Situational Awareness of E-learning System Based on Cyber-Attack and Vulnerability

Linkai Zhu[1,2(✉)], Wennan Wang[2], Ruijie Luo[2], Zhiming Cai[2(✉)], Sheng Peng[2,4], and Zeyu Zhang[3]

[1] Institute of Software Chinese Academy of Sciences, Beijing, China
linkai@iscas.ac.cn
[2] Institute of Data Science, City University of Macau, Macau, China
caizhiming@cityu.mo
[3] School of Applied Sciences, Macao Polytechnic Institute, Macau, China
[4] Zhuhai Yingying Technology Co., Ltd., Zhuhai, China

Abstract. As technology changes and advances, E-learning has come a long way, providing a personal and interactive wealth of content. However, unethical behavior and the severity of network security attacks have received limited attention. While E-learning systems have been embraced for training and virtual team collaboration, little is known about the motivations of these systems for cybersecurity attacks. E-Learning network security situation assessment technology can synthesize various network attack data and combine them with security elements to reflect the network security status of E-Learning systems. This paper is based on the analysis of the existing network security situation assessment methods and technologies, so it proposes a situational awareness framework based on an E-learning system and implements an E-learning situation monitoring and warning system prototype system. Finally, we tested the real system in seven days to calculate the network security situation value. The proposed evaluation model, quantitative evaluation algorithm, and prediction algorithm are verified.

Keywords: Cybersecurity · Cyber-attack · E-learning systems security · Situational awareness · Vulnerability

1 Introduction

The main source of network hidden danger is that the system platform and some important service programs have found significant security loopholes, especially since several serious vulnerabilities were disclosed in the Windows' system in successive months, followed by the widespread prevalence and outbreak of worm programs using the vulnerabilities [1]. There are security loopholes in many E-learning network applications. The threat of network attacks is increasingly rampant. The risk of network security is increasingly complex, which has caused great economic losses to the education system and individuals [2]. Meet the security requirements of e-learning systems is a complicated problem since it is not only the content, services, and personal data that must be secured,

W. Zhou and Y. Mu (Eds.): ICWL 2021, LNCS 13103, pp. 154–159, 2021.
https://doi.org/10.1007/978-3-030-90785-3_15

but the E-learning system manager or staff [3]. E-learning course resources face security threats, since E-learning data is distributed, shared, open, and based on teamwork, so it is critical to protect confidentiality and integrity from any security issues. The purpose of the paper is to synthesize different cyber-attacks that will affect the E-learning system. And against these cyber threats, we propose a network security situational awareness system for detection, prediction, and protection by analyzing the internal relationship between the data and the network events, it can help network administrators to predict the possible network security problems in the next period, to prevent and respond in time based on E-learning system.

2 Background

2.1 E-learning

Traditional distance education is referred to teach by correspondence commonly. Educational information is mainly disseminated through the printed word. It is characterized by low cost, easy to organize and implement. But the drawbacks are also obvious, less information, difficulty in learning, lack of communication between teachers and students, the long learning cycle, and the low learning efficiency. E-learning is a new educational pattern with the rapid development of network technology and multimedia technology [4]. Compared with traditional education, it is not limited by the time and space of education. E-learning is a new educational pattern with the rapid development of network technology and multimedia technology. People cannot be limited by time and space and complete interactive teaching and learning activities anytime and anywhere. They do not have to be at the designated place and time.

2.2 Situational Awareness

Before situational awareness, the main idea of the security event statistical analysis method is to obtain the network security situation by using the influence of the intrusion detection system or other detection systems. The generated alarm logs are statistically analyzed to obtain network security event information to analyze the network attack.

Tim Bass [5] proposed to use distributed multi-sensor data fusion method of the intrusion detection system to evaluate the security situation of computer networks and to evaluate the security of computer networks through data fusion and data mining method. The intrusion detection data fusion framework is shown in Fig. 1. The security situation assessment results are obtained through steps such as data extraction, object extraction, situation extraction, threat assessment, and resource management.

Situational awareness is an environment-based, dynamic, and comprehensive insight into security risks. It is based on security big data to improve the ability to detect, identify, understand, analyze, and respond to security threats from a global perspective [6]. It is to predict the future development trend of the network for decision-making and action. Situational assessment first appeared in the field of aviation and military, and then gradually spread to various technical fields, including traffic management, production control, logistics management, medical research, and ergonomics. In recent years, situation assessment techniques have been applied to computer networks. The cyberspace situational awareness process [7] can be divided into three stages.

2.3 Cyber Security and E-learning

The security of an e-learning system includes steps to limit the danger and threat of network assaults, such as the deployment of security management (security rules, procedures, and processes), enhanced verification tools and control of access; Users with varying levels of permission based on their status; Backup software that runs automatically; Encrypt critical or sensitive data; Firewall, antivirus, and anti-spam software [3]. Most of the E-learning security research is focused on four areas: vulnerabilities, security threats, cyber-attacks and privacy.

Ramim and Levy (Ramim & Levy, 2006) advocate for academic institutions to develop proactive security measures for e-learning systems. Zuev [1] suggests using cybersecurity metrics as a tool that can also help assess the level of risk in not performing a particular action, and in that way provide direction in prioritizing corrective action. Rjaibi et al. [8] discuss that security techniques for quantifying security threats in E-learning are like those used in other E-services. Anghel and Pereteanu [10] stated that E-learning devices can be vulnerable, hacked, and when connected to networks, they can cause cybersecurity breaches and influence data that are vulnerable to protection and privacy. Hage [11] E-learning systems can collect information about learners, which has implications for their privacy, and people are concerned about protecting the privacy of learners.

3 Methodology

Raw data are classified into asset data, threat data, and vulnerability data. The security event data set is obtained through comprehensive analysis by correlating asset threat and vulnerability. After obtaining the threat information, it is necessary to carry out intrusion detection on the E-learning system. By collecting and analyzing network behavior, security logs, audit data, other information available on the network, and information of some key points in the E-learning system, it checks whether there is behavior violating security policy or signs of an attack in the network or system.

3.1 E-learning Situation Monitoring and Warning System

Based on the network attack database to form a multi-dimensional knowledge map of the event components, and based on the algorithms, tools, and knowledge models of relational reasoning, network terrorist attack events can be excavated and analyzed in the space-time dimension. The situation analysis of the cyber-attack event "4W1H" (who, when, where, what, how) is realized in the department of electronics.

The security situation assessment value of the whole network can be written as:

$$A = \sum_{i=1}^{n} (V_i, T_i, S_i) * (s_{iv}, s_{iT}, s_{iw})$$

Where Vi represents the vulnerability state value of node i, Ti represents the threat state value of node i, and Si represents the operating state value of node I. S_{iV} represents

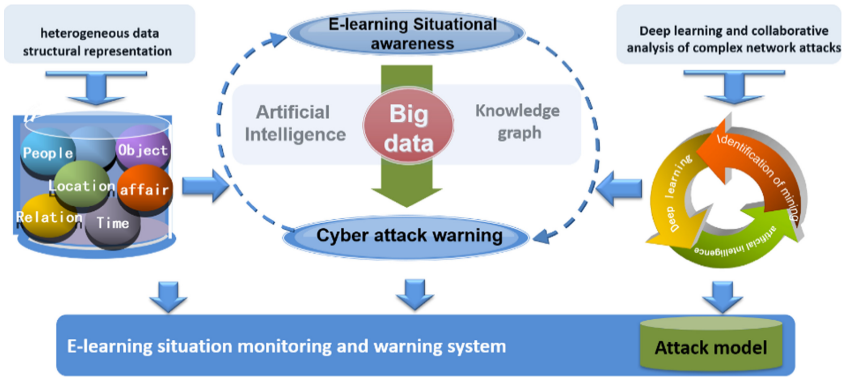

Fig. 1. E-learning situation monitoring and warning system

the vulnerability weight of node i, S_{iT} represents the threat weight of node i, and SIS represents the health status weight of node i. The value weight of each situation can be based on the topology structure of different nodes in the network and the importance of the cluster.

Algorithm 1 E-learning cyber-attack detection rate

Input: Enter E-learning system information, Vulnerability of user, cyber-attack information;

Output: Attack detection rate

```
HashMap ElearningInfo(key:userVulnerability, value:List[Cyber-attackInfo])
HashMap
DetectElearningAttack(userVulnerability,cyber-attackInfo, ElearningInfo)
function MatchVulnerability(userVulnerability,cyber-attackInfo)
att_i == Hashmap(vul_i)
return vul_i
end function
let Attack detection rate = 0
for attack type att_0, att_1, ..., att_n do
    Elearning_Defence = detect_vul(vul_i, UserInfo)
end for
if then(Elearning_Defence == 1)
    Attack_detection_rate+=weight_i
    Where weight is the weight vul_i
else
    return 0;
end if
return Attack_detection_rate
```

As shown in Algorithm 1, the E-learning system vulnerability information contains all the necessary vulnerabilities store in a HashMap. The vulnerabilities match the cyber-attack, for example, DDoS, that exploit the type of E-learning system vulnerability to attack. If the E-learning defensive successful rate is 1, then it will return the add up the

weights of user vulnerabilities included, namely, attack success support probability Si. Finally, the attack detection rate will be calculated correctly.

4 Evaluation

In the network security situation analysis of this example, the network security situation is directly calculated by using the expected threat of the network host node. The network security situation quantitative assessment algorithm uses the information fusion method to calculate the number of attacks on the e-learning network host and then calculates the security situation value of each period through the comprehensive calculation method.

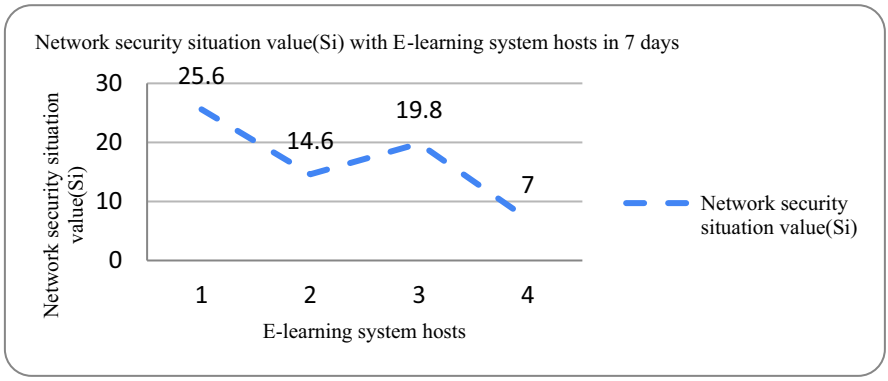

Fig. 2. Network security situation value with E-learning system hosts in 7 days

According to the calculation results of the actual e-learning system experiment, the graph of the network security situation is obtained, as shown in Fig. 2. Then, when the weight of the No.1 Host is relatively large, the system will be subjected to a relatively large value of network security situation.

5 Conclusion

This paper proposes three functional requirements, namely situational awareness scheme to access E-learning system, emergency disposal decision support and intelligent optimization of network security system, analyzes the E-learning system network security situation value and corresponding technical requirements of the network security vulnerability data platform, and designs the technical architecture of the platform accordingly. The system adopts a layered modular architecture with high scalability. Combined with operational modules such as work order distribution and one-click processing, the system can run a detection algorithm of network attack rate based on an E-learning system. The application layer of the E-learning situational awareness system platform can cover the network security domain, from the whole chain of attack detection, threat awareness, event processing, knowledge base construction, and sustainable feedback improvement, to realize a more comprehensive, timely, and intelligent network security comprehensive defense and protection.

Acknowledgment. This research is supported by the: 1. project funded by Zhuhai Industry-University-Research Cooperation Project: Research on Key Technologies of Cross-domain Data Compliance and Mutual Trust Computing in Zhuhai and Macau (No. ZH22017002200011PWC) 2. Research on knowledge-oriented probabilistic graphical model theory based on multi-source data (FDCT- NSFC Projects: 0066/2019/AFJ) 3. Research and Application of Cooperative Multi-Agent Platform for Zhuhai-Macao Manufacturing Service (0058/2019/AMJ).

References

1. Zuev, V.I.: E-Learning security models. Manag. Inf. Syst. **7**, 24–28 (2012)
2. Mohd Alwi, N.H., Fan, I.S.: Information security threats analysis for e-learning. In: Lytras, M.D., et al. (eds.) Technology Enhanced Learning. Quality of Teaching and Educational Reform. TECH-EDUCATION 2010. Communications in Computer and Information Science, vol. 73, pp. 285–291 Springer, Berlin (2010)
3. Costinela-Luminita, C.D., Nicoleta-Magdalena, C.I.: E-learning security vulnerabilities. Proc. Soc. Behav. Sci. **46**, 2297–2301 (2012)
4. Lam, T. Y., Dongol, B.: A blockchain-enabled e-learning platform. Interact. Learn. Environ. 1–23 (2020)
5. Bass, T.: Intrusion detection systems and multisensor data fusion. Commun. ACM **43**, 99–105 (2000)
6. Li, Y., Huang, G., Wang, C.Z., Li, Y.C.: Analysis framework of network security situational awareness and comparison of implementation methods. Eurasip J. Wirel. Commun. Netw. **2019**(1), 1–32 (2019)
7. Vicentel, K.J., Rasmussen, J.: Proceedings of the human factors society 32nd annual meeting 1988, pp. 254–258 (1974)
8. Rjaibi, N., Rabai, L., Aissa, A., Louadi, M.: Cyber security measurement in depth for E-learning systems. Int. J. Adv. Res. Comput. Sci. Softw. Eng. **2**, 1–15 (2012)
9. Ramim, M., Levy, Y.: Securing e-learning systems: a case of insider cyber attacks and novice IT management in a small university. J. Cases Inf. Technol. **8**, 24–34 (2006)
10. Anghel, M., Pereteanu, G.C.: Cyber Security Approaches in E-Learning. INTED2020 Proceedings, vol. 1, pp. 4820–4825 (2020)
11. Hage, H.: Web2.0, Knowledge Sharing and Privacy in E-learning. vol. NR74910 (2010)
12. Aïmeur, E., Hage, H., Onana, F.S.: M. Anonymous credentials for privacy-preserving E-learning. In: Proceedings 2008 International MCETECH Conference e-Technologies, MCETECH 2008, pp. 70–80 (2008). https://doi.org/10.1109/MCETECH.2008.26