Security and Privacy in E-learning

Weigong Feng[1,2](✉), Wennan Wang[1], and Fengling Wang[1,3]

[1] Institute of Data Science, City University of Macau, Macao 999078, China
[2] Beijing Institute of Technology, Zhuhai 519000, China
[3] Hezhou University, Hezhou, Guangxi 542899, China

Abstract. E-learning has the advantages of flexible and diverse learning methods, and the high-quality teaching resources can be shared without limitation by time and space, it has been developed rapidly. Especially after the outbreak of the COVID-19, World began to widely replace traditional classroom teaching with E-learning methods, it leading to an explosive growth. During the use of E-learning, many security problems and privacy leakages have occurred. In This paper, we have analyzed the four main security threats faced by E-learning, summarized the current main research results and gave corresponding countermeasures and suggestions, which have certain positive significance for improving the security and privacy in E-learning.

Keywords: E-learning system · Data security · Communication safety · Virus prevention · Intrusion defense

1 Introduction

E-learning refers to the use of computers or other smart devices and Internet technology to use certain methods to teach in a virtual space online. E-learning systems have the advantages of flexible learning forms, diverse learning methods, and high-quality teaching resources that can be widely disseminated. In the past two years, especially in the context of the global COVID-19 pandemic, there is a great demand for E-learning and online meetings, leading to an explosive growth. E-learning platforms include ZOOM, MOOC, Tencent Class, NetEase Cloud Class, Litchi Micro Class, etc. Although they have corresponding privacy protection protocols and measures, they still have security issues and the privacy leakage risks in the application process. So the research on the security and privacy protection of E-learning is of great practical significance.

2 Main Threats Facing E-learning

E-learning are faced with the risk of man-made, natural or external intrusions, which are specifically reflected in:

W. Zhou and Y. Mu (Eds.): ICWL 2021, LNCS 13103, pp. 129–133, 2021.
https://doi.org/10.1007/978-3-030-90785-3_11

2.1 Computer Virus Attacks

Computer viruses will cause different degrees of damages to the computer or network, including disrupting normal operations, deleting data, occupying system resources, stealing privacy, automatically restarting the computer, crashing, and freezing, etc. In the large-scale E-learning carried out since 2020, virus infections have often occurred, Therefore, virus attacks are one of the main threats to the security of E-learning platforms.

2.2 Data Leakage of E-learning Platforms

E-learning platforms hold huge amounts of data which are related to personal privacy. If these data or part of the data are leaked, attackers can obtain a large amount of personal private information through data analysis and mining. If this information is used to infringe upon others, it will inevitably have a serious impact on the people involved. Recently, there have been many incidents of data leakage from online teaching platforms. Therefore, it is very necessary to take corresponding measures to protect the data of E-learning platforms.

2.3 Risks of Online Communication

E-learning is a way of classroom teaching and knowledge dissemination through PC, mobile phone, PAD, Internet, wireless network and so on. Due to the openness and complexity of the system, it inevitably has some defects and vulnerabilities, such as protocol vulnerabilities, hardware vulnerabilities, and system vulnerabilities. Therefore, the network communication security in E-learning is also one of the key topics of research.

2.4 Illegal Invasion

Illegal intrusion is leading to the destruction of the availability, confidentiality and integrity of the system or network. From the beginning of E-learning practice, it can be seen that illegal intrusions have occurred from time to time, and there are diversified ways of intrusions. Therefore, in the face of the new complex environment, traditional intrusion detection is not suitable for direct deployment, and a new solution should be designed to deal with illegal intrusions.

3 Countermeasures

3.1 Virus Detection and Removal

Computer virus detection technologies are mainly divided into two types, one is to establish virus detection based on the feature classification. The other is a detection technology that does not target the viruses themselves. Antivirus software can detect the existence of computer viruses, prevent infection and damage caused by the viruses, and repair programs infected by viruses. At present, the mainstream domestic antivirus software includes Rising Antivirus, 360 Antivirus, Norton Internet Security Guardian, etc. Anti-virus software is mainly used to prevent the harms caused by viruses, and firewall software can be used to prevent hacker attacks. In order to prevent illegal platform data access and maintain the security of the system, E-learning systems should install anti-virus software in the terminals, and set up firewall software between the system and the Internet. Regular maintenance and upgrades are also necessary.

3.2 Solutions of E-learning Data Security

One of the security technologies can be used in E-learning data security is data encryption. Since the teaching platform terminals include devices with limited computing capacity and storage space, lightweight cryptography can be used to provide security protection. The method of digital signature can provide security performance which is difficult to achieve by other methods. The elliptic curve digital signature algorithm has the characteristics of high computational efficiency, so it is widely accepted in many applications with short key lengths. Such typical lightweight password protection technologies be adopted for the data or part of the data in E-learning platforms.

In terms of copyright protection, data authorization management is one of the main strategies to reduce the copyright risk of E-learning. In terms of student privacy and trust. Deraw [1] proposed solutions to the security vulnerabilities of Moodle, an open-source E-learning platform. Amor AB et al. [2] proposed a security fog E-learning solution, achieve the effects of data confidentiality, fine-grained access control, anti-collusion in exams, high efficiency and low encryption cost. Banerjee et al. [3] proposed an E-learning system security model based on the Unified Modeling Language (UML) to ensure the trust and security among participants in the E-learning system.

In terms of data statistics and release, a differential privacy mechanism can be used, it can ensure that the statistical characteristics of the data set remain unchanged, while protecting the privacy of the users. In terms of data identification in the process of E-learning, blockchain technology can be adopted. Combining blockchain technology with E-learning platforms will be the future trend.

3.3 Communication Security Protocol of E-learning

IP security (IPsec) is an open standard of IP network security. It provides a security strategy for each IP data packet transmitted from the source to the destination, and provides a security performance in the communication on LAN, WAN, and Internet. Another security encryption protocol is the Transport Layer Security (TLS), which can provide a complete set of digital certificate-based identity authentication and data encryption solutions. Hyper Text Transfer Protocol over Secure Socket Layer (HTTPS) provides methods of identity verification and encrypted communication, and is widely applied in security-sensitive communications on the World Wide Web. Secure Shell (SSH) can effectively prevent information leakage in the process of remote management. The security of E-learning platforms may also involve the security of the wireless network. The main threats faced by wireless transmission are eavesdropping, modification of messages, insertion of messages, and damages. The security countermeasures against eavesdropping are signal hiding technology and encryption; the standard methods for dealing with attacks of modification or inserting are encryption and authentication protocols;

the technologies against DOS attacks include prevention, detection, filtering, tracking, and identification.

3.4 Intrusion Prevention Technologies

Intrusion detection technology is currently one of the core technologies for network security defense It is an active defense technology that can effectively prevent unknown attacks. It is a necessary supplement to the firewall, and the two together constitute a complete solution of network security. H Ibrahim [4] put forward the idea of using firewall, biometric authentication, data encryption and digital rights management to build an E-learning database management system to cope with network security challenges.

Intrusion detection technology can detect attacks, send alarms, and form logs, while intrusion prevention system (IPS) can conduct real-time active detection, prevent intrusions and attacks from occurring. IPS integrates firewall technology and intrusion detection technology. IPS can be divided into host-based intrusion prevention system (HIPS) and network-based intrusion prevention system (NIPS). HIPS can monitor file operation and registry modification in the host, and make requests for permission. It represents a trend in the development of system security, which can prevent information tampering, Trojan horse backdoor attacks, process termination, etc. But HIPS cannot prevent other computers on the network from attacking the host; NIPS can provide various functions of attack detection and defense, accurately identify network traffic, reduce the rate of false reports and under-reports, and can meet high-performance requirements, guarantee the quality of normal network communication. Nowadays, in the context of increasing threats of viruses, worms, Trojan horses, spyware, DDOS, and hacker attacks, E-learning platforms should deploy intrusion prevention systems in a timely manner based on their actual conditions.

4 Suggestions

E-learning security is a systemic issue, and only a robust security mechanism can ensure the safe operation of the teaching system. For different risks of the E-learning, different protection methods can be adopted. The traditional method of password login has high security risks; Therefore, third-party authentication, dynamic password authentication, or face recognition should be used to improve security. At the same time, platforms must have mechanisms to defend against viruses, Trojan horses, and various types of attacks, and constantly improve their defense capabilities.

Platform developers should regard security and privacy protection as part of system development, continuously enhance the security performance of the system. In the process of platform development and use, they should do a good job in the security maintenance of the platform, and conduct timely inspections and updates. Relevant administrative authorities should establish and improve relevant legal systems and establish a complete legislation system of network safety. Users of E-learning platforms should do a good job in the safety management of the terminal equipment, deal with the security incidents of the terminal equipment in a timely manner, use the E-learning platform in a reasonable and normative manner, thus jointly creating a safe and stable teaching and learning environment.

References

1. Derawi, M.: Securing e-learning platforms. In: International Conference on Web and Open Access to Learning, IEEE (2015)
2. Amor, A.B., Abid, M., Meddeb, A.: Secure Fog-Based E-Learning Scheme. IEEE Access **8**, 31920–31933 (2020)
3. Banerjee, S.: Designing a secure model of an e-learning system—a UML-based approach. IEEE Potentials **29**(5), 22–27 (2010)
4. Ibrahim, H., Karabatak, S., Abdullahi, A.: A study on cybersecurity challenges in e-learning and database management system. In: 2020 8th International Symposium on Digital Forensics and Security (ISDFS), IEEE (2020)