Modeling the cyber attacks vector based on fuzzy cognitive maps

V.I. Vasilyev[1], A.D. Kirillova[1], A.M. Vulfin[1], A.V. Nikonov[1]

[1]*Ufa State Aviation Technical University, K. Marks st. 12, Ufa, Russia, 450008*

Abstract

The modeling of scenarios of complex multistep targeted cyber attacks is considered. To determine all scenarios for the implementation of the attack, the draft Methodology for modeling security threats of the FSTEC of Russia and CAPEC attack patterns are used. Attack vector is presented in the form of an attack graph with further formalization in the form of a hierarchical fuzzy cognitive map for the possibility of multiple scale analysis. Automated modeling of a set of possible attacks allow extract information about infrastructure weaknesses, the most dangerous vulnerabilities and potential weaknesses of system components, identify the most successful attack scenarios and assess their consequences for the enterprise.

Keywords

Cyber attack vector, scenario, CAPEC, fuzzy cognitive map, risk assessment

1. Introduction

Today multi-stage distributed coordinated attacks with a complex organization, complex implementation process, and a variety of purposes prevail [1]. When ensuring the cybersecurity of information infrastructure objects, the creation of intelligent means of protection that allows detecting complex targeted attacks is highlighted. Modeling the attack vector at various stages of its life cycle becomes the main tool. Building an attack vector without the use of computer automation tools is laborious and requires highly qualified specialists. It is proposed to automate the process of modeling the attack vector based on formalized meta attack patterns in the basis of fuzzy cognitive maps (FCM).

2. Analysis of methods for modeling the cyber attacks vector

One of the most famous technique in the field of cyberattack analysis is a technique based on modeling scenarios for their implementation using the Cyber Kill Chain model [2]. The draft Methodology for Modeling Information Security Threats [3] uses tactics and techniques and information from the FSTEC information security threat database to determine all possible attack scenarios. The main tools for attack modeling are the MITER ATT&CK [4] database and the CAPEC [5] database. Using the CAPEC database in addition to the FSTEC Methodology for modeling cyber attack vectors allows to structure the source data for modeling cyber attack vectors. It is advisable to formalize attack vectors in the form of attack graphs containing all possible scenarios for the implementation of a cyberattack, and to further formalize the attack graph in the form of a hierarchical FCM, which allows analyzing attack vectors with the required level of detail using decomposition and aggregation mechanisms.

3. Cyber attack vector modeling

The attack vector is constructed as a chain of probabilistic transitions between the nodes of the attack graph. To assess the probabilities of transitions, the vulnerability corresponding to the meta attack pattern element and the level of its severity (CVSS assessment) were used [6, 7]. The paper considers the procedure of “folding” the detailed FCM, which reveals the content of the attack vector, to the consolidated FCM of the level of cyber attack presentation. The most detailed level of FCM reflects a series of actions of an attacker at each stage of an attack, the next level allows to roll up these actions to a scenario for implementing a cyber attack. Each attack is scaled up to the FCM concept with appropriate weighting factors to assess the probability of an attack in each of the possible scenarios. The resulting FCM makes it possible to assess the level of local relative risks in the implementation of the attacker's influence on the information system.

4. Conclusion

Application of this approach allows to obtain a detailed assessment of cybersecurity risks and to provide a more informed choice of means for implementing the defense in depth strategy. Building FCM to model a set of all possible attacks and their implementation scenarios facilitates security analysis and allow choosing the required level of detail of the attack vector, bringing the solution to quantitative estimates of local relative risk, based on the CVSS threat assessment metrics of vulnerabilities and software, hardware and organizational software flaws.

5. Acknowledgments

The reported study was funded by RFBR according to the research project No. 20-38-90078 and No. 20-08-00668.

6. References

[1] Kim, Y. Involvers' Behavior-based Modeling in Cyber Targeted Attack / Y. Kim, I. Kim // Eighth International Conference on Emerging Security Information, Systems and Technologies. IARIA. – 2014. – P. 132-137.

[2] Cho, S. Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture / S. Cho, I. Han, H. Jeong, J. Kim, S. Koo, H. Oh, M. Park // International Conference on Cyber Situational Awareness, Data Analytics and Assessment (Cyber SA). IEEE. – 2018. – P. 1-8.

[3] Methodology for modeling security threats. FSTEC of Russia project [Electronic resource]. – Access mode: https://fstec.ru/component/attachments/download/2727 (10.01.2021).

[4] ATT&CK Matrix for Enterprise [Electronic resource]. – Access mode: https://attack.mitre.org/ (10.01.2021).

[5] CAPEC. Common Attack Pattern Enumeration and Classification [Electronic resource]. – Access mode: https://capec.mitre.org/index.html (10.01.2021).

[6] Vasilyev, V.I. Cybersecurity risk assessment of industrial objects' ACS of TP on the basis of nested fuzzy cognitive maps technology / V.I. Vasilyev, A.M. Vulfin, M.B. Guzairov, V.M. Kartak, L.R. Chernyakhovskaya // Informacionnye tekhnologii. – 2020. – Vol. 26(4). – P. 213-221. DOI: 10.17587/it.26.213-221.

[7] Zhang, J.Y. Quotient FCMs-a decomposition theory for fuzzy cognitive maps / J.Y. Zhang, Z.Q. Liu, S. Zhou // IEEE transactions on fuzzy systems. – 2003. – Vol. 11(5). – P. 593-604.