CYBER SECURITY: AN ATTACK GRAPHS PERSPECTIVE

Valentin PAU[1] Dorina-Luminița COPACI [2], Constantin Alin COPACI[3]

Rezumat. *Graficele de atac sunt folosite pentru a modela vulnerabilitățile sistemului și exploatările potențiale ale acestora. Măsurile de securitate servesc drept instrument puternic pentru organizații, pentru a înțelege eficacitatea protecției rețelelor de comunicații. Lucrarea de față prezintă o metodă de analiză și evaluare a securității cibernetice, bazată pe grafice de atac. Se utilizează o reprezentare a relațiilor dintre resursele vulnerabile și incidentele de securitate produse în rețele și se obține cuantificarea nivelului de securitate al acestora.*

Abstract. *Attack graphs are used to model system vulnerabilities and their potential exploits. Security metrics serve as a powerful tool for organizations to understand the effectiveness of protecting communications networks. The present paper presents a method for analyzing and assessing cyber security, based on attack graphs. It uses a representation of the relations between vulnerable resources and security incidents produced in networks and allows the quantification of their security level.*

Keywords: cyber security, attack graph, security metrics, vulnerability

DOI https://doi.org/10.56082/annalsarscieng.2023.2.35

1. Introduction

The complexity of the analysis and evaluation of current systems security is generated by the multitude of technologies, by the nature of the systems' resources, but also by the diversification of the threat types. [1] The current methods of network security analysis and evaluation are based on quantitative and qualitative approaches.

The attack graph method is a system security analysis and assessment method which uses symbolic representations of the relations between threats, system resources and the potential consequences of attacks. These symbolic representations are called attack graphs and also allow the quantification of the security level for a communication system. [2. 3]

With the expansion of network connectivity, there has been a rapid increase in the number of cyber attacks on corporations and government offices, damaging the reputation as well as the financial stability of these corporations.

[1]Professor, PhD, full member of Academy of Romanian Scientists, str. Ilfov nr. 3, sector 5, Bucharest; (e-mail: valentin.pau@prof.utm.ro);
[2] PhD, Titu Maiorescu University, Bucharest;
[3] Engineer, ANCOM, Bucharest

Building appropriate models and understanding the relationship between vulnerabilities and their lifecycle events will take place by identifying vulnerability trends and anticipating security gaps in a network. Therefore, resources can be effectively allocated to ensure protection.
Table 1 shows the existence of several levels of understanding system threats and vulnerabilities.

Table 1. Understanding cyber situation

Level 1	**Perception**	**Security monitoring**
		Intrusion detection techniques
Level 2	**Understanding**	**Risk analysis**
Level 3	**Mitigation**	**Risk mitigation**
Level 4	**Prevention**	**Predictive modeling**

2. Attack Graphs

A threat to a system is an event produced at the level of the infrastructure, which leads to the compromise of at least one function of the system. An attack is a set of threats that compromise all system functions. [1][3] [4]

An attack graph G_{atac} is a directed acyclic graph which abstracts the characteristics of possible threats to a system's resources and it is used to determine whether the target of an attack is tangible.

A G_{atac} attack graph is defined as: $G_{atac} = \{V, E\}$, where: [4]

- $V=\{s/s = state\_system(var1, var2,..., varn)\}$: is the set of nodes of the attack graph corresponding to the states of the network. Each state of the system is described by a set of state variables *varj*, j =1,2,...,n. State variables are associated with system functions. The initial state, *state_initialsystem*, is the state of the system before the occurrence of any event at the level of its infrastructure. The final state, *state_finalsystem*, is the compromised state of the system, a state in which all system functions are compromised.
- $E = \{(s, t) | s,t \in V\}$: the directed arcs of the graph correspond to the state transitions of the system. Each ordered pair (s, t) defines a system state transition that occurs when an event produced at the level of the system infrastructure determines the modification of at least one state variable.

The attack path represents any path in the attack graph where the source node corresponds to the initial state of the system and the destination node corresponds to the compromised state:

$P=\{(s_i,s_{i+1}) \in E,\ i=0,..,r-1 \mid s_0 = state\_initialsystem,\ s_r = state\_finalsystem,\ r \leq |V|\}$

The attack graph is built on the basis of the possible attack scenarios for the communication system. An attack scenario is a list of threats to the communication system (path of attack), together with the targeted resources and the list of conditions necessary for the execution of the respective actions. [3] [4]

3. Security classes

There are different classes that network security metrics fall into. These classes are shown in Figure 1.

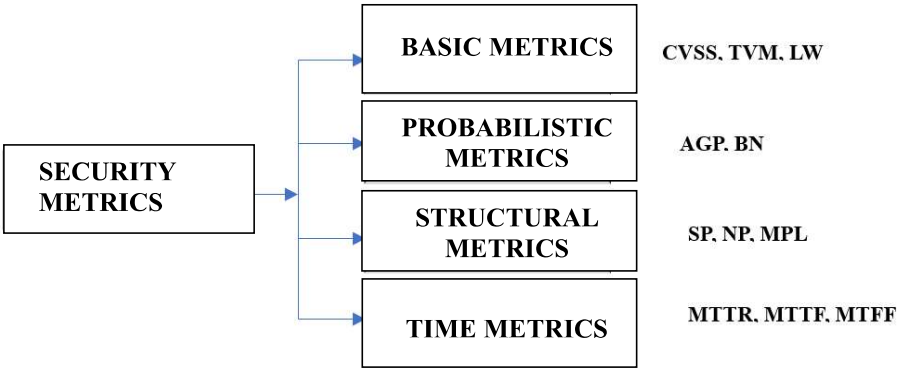

Fig. 1 Security metrics classification

- *Basic metrics* – usually, these metrics do not use any graph structure to quantify network security. Some examples that fall into this category are the Total Vulnerability Measurement (TVM) [5] and the Langweg (LW) metric [6].
- *Structural metrics* - these values use the underlying structure of the attack graph to aggregate the security properties of individual systems in order to quantify network security. The shortest path (SP) metric [7], [8] measures the shortest path for an attacker to reach an end goal. The number of paths (NP) metric [8] measures the total number of paths for an attacker to reach the final goal. The path length metric (MPL) [9] measures the arithmetic mean of the length of all paths to the final target in the attack graph.

- *Probability-based metrics* - these metrics associate probabilities with individual entities in order to quantify network security. Some examples that fall into this category are based on Attack Graph-Based Probabilistic Metrics (AGP) and Bayesian Network (BN) metrics [10], [11], [12]. In AGP each node/edge in the graph represents a vulnerability being exploited and is assigned a probability score. The assigned score represents the probability that an attacker might exploit the exploit because all prerequisites are met. In BN-based metrics, the probabilities for the attached graph are updated based on new evidence and on the previous probabilities associated with the graph.
- *Temporal metrics* - these values quantify how quickly a network can be compromised or how quickly preventive measures can be taken in order to respond to attacks. The common values that fall into this category are: mean time to breach (MTTB), mean time to recovery (MTTR) [13] and mean time to first failure (MTFF) [14].

4. Security analysis and assessment

The method of analyzing and assessing system security using attack graphs is based on scenarios and attack paths defined in the system design and development stage.

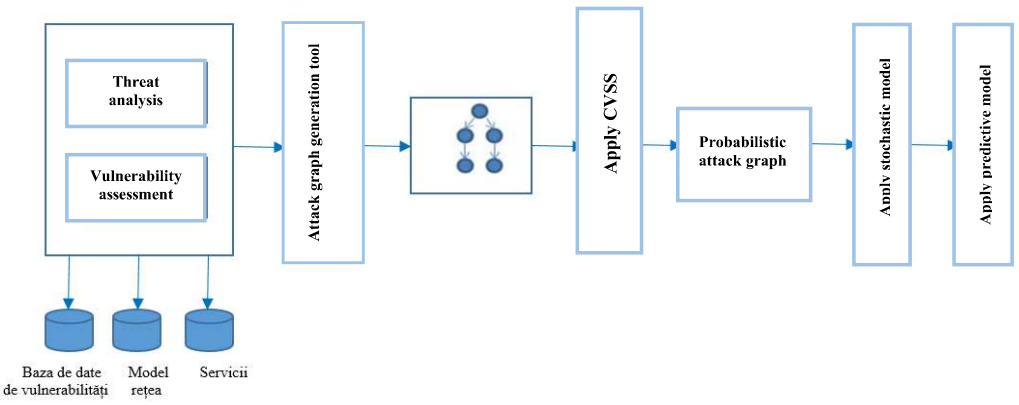

Fig. 2. Cyber security analysis framework

In this part of the paper, we analyze the concept of modeling the attack graph as a stochastic process. Figure 2 shows the cyber security analysis framework [15], [16], in which all the processes involved in building the security metrics framework are presented.

The analysis and assessment of system security is carried out in the following stages:

a. specifying the components of the attack scenario;

The components of the attack scenario are: the list of system resources and the list of events that undermine the security of the system infrastructure [4].

The resources of a system include servers, routing equipment, signal processing or conversion equipment or nodes, user workstations.

Security incidents are events produced in the system which exploit existing vulnerabilities at the level of its resources. An event produced at the infrastructure level of a system is formally defined as a mapping relationship of a set of conditions on a set of results (consequences) of the event [3], [4]:

b. generating the attack graph;

The attack graph is generated manually or automatically, depending on the complexity of the system for which the security analysis and assessment is performed. In both cases, the attack graph is built using the attack scenarios defined for the analyzed system.

The complexity of generating the attack graph is determined by the complexity of the attack actions or security threats for the reactive system. It depends on the number of system resources, as well as on the number and location of its vulnerabilities [3], [4], [17].

The complexity of the attack graph analysis is determined by the complexity of traversing the attack graph in depth ("depth-first") and it is $O(|V|+|E|)$. [3] [17] [18]

c. assessing the security level for the analysed system [3] [4]

The assessment of system security is carried out by means of numerical indicators: the effectiveness factor of the event, the effectiveness factor of the remedy and the level of security of the system.

5. Case study

In order to illustrate the proposed approach, a network has been created in Figure 3.

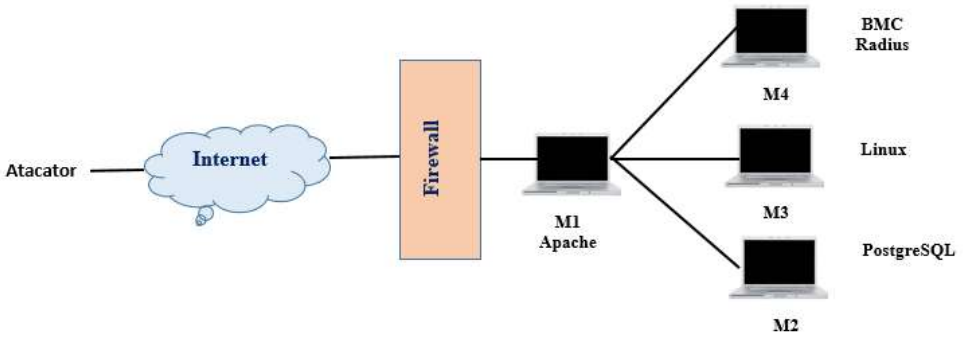

Fig. 3. Network topology

The network is made up of 4 machines that are interconnected and run internally behind a firewall. The attacker or threat is outside the firewall and connected externally to the network. The firewall has only one open port (port 80) to the external network for access to its web server. The machine hosting the M1 web server is running Apache Webserver. The attacker's goal is to infiltrate the network and gain M4 root access. To achieve this, the attacker must first start with the apache web service, which is the only port (80) accessible from the firewall.
Table 2 contains a list of network vulnerabilities that can be exploited by an attacker if certain conditions are met.

Table 2. Vulnerabilities

Service name	CVE-ID	Partial Exploitability Score	Host machine	Date of Disclosure
Apache	CVE-2014-0098	10	M1	18.03.2014
PostgreSQL	CVE-2014-0063	7,9	M2	17.02.2014
Linux	CVE-2014-0038	3,4	M3	06.02.2014
bmc	CVE-2013-4782	10	M4	08.07.2013
Radius	CVE-2014-1878	10	M4	28.02.2014

Each of the six vulnerabilities is unique and publicly known and it is indicated by a Common Vulnerability and Exposure (CVE). For example, the Apache web server was found to have the CVE-2014-0098 vulnerability dated 03/18/2014 that allows remote attackers to cause segmentation faults.
Similarly, the postgresql service hosted by M2 had a vulnerability designated CVE-2014-0063 that allowed remote attackers to execute arbitrary code. Several public sites like NVD (National Vulnerability Database), MITRE, Nessus provide information about well-known vulnerabilities and, at the same time, about their

severity using score values adopted by CVSS (Common Vulnerability Scoring System).

By combining the vulnerabilities present in the network configuration (Figure 4), we can create several scenarios in which an attacker can achieve a goal state. In this particular case, the attacker's goal state would be to gain root access on the M4 machine. Figure 4 shows the paths the attacker can take to reach the goal state. By combining these different paths, we can obtain an attack graph.

Several practical approaches have been proposed [20], [21], [22] for the automatic generation of attack graphs.

In the present analysis, the MulVAL tool has been used [21] to generate a polynomial time attack graph.

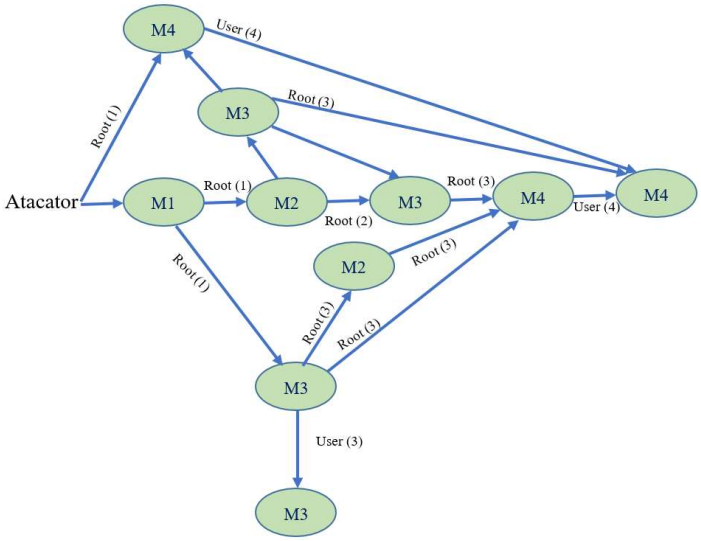

Fig. 4 Network topology - graph

Table 3 provides an overview of the different attack graph generation toolsets which are available [19].

Table 3. Attack graph generation toolsets

Tool name	Complexity	Open source	Developer
MulVAL	$O(n^2)$~ $O(n^3)$	da	Kansas of University
TVA	$O(n^2)$	NU	George Mason University
Cauldrom	$O(n^2)$	nu	Comercial
NetSPA	O(nlogn)	Nu	MIT

Security analysis consists in determining how the distribution of values of proposed attack graphs varies over a certain period of time. In the attack graph model, each node corresponds to a software associated with a vulnerability existing on a particular machine in the network. The transition probability for an edge in the attack graph is calculated by normalizing the CVSS exploitation scores over all edges from the attacker's source node.

6. Conclusions

The attack graph method is a quantitative method of analysis and assessment of the security of network infrastructures and communication systems. This method can be applied for determining their vulnerabilities, because it is based on the relations between the resources of communication systems, the types of events produced at their level and the potential consequences they produce at the level of communication systems and end users.

The security analysis and evaluation method using attack graphs also allows determining the critical sequences of events for communication systems, that is, of those events that have the highest potential to compromise their functions.

R E F E R E N C E S

[1] John Steven, Gunnar Peterson: Using Attack Graphs to Design Systems, IEEE Computer Societym IEEE SECURITY & PRIVACY, 2007.

[2] Jeannette Wing: Scenario Graphs Applied to Network Security, Carnegie Mellon University, 2008.

[3] Sorin Soviany: Studiu privind metode moderne de securizare a accesului la sisteme de comunicaţii de bandă largă, proiect PN 09-08 03 04 INSCC (faza 2, decembrie 2010). (Study on modern methods of securing access to broadband communication systems, project PN 09-08 03 04 INSCC (phase 2, December 2010).

[4] Zhang Lufeng, Tang Hong: Network Security Evaluation through Attack Graph Generation, World Academy of Science Engineering and Technology 54 2009.

[5] M. Abedin, S. Nessa, E. Al-Shaer, and L. Khan, “Vulnerability analysis for evaluating quality of protection of security policies," in Proceedings of Quality of Protection 2006 (QoP '06), October 2006.

[6] H. Langweg, "Framework for malware resistance metrics," in Proceedings of the Quality of Protection 2006 (QoP '06), October 2006.

[7] C. Phillips, L.P. Swiler, “A graph-based system for network-vulnerability analysis,”Proc. WNSP’98, pp.71-79.

[8] R. Ortalo, Y. Deswarte, and M. Kaaniche, “Experimenting with quantitative evaluation tools for monitoring operational security,” IEEE Transactions on Software Engineering, vol. 25, pp. 633–650, September 1999.

[9] W. Li and R. Vaughn, “Cluster security research involving the modeling of network exploitations using exploitation graphs,” in Sixth IEEE International Symposium on Cluster Computing and Grid Workshops, May 2006.International Journal of Computer Networks & Communications (IJCNC) Vol.7, No.1, January 2015.

[10] M.Frigault and L. Wang, "Measuring Network Security Using Bayesian Network-Based Attack Graphs," in Proceedings of the 3rd IEEE International Workshop on Security, Trist and Privacy for Software Applications (STPSA’08), 2008.

[11] L. Wang, T. Islam, T. Long, A. Singhal, and S. Jajodia, "An attack graph-based probabilistic security metric," DAS 2008, LNCS 5094, pp. 283-296, 2008.

[12] L. Wang, A. Singhal, and S. Jajodia, "Measuring overall security of network configurations using attack graphs," Data and Applications Security XXI, vol. 4602, pp. 98-112, August 2007.

[13] A. Jaquith, Security Metrics: Replacing Fear, Uncertainty, and Doubt. Addison-Wesley, Pearson Education, 2007.

[14] K. Sallhammar, B. Helvik, and S. Knapskog, "On stochastic modeling for integrated security and dependability evaluation," Journal of Networks, vol. 1, 2006.

[15] S.Abraham and S.Nair, "Cyber Security Analytics: A stochastic model for Security Quantification using Absorbing Markov Chains" 5th International Conference on Networking and Information Technology, ICNIT 2014.

[16] S.Abraham and S.Nair, "A Stochastic Model for Cyber Security Analytics" Tech Report 13-CSE-02 , CSE Dept, Southern Methodist University, Dallas, Texas, 2013.

[17] Xinming Ou, Wayne Boyer: A Scalable Approach to Attack Graph Generation, ACM CCS06, 2006.

[18] Oleg Sheyner, Jeannette Wing: Tools for Generating and Analysing Attack Graphs, Carnegie Mellon University, 2007.

[19] Shengwei Yi, Yong Peng, Qi Xiong, Ting Wang, Zhonghua Dai, Haihui Gao, Junfeng Xu, Jiteng Wang and Lijuan Xu "Overview on attack graph generation and visualization

technology", AntiCounterfeiting, Security and Identification (ASID), 2013 IEEE International Conference on, Issue Date: Oct. 2013.

[20] O. Sheyner, J. W. Haines, S. Jha, R. Lippmann, and J. M. Wing, "Automated generation and analysis of attack graphs," in IEEE Symposium on Security and Privacy, 2002, pp. 273–284.

[21] Xinming Ou, Sudhakar Govindavajhala, and Andrew W. Appel. MulVAL: A logic-based network security analyzer.

[22] S. Jajodia and S. Noel, "Advanced Cyber Attack Modeling, Analysis, and Visualization," George Mason University, Fairfax, VA, Technical Report 2010.

[23] V. Pau, M.I. Mihăilescu, "Big data and e-learning: The impact on the future of learning industry"., Vol 7, Nr. 2/2015 Annals of the Academy of Romanian Scientists, Series on Engineering Sciences, ISSN 2066 – 8570.

[24] V. Pau, I. Mihăilescu, O Stănescu – Avoiding security and privacy issues by using specific patterns in biometric and RFID systems, International Conference „Promoting partnership in higher education for a knowledge-based society", 2011.