Constructor* and *Security Level Evaluator*. Additionally the prototype includes the MySQL database as a common repository. *VDBUpdater* allows updating the internal database of known vulnerabilities, using information obtained from National Vulnerability Database (NVD, 2012). *Network Constructor* allows creating models of tested computer networks and checks selected software and hardware to match NVD dictionary. *Security Level Evaluator* makes topological vulnerability analysis and evaluates the security level of the network.

A set of experiments with the prototype of AMSEC was conducted. The prototype makes use of two scenarios (MASSIF, 2012): "Managed Enterprise Service Infrastructures" and "Critical Infrastructure Process Control (Dam)".

Let us consider the experiments where we chose a malefactor located outside the controlled network of the dam infrastructure. After constructing the attack graph, the AMSEC provides the following information: the malefactor knowledge after all possible attacks, the attack tree in the graphic form and the log of the malefactor's actions. Figure 1 illustrates different attacks traces that the malefactor can perform in the tested network. The malefactor, carrying out attack actions, is located in the centre of the spherical representation. The other icons are as follows: "A" – an attack action, "S" – a scenario which does not use vulnerabilities (for example, host discovery (PING)), "V" – an attack action which exploits some vulnerability. According to the suggested metrics the security level of the tested network is evaluated.

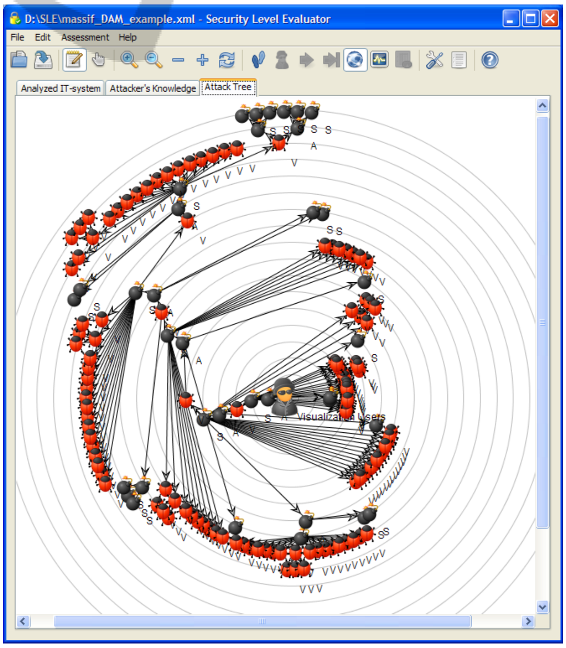

Figure 1: Attack graph.

4 CONCLUSIONS

In the paper we presented our approach to the attack modelling and security evaluation. We also described the developed prototype of the AMSEC, which can generate a possible attack tree for a predefined network and a simple experiment was considered.

The future steps of the research will be devoted to detailed elaboration of all AMSEC components. One of the important research issues is development of techniques which can cope with large networks, such as those in enterprise infrastructure.

Also it is planned to optimize the generation of attack trees through the use of the ontology based repository, to expand the list of parameters, characterizing the hosts and the network, to improve the malefactor model, and to add currently unrealized components.

ACKNOWLEDGEMENTS

This research is being supported by grant of the Russian Foundation of Basic Research (projects 10-01-00826), the Program of fundamental research of the Department for Nanotechnologies and Informational Technologies of the Russian Academy of Sciences, the State contract #11.519.11.4008 and by the EU as part of the SecFutur and MASSIF projects.

REFERENCES

CPE, 2012. Common Platform Enumeration, viewed 01 March 2012, <http://cpe.mitre.org/>.

CVE,2012. Common Vulnerabilities and Exposures. viewed 01 March 2012, <http://cve.mitre.org/>.

CVSS,2012. Common Vulnerability Scoring System, viewed 01 March 2012, <http://www.first.org/cvss/>.

Dawkins, J., Campbell, C., Hale. J., 2002. Modeling network attacks: Extending the attack tree paradigm. In Workshop on Statistical and Machine Learning Techniques in Computer Intrusion Detection, Johns Hopkins University.

Hariri, S., Qu, G., Dharmagadda, T., Ramkishore, M., Raghavendra C. S., 2003. Impact Analysis of Faults and Attacks in Large-Scale Networks. In *IEEE Security and Privacy*, vol.1 pp.49-54.

Huang, M.-Y., Wicks, T. M., 1998. A Large-scale Distributed Intrusion Detection Framework Based on Attack Strategy Analysis. In *First International Workshop on the Recent Advances in Intrusion Detection, Raid'98*, Louvain-la-Neuve, Belgium.

Ingols, K., Chu, M., Lippmann, R., Webster, S., Boyer, S., 2009. Modeling modern network attacks and countermeasures using attack graphs. In *Proceedings of the 2009 Annual Computer Security Applications Conference (ACSAC '09)*, Washington, D.C., USA, IEEE Computer Society.

Kheir, N., Cuppens-Boulahia, N., Cuppens F. and Debar H., 2010. A service dependency model for cost-sensitive intrusion response. In *Proceedings of the 15th European Symposium on Research in Computer Security (ESORICS),* Athens, Greece.

Kotenko, I., Stepashkin, M., 2006. Attack Graph based Evaluation of Network Security. In *Lecture Notes in Computer Science*, Vol. 4237, pp.216-227.

Kotenko, I., Stepashkin, M., Doynikova, E., 2011. Security Analysis of Computer-aided Systems taking into account Social Engineering Attacks In *Proceedings of the 19th Euromicro International Conference on Parallel, Distributed and network-based Processing* (*PDP 2011*), Los Alamitos, California. IEEE Computer Society, pp.611-618.

Lippmann, R., Ingols, K., 2006. Validating and Restoring Defense in Depth Using Attack Graphs. In *Proceedings of MILCOM 2006*. Washington, DC.

MSM, 2012. Making Security Measurable, viewed 01 March 2012, http://measurablesecurity.mitre.org/index.html>.

MASSIF, 2012. Massif project, viewed 01 March 2012, <http://www.massif-project.eu>

Miller, D. R., Harris, Sh., Harper, A. A., VanDyke, S., Black, Ch. 2011. *Security Information and Event Management (SIEM) Implementation*. McGraw–Hill Companies. 2011. 430 p.

Moore, A. P., Ellison, R. J., Linger, R. C., 2001. Attack Modeling for Information Security and Survivability. *Technical Note CMU/SEI-2001-TN-001. Survivable Systems*.

Noel, S., Jajodia, S., O'Berry, B., Jacobs, M., 2003. Efficient minimum-cost network hardening via exploit dependency graphs. In *Proceedings of the 19th Annual Computer Security Applications Conference (ACSAC'03)*.

NVD, 2012. National Vulnerability Database viewed 01 March 2012, <http://nvd.nist.gov/>

Wang, L., Islam, T., Long, T., Singhal, A., Jajodia, S., 2008. An attack graph-based probabilistic security metric. In *Proceedings of the 22nd Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec'08)*.

Wang, L., Jajodia, S., Singhal, A., Noel, S., 2010. k-Zero Day Safety: Measuring the Security Risk of Networks against Unknown Attacks. In *ESORICS'10 Proceedings of the 15th European conference on Research in computer security*. Springer-Verlag, Berlin, Heidelberg, pp.573-587.

Wang, L., Whitley, J. N., Phan, R. C. W., Parish, D. J., 2011. Unified Parametrizable Attack Tree. In *International Journal for Information Security Research*, Vol.1 (1), pp. 20-26.