Research on the Network Security Strategy for Digital Distance Education Platform

Minzhu Zhang[1,*] and *Xiaofei* Dong[2]

[1]Teaching Affairs Department, Suzhou Chien-Shiung Institute of Technology, 215411 Taicang, China
[2]School of Mecheanical Engineering, Yancheng Institute of Technology, 224051 Yancheng, China

Abstract. Distance education has been an important development tendency and learning platform with the emphasis of lifelong learning of the society. Networked learning and teaching is a main characteristic of distance education, which inevitably needs to transmit large magnitude of private data among students, teachers and the education platform. To protect the security of data transmission and storage, a networked security strategy was proposed. The security strategy is based on the technologies of intrusion detection and digital signature. An intrusion detection model was established in accordance to the main tasks of distance education platform. The encryption process of digital signature was illustrated along with the information flow of the distance education platform. The paper offers an effective reference for solving security problems of distance education platforms.

1 Introduction

Distance education, also called distance learning, is defined as an education model that lesson giver and accepter are not face-to-face but through media such as networked computer. Distance education is not a fixed concept but a developing one, which is based on the development of computer network. Current trends in the field of distance education indicate a shift in pedagogical perspectives and theoretical frameworks, with student interaction at the heart of learner-centered constructivist environments [1]. It has been said that correspondence study represents not only as historical legacy but a continuing dominance of distance education practice. And assumptions regarding learning are implicit in designs of instruction and education [2]. With the development of distance education, many researches about networked technology of distance education have been studied. For example, Hillman et al [3] have found that the interaction occurred between the learner and the technologies used to deliver instruction has not been well considered. Therefore they presented the concept of learner-interface interaction and recommends instructional design strategies that facilitate students' acquisition of the skills needed to participate effectively in the electronic classroom. Berge [4] has list the roles, tasks, and functions of a computer conference moderator used to promote students' learning skills.

Modern distance education mainly relies on digital satellite transmission and computer network, adopting multi-media resource and methods, to form a personalized learning style, which is suitable for different students, especially for those who are not convenient assessable to school. Distance education has become an expectation with students who have grown up with technology as well as nontraditional and working students. Most universities now offer a wide range of online courses and degree programs to meet these needs [5]. The education department of many countries, such as America, British, German, and China, have taken distance education as an important tendency of developing lifelong learning. Distance education has many special merits that traditional education cannot achieve, such as owning broad coverage over students of different ages, low cost, not limited to the basic infrastructures, and not limited to teachers and other teaching materials, which has been widely accepted by mass.

However, with the rapid development of Internet, network security has been a more and more severe problem. And web-based distance education is also facing the same problem, such as virus infection, illegally access to database, account and PIN code theft, information leakage, distance attack, which often lead to teaching activities not carried normally. Unsafe environment will bring lots of incontinence to students. Lin et al [6] focused on how tool development can combine with security to provide a safe, efficient, and effective learning environment, and put forward a number of distance education applications developed in our lab and show how security and privacy may be integrated into these applications. Stallings [7] proposed there are two requirements for secure use of symmetric encryption: a strong encryption algorithm and a secret key known only to senders or receivers. Hoque et al [8] adopted Genetic Algorithm to implement the intrusion detection system. The evolution theory to information evolution is applied in this paper to filter the traffic data

[*] Corresponding author: 310897265@qq.com

and thus reduce the complexity. Rao et al [9] presented a support vector machine-based intrusion detection system, and the paper has given a comparison of detection ability between different detection method and the method proposed in this paper. Bauer and Koblentz [10] have described a knowledge-based prototype network intrusion detection expert system, which combines knowledge describing the target system, history profiles of users' past activities, and intrusion detection heuristics from a knowledge-based system capable of detecting specific violations that occur on the target system. Patel et al [11] identified a list of germane requirements by considering the desired characteristics of intrusion detection system and cloud computing systems and provided an appropriate set of all possible solutions and a layered taxonomy of intrusion detection system. Johnson et al [12] has described the digital signature technology called the elliptic curve digital signature algorithm and discusses related security, implementation, and interoperability issues. Courtois et al [13] has studied an approach of achieving McEliece-based digital signature scheme, which is based on one of the oldest known public key crptosystems.

In this paper, the strategy network security management will be studied in accordance to the requirement of distance education system.

2 Safety requirements of distance education system

The network system of distance education has distinct deficiency of existing network, operation system and serve leakages, the distance education platform sometimes will receive active and inactive attacks from Internet visitors. The adoptable security measures for distance education mainly includes following sides.

- The security of Internet serve is mainly assured through setting management of password and user access limitation, visiting control of networked resources. Feasible and useful measurements of maintaining Internet serve is the best method of defending outside attacks.
- Establishing physical security transmission media and encrypting transmitted data are two different ways of ensuring transmission security of Internet platform of distance education. For transmitting teaching resources such as students' test paper or grades, an encrypting algorithm will be applied to the communication of data link and end-to-end. Thus even the illegal invader has got the data, he still cannot read the data, and the security of the network is safeguarded.
- The firewall is the primary security technology of computer network system, which is assembled between outside Internet and the innernet of distance education platform. The firewall is currently one of the most effective security measures to prevent illegal invasion. As the blocking and control point, firewall can greatly reduce the risk of network system through filtering unsafe and uncertain services.

Detection technique is divided into anomaly detection and misuse detection. Pattern matching technology belongs to misuse detection, which is the most commonly used. A data detection technology is the most practical and widely used technology. Only deepen research on intrusion detection method can make faster and better development of intrusion detection technology. The intrusion detection method of the core will be very meaningful and effective. The efficiency of detection can be improved by integrating more flexible and effective into the intrusion detection system.

3 Intrusion detection of distance education system

In a practical intrusion detection system, the most important part is the detection model, which determines what kind of technology will be used for the intrusion detection. Intrusion detection system provided in this paper aims on transferring static protection to dynamic protection, through consistency inspection, traffic statistics, and pattern matching and application. Intrusion detection system of distance education platform is based on common intrusion detection framework, of which the basic framework is shown in Figure 1. The intrusion detection system is mainly made up of the following four pats. The system need to analyse the data known as events, and the events is based on network data packet, which can also be based on a host system log. The main function of event generator is to acquire events from the whole computer environment and offer the events to other parts of the system. The analysing results will be sent to the event analyser. Responding element will make out suitable and repaid responds to results sent by event generator. The responding element can make drastic responds such cutting off linkage and revising file attributes. Event database is a place in the system where the intermediate and final data are stored.

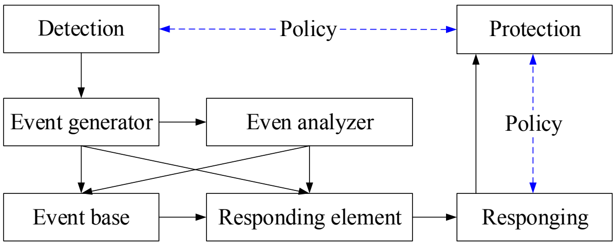

Fig. 1. Intrusion detection model for distance education system

The technology of intrusion detection system can be simply divided into two categories: feature based detection and anomaly based detection. The feature based detection mainly includes protocol analysis and pattern matching. Network intrusion detection method based on information system and pattern matching is known and will be collected from the misuse of pattern knowledge were compared to find the intrusion. The protocol analysis with respect to the pattern matching technology is a kind of intrusion update the detection technology. It captures data packets, and then analyze the data packets, including network protocol and command parsing, quickly detect some attack characteristics in the parsing code. Anomaly detection technology based on a lot of factors, such as the use of statistical model, expert system technology. It is the first important thing to make a statistics on the behavior of the system, the statistical performance of normal use of the system, such as the number of visits, operation failure times and delay. The statistical performance is used to compare with the network, the behavior of the system, when the observed values in the normal range, the intrusion detection system will determine the invasion.

3.1 Main tasks of intrusion detection system of distance education platform

The main task of intrusion detection system for distance educations platform has its own specialties, which are mainly generalized as the following items: 1) monitoring, analysis of user and system activity of the distance education platform; 2) proceeding statistical analysis of abnormal behavior patterns and issue intrusion regulations; 3) checking the correctness of configuration and security vulnerabilities of the distance education system, and prompting the administrator to patch the vulnerability; 4) responding in real-time to the intrusion behaviors; 5) assessing the integrity of key resources and data files of the system; 6) tracking audit management of the operating system, and identifying the breach of security strategy. Though firewall and intrusion detection system are both helpful to the security of the distance education system, but there still exists distinctive difference. System firewall is an important defense, which no longer do any operation on the data that has passed through the firewall. However real-time intrusion detection will respond immediately in case of new invasions, which is an important completion of the defense of firewall. Firewall allows some inner hosts can be accessed externally, while intrusion detection does not have these functions, but monitoring and analyzing the activities of the users (students, teachers, and local teaching spots) and the system of distance education.

3.2 Framework of intrusion detection system

A complete intrusion detection system is typically made of data collecting model, data analyzing model, data management model, data preprocessing model, communication model, data storing model, and data responding model. Data from Internet are collected by the data collecting model and preprocessed by data preprocessing model, and transferred to data analysis model. Data management model provides information overflow with users through user interface model. Data preprocessing model includes many functions such as data filtering, data classifying, data merging and data converting. A typical structure of an intrusion detection system can be illustrated by the following figure (as shown in Figure 2).

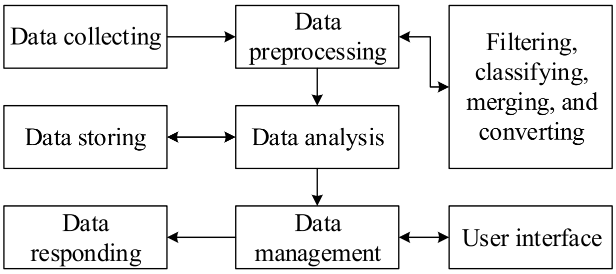

Fig. 2. The basic structure of an intrusion detection system

3.3 Strategy of digital signature for distance education platform

With the rapid growth of Internet, a great need has appeared for a mechanism capable of protecting the ownership of video or image authors and distant learning resource providers. A classical means to protect distant learning material is known as "Digital Signature", where the video or image-data material is slightly modified ("signed") in order to embed a number or image or other information, which can later be retrieved [14][15]. With the application of digital signature, the teaching resources and private information of learners are well protected. Digital signature is a kind of technology that utilize sending port to produce an encoding algorithm which is difficult to be enciphered.

The digital signature has a unique specialty of the signer, which is difficult to be stolen and revised by illegal attackers. The encoding, transmission and decoding process of the digital signature can be expressed as the following three steps: firstly, the learner encodes the information by encoding key which only be mastered by himself or herself; secondly, the learner transmits the encoded information to the other person who he or she want to send to; finally, the accepter decoding the information by secret key and calculate the characteristic value through a HASH function, and compare the characteristic value with digital signature. If the characteristic value is not changed that means the information has been safely transmitted and accepted.

For distance education platform, the strategy of digital signature needs to meet following requirements. The digital signature needs to be pre-versified. The distal signature can keep the intact of the file which is transmitted between the learner and teacher through Internet. The application model of digital signature used between teachers and learners for distance education plater is illustrated by Figure 3.

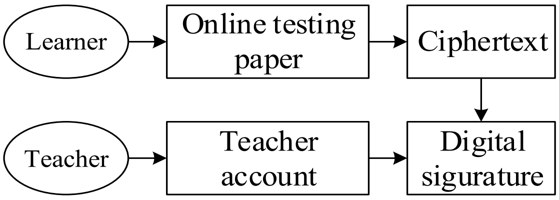

Fig. 3. The basic structure of digital signature for distance education platform

3.4 Strategy of digital signature for distance education platform

Through distance education platform, students carried a series of learning activities, which are encrypted into protective Class-One File by Key One, then encrypted into Class-Two File by Key Two, next into Class-Three File by Key One, finally applying for an public key of a certain curriculum from the distance education platform. The Class-Three File will be finally encrypted into a Class-Four File by the public key, thus the whole encrypting process is complete. When students or local learning spot received a secret file from education management department through the distance education platform, a private key need to be applied from the private key generator to decrypt the secret file into a readable file. The process of applying digital signature on the platform of distance education can be modelled by the Figure 4.

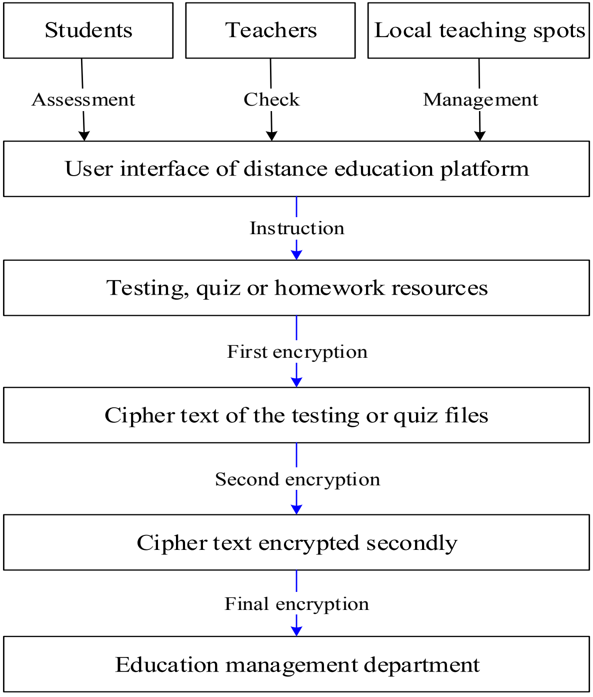
Students
Teachers
Local teaching spots
Assessment
Check
Management
User interface of distance education platform
Instruction
Testing, quiz or homework resources
First encryption
Cipher text of the testing or quiz files
Second encryption
Cipher text encrypted secondly
Final encryption
Education management department

Fig. 4. The process of applying digital signature on the platform of distance education

4 Conclusions

With the development of the concept of lifelong learning, more and more people, especially adults, have resorted to Internet to acquire the knowledge they want. Under the requirement of convenient accessing learning resources and guidance of teachers, lots of distance education platforms have been developed and applied on the purpose of mass learning. However, information security is an important task that needs to be dealt with by the developers of the distance education platforms. Learning and teaching via user interface is a main characteristic of distance education, which inevitably needs to transmit large magnitude of private data (such as delivering test paper, individual homework and quizzes, handing over finished paper, and correcting and grading the test paper) among students, teachers and the education platform. A strategy of intrusion detection and digital signature is very useful to protect the security of data transmission and storage through distance education platform. An intrusion detection model was established in accordance to the main tasks of distance education platform. The encryption process of digital signature was illustrated along with the information flow of the distance education platform.

6 Acknowledgments

The authors gratefully acknowledge the support by Taicang Key Project of Research and Development Plan (Industry Perspective and Common Key Technologies) under Grant No. TC2016GY07 and Jiangsu Provincial Policy Guidance Program (Enterprise-University-Research Institute Cooperation)-Perspective Joint Research Program under Grant No. BY2016065-52.

References

1. Y. Beldarrain. *Distance education*. 27, 2 (2006). *Distance education*. 27, 2 (2006)
2. D.R. Garrison. *Distance education.* 14, 2 (1993).
3. D.C. Hillman, D.J. Willis, and C.N. Gunawardena. *American Journal of Distance Education*. 8, 2 (1994)
4. Z.L. Berge. *Educational Technology-Saddle Brook NJ-*, 35, 22-22 (1995).
5. S.W. Tabor. *Quarterly Review of Distance Education.* 8, 1 (2007)
6. N.H. Lin, L. Korba, G. Yee, T.K. Shih, and H.W. Lin. *In Advanced Information Networking and Applications, 2004. AINA 2004. 18th International Conference on* IEEE. 1 (2004)
7. W. Stallings. *Pearson Education India.* (2006)
8. M.S. Hoque, M. Mukit, M. Bikas, and A. Naser. *arXiv preprint arXiv*. 1204.1336 (2012).
9. X. Rao, C.X. Dong, and S.Q. Yang. *Journal of Software*. 14, 4 (2003): 798-803.
10. D.S. Bauer, and M.E. Koblentz. *In Computer Networking Symposium, Proceedings of the IEEE.* (1988) 98-106
11. A. Patel, M. Taghavi, K. Bakhtiyari and J.C. JúNior. *Journal of network and computer applications*, 36, 1 (2013) 25-41
12. D. Johnson, A. Menezes, and S. Vanstone. *International Journal of Information Security.* 1, 1 (2001) 36-63.
13. N. Courtois, M. Finiasz, N. Sendrier. *Advances in Cryptology-Asiacrypt*. 2248 (2001) 157-174.
14. T. Vynne, and F. Jordan, Cray Research, Inc., Embedding a digital signature in a video sequence. *U.S. Patent 5,960,081*. (1999)
15. M. Abdalla, and L. Reyzin. *In International Conference on the Theory and Application of Cryptology and Information Security*. *Springer Berlin Heidelberg* (2000)