Impersonation Attack-Defense Tree

https://doi.org/10.3991/ijet.v15i19.12699

Yusep Rosmansyah (✉), Ignatius Leo Sri Hendarto, Demby Pratama
Bandung Institute of Technology, Bandung, Indonesia
yusep@stei.itb.ac.id

Abstract—Nowadays, online learning or e-learning has become increasingly popular and evolved. Many academic institutions use the Learning Management System (LMS) as a medium for delivering e-learning. A vital feature in such a system is the electronic examination (e-exam), where verifying student's authentic competence is a challenge. This paper aims to present countermeasures for impersonation attacks. This research was a more focused effort and a continuation of previously owned one and many others found in works of literature. The method of protection is presented in the form of an attack-defense tree model.

Keywords—Attack-defense tree, impersonation, online exam.

1 Introduction

Educational institutions use online learning systems to deliver learning materials. Through these systems, students can interact and perform learning activities from remote locations online. This practice raises stakeholder's security concerns. Concerns have also increased in the integrity of the online exam process, which is one of the crucial activities in online learning [1].

Despite information security technological advancement, which has also been developed in recent years, reportedly, integrated and holistic security models have not been completely implemented yet. Learning Management Systems (LMS) have deployed advanced security methodologies, but there are too many problems that cannot be solved [2]. Electronic examination (e-exam), which is one of the critical activities in the learning environment for assessing students, is a significant concern in education. E-exam has started to replace the traditional paper-based exam in learning environments. E-exam delivers several advantages, including opportunities for optimum learning, automatic marking, and immediate feedback. Furthermore, e-exam procedures are developed to enhance the educational learning environment and provide adequate information regarding the progression of the educational process [2].

E-exams can be delivered through specific applications or incorporated into e-learning systems, namely the learning management systems (LMS). Open-source LMS that provides e-exams is freely available to users who can modify it accordingly [3]. Many educational institutions adopt this system because of its greater flexibility and lower cost than other systems. Another advantage is that even though their code is

freely available, technical support teams are required to change or modify the code, install the system and maintain it. The integrity of free source codes can also be a cause of security problems. Some examples of open-source LMS are Sakai, Chamilo, and Moodle. Two open-source LMS, Moodle and Chamilo, are considered more user-friendly for students and instructors than some other proprietary systems.

According to [4], there are seven types of e-exam cheating attacks [5], which are:

1) Impersonation
2) Assistance/collaboration
3) Plagiarism
4) Using aids not allowed for the exam
5) Time violations
6) Lying to proctors
7) Smuggling out the exam questions after the exam

To study attacks and defenses that can be used in e-exams, the researchers developed several models. One model that can be used is the Attack Defense Tree (ADTree) model. The ADTree is a development of the Attack Tree introduced by Bruce Schneier [6]. The ADTree is a method created by researchers to introduce and formalize defense trees as a graphical representation of the steps an attacker might take to attack a system and create protection for the system by defining defenses that can be used for countries to measure attacks. Researchers made the ADTrees formalization done by expanding the attack tree in two methods [3].

In this paper, we will discuss how to extend the Impersonation Attack node in the ADTree e-exam. The process of extending this node is utilizing ADTools by conducting study literature on research that has topics related to the authentication method in the e-exam. Additional objects from each literature are designated as new subnodes.

2 Attack-Defense Tree e-Exam System

An ADTree is a rooted tree with labeled nodes describing the steps an attacker might take to infiltrate a system and the defenses that the owner, as a defender, can apply to guard or secure the system. An ADTree has two different nodes: attack nodes for attackers and defense nodes for defenders. The representation of refinements and countermeasures are two key features that ADTree has. Every node may have one or more children with the same type representing a refinement into sub-goals of the node's goal. If a node does not have any children of the same type, it is called a non-refined node, which represents rudimentary actions. Every node may also have one child with a different type to depict countermeasures. Therefore, an attack node may have several child nodes that represent the attack and one other which defends against the attack. The defending child, in turn, may have several children who refine the defense and one child that is an attack node and counters the defense [4], [7].

Researchers state that six types of attacks can be carried out against e-exam. Those attacks are:

1. Examinee Attack
2. Proctor Attack
3. Device Attack
4. Software Attack
5. Availability Attack
6. Cheating Attack

Each of those attacks has different attack child nodes. In this paper, we will discuss attacks that are part of the cheating attack, the impersonation attack.

3 Cheating Attack-Defense Tree

There are seven types of child nodes that belong to the cheating attack node. They are:

1) Time violations
2) Plagiarism
3) Impersonation
4) Using aids not allowed for the exam
5) Assistance/collaboration
6) Lying to proctors
7) Smuggling out the exam questions after the exam

According to [5] and [8], several methods can be executed to countermeasure the cheating attacks in e-exam as follows:

1. Random seating, especially in exam rooms where students should be from different classrooms.
2. Random questions, such as making choices in multiple-choice questions to 100 types of choices, can use alphabets, letters, and even hex symbols and so on. It can also be done by randomizing the question's number between one student and another.
3. Prohibit calculators and books. Create or add identical applications into the exam system.
4. Random question/answer sequence and display one question at a time.
5. Automated plagiarism checking using specific software.
6. Use biometric authentication, such as face recognition, fingerprint, voice recognition, and behavior.
7. Add a firewall and antivirus.
8. Implementing security management (ISM);
9. Improving confidentiality, authorization, authentication, and accountability.
10. Using cryptography and DRM.
11. Improve the professionalism of officers by training them in the officer's security professional course.

4 Impersonation Attack-Defense Tree Extended

One researcher stated that the impersonation attack node has two sub-nodes, which are label swapping and spoofing candidate [4]. The label swapping attack is done by two collaborating students. They exchange their answers label to each other. If there are Alice and Bob, Alice writes bob's name on her paper and vice versa. This label swapping attack only can be made in a paper exam. It is challenging to implement in the online exam because the label had been done automatically by the system. Spoofing candidate is a type of attack in online exams by impersonating exam users. To prevent this attack, the system must verify the candidate identity by authenticating the users. Several methods can be used to verify the candidate identity. The traditional method to verify the candidate is a Picture ID. The weakness of this method is that the user can fake the ID or use someone who looks a lot like the user, maybe a sibling or a relative. LMS, as a system that delivers the online exam, utilizes usernames and passwords to authenticate users. However, the username and password method will be far more insecure than the picture ID, because candidates can give their access code to someone else (impostors) before the test or while the test is taken [5].

Table 1. Defense for impersonation attack in e-exam

No	Defense	Detailed	Attack	Researcher
1	Biometric	Fingerprint Face Recognition Voice Recognition Behavioral Characteristics (Mouse Movement, Keystroke, Signature, Stylometry)	Replay Attack,	[9],[10],[11] [11],[12],[13] [14] [14]
2	Picture ID	ID Card	Fake ID, Looka-like/Doppelgängers	[5],[11]
3	Username & Password	Website Field Filling	Sharing Credentials	[5],[15]
4	Token-based	Hardware, Smartphone	Sharing Object or applications	[11]
5	Monitoring	Remote Proctors	Censor Bypass	[14]
6	Location	Wi-Fi, IP Address, GPS	Proxy, Fake GPS	[16]
7	Challenge Questions	Text, Image, Dynamic	Sharing Credentials	[1],[17]

Another text-based authentication is challenge questions. This approach is made by building a profile database when users are registering on the e-exam system. Then the question is asked again to be answered following the profile database. Researchers combine this method with the username password method. Three researchers designed a profile-based authentication framework (PBAF) together with a username and password for the authentication of students during online examinations, utilizing a cohort of personal and academic questions as challenge questions [1]. They conducted multiple empirical studies to analyze usability and security threats of text-based, image-based, and dynamic profile questions to mitigate impersonation and abetting at-

tack. In their paper, they invite a third party to impersonate students in an e-exams scenario. They can improve the authentication and defense e-exam system using this method if an impostor share questions to the real account holder using email or instant messaging [17].

Another researcher creates another type of challenge question by using location-based challenge question generating schemes where different types of questions are generated based on users' smartphone locations and presented them to users. They developed a location tracking application on users' smartphones and conducted two real-life studies using four different kinds of challenge questions. The application collects Wi-Fi access point (AP) information periodically in the background and use the information as a profile database of questions [16].

The growth of technology in the biometrics field has led researchers to develop biometric authentication in e-exam systems. One researcher develops a web-based application that offers biometric authentication based on face recognition. The application can use face-recognition during access control, tracking, and assessment. This application could be integrated into currently available LMSs. One research showed that this approach improves security during critical phases in the learning process, especially in e-exam [12].

Another researcher combines traditional authentication (password and username) with fingerprint authentication. That researcher applied the authentication model in distance education where courses are developed in learning management systems. They integrated the authentication in Moodle [10]. Another researcher proposed FingerID, a one-stop solution to eliminate the traditional authentication problem. Other researchers demonstrated that this approach made authentication in LMS more secure, useful, and accessible [9].

Biometric authentications, such as fingerprint, face recognition, voice recognition, or behavior, need specific hardware, such as webcams, fingerprint devices, and microphones. Currently, all these devices are included in notebooks or smartphones so that they are widely used. However, the authentication process requires a high computational ability. For example, in face recognition, both GPU and CPU are processing images and videos, which resulted in a high computing load [11].

Researcher [11] showed token authentication, such as those in banks, can also be used on e-exam. Tokens can be in the form of hardware or software developed by third parties such as Google. The drawback of using tokens as an authentication device is that the devices or applications which generating tokens can be shared.

According to [13], research was combining several technologies to verify e-exam users. They presented an automatic online exam proctoring using a multimedia analytics system. They combined key behavior cues: text detection, voice detection, user verification, active window detection, phone detection, and gaze estimation to continuously monitoring e-exam users. To monitor the visual and audio environment in a remote exam location, the system used multiple hardware, which are one wearcam, one webcam, and a microphone. This method allowed them to detect test-takers cheating at any moment during the exam.

Based on the literature review that we summarized in table 1, we extended ADTree for impersonation attacks, as shown in figure 1. We added five new child defense

nodes as countermeasures for spoofing attacks. In figure 1, the verifying candidate ID can be done by biometric authentication, picture ID, token authentication, location tracking, monitoring by the physical proctor or virtual proctor, username and password and challenge questions. Each defense node had a counterattack to bypass the defense node.

In ADTree, the defense node can be used separately or in combination. For example, researcher [17] combined username password and challenge questions for authentication in the e-exam system. Researcher [14] coalesced username password method, proctor, audio monitoring, and webcam monitoring method as the automated online proctor for e-exam. Researcher [11] fused username password, token, face recognition, and proctor as one system to protect e-exam in a mobile learning environment.

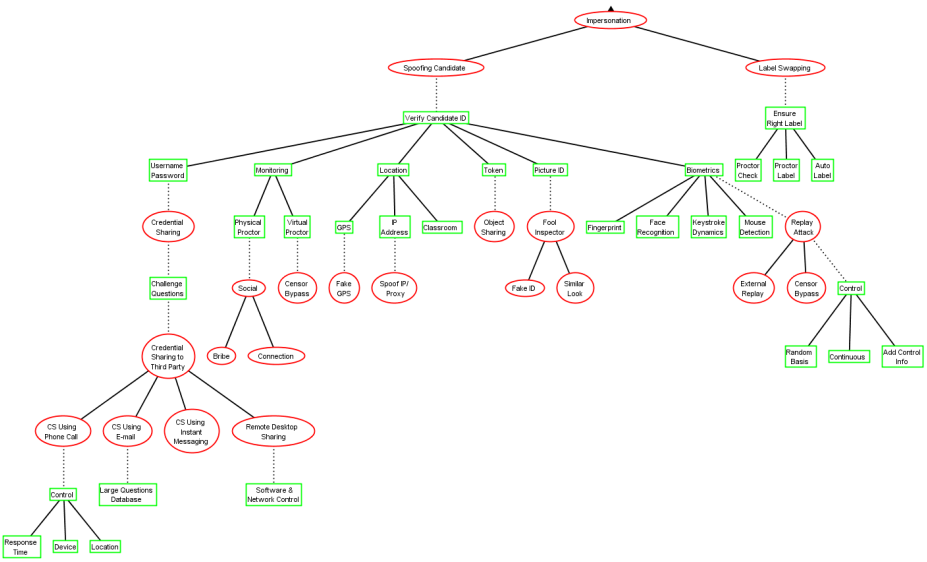

Fig. 1. ADTree Impersonation Attack Extended

5 Conclusion

Present-day e-exam systems face many challenges and attacks. To investigate types of attacks and defenses on the e-exam, the Attack and Defense Tree method were developed. One type of attack that often occurs is impersonation. Impersonation attacks and defenses nodes displayed on the ADTree Secure E-exam are still embryonic. By studying new kinds of literature about authentication on e-exam, the ADTree node of impersonation attack can be extended. In the future, with the advancements of technological developments, there may be newly unpredictable types of impersonation attacks and thus new countermeasures should be added to the ADTree.

6 References

[1] A. Ullah, H. Xiao, and T. Barker, "A study into the usability and security implications of text and image-based challenge questions in the context of online examination," *Education and Information Technologies*, vol. 24, no. 1, Education and Information Technologies, pp. 1–27, Jun-2018. https://doi.org/10.1007/s10639-018-9758-7

[2] Y. Khlifi and H. A. El-Sabagh, "A Novel Authentication Scheme for E-assessments Based on Student Behavior over E-learning Platform," *Int. J. Emerg. Technol. Learn.*, vol. 12, no. 4, pp. 62–89, 2017. https://doi.org/10.3991/ijet.v12i04.6478

[3] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, *Foundations of attack-defense trees*, vol. 6561 LNCS, no. C. Berlin, Germany: Springer Berlin Heidelberg, 2011. https://doi.org/10.1007/978-3-642-19751-2_6

[4] Y. Rosmansyah, M. H. Ritonga, and A. B. Hardi, "An Attack-Defense Tree on e-Exam System," *Int. J. Emerg. Technol. Learn. (iJET); Vol 14, No 23*, pp. 251–260, Dec. 2019. https://doi.org/10.3991/ijet.v14i23.11088

[5] G. Sindre and A. Vegendla, "E-exams versus paper exams: A comparative analysis of cheating-related security threats and countermeasures," *Nor. Internet Secur. Conf.*, p. 12, 2015.

[6] B. Schneier and B. Schneier, "Attack Trees," *Secrets and Lies*. pp. 318–333, 06-Oct-2015. https://doi.org/10.1002/9781119183631.ch21

[7] B. Kordy, S. Mauw, S. Radomirović, and P. Schweitzer, "Attack – Defense Tree Methodology for Security Assessment," *Fonds Natl. la Rcherche Luxemb.*, p. 59.

[8] Y. Chen and W. He, "Security risks and protection in online learning: A survey," *Int. Rev. Res. Open Distrib. Learn.*, vol. 14, no. 5 SE-Research Articles, Dec. 2013.

[9] S. J. Alotaibi and D. Argles, "FingerID: A new security model based on fingerprint recognition for personal learning environments (PLEs)," in *2011 IEEE Global Engineering Education Conference (EDUCON)*, 2011, pp. 142–151. https://doi.org/10.1109/educon.2011.5773128

[10] R. Gil *et al.*, "Fingerprint Verification System in Tests in Moodle," *IEEE Rev. Iberoam. Tecnol. del Aprendiz.*, vol. 8, no. 1, pp. 23–30, Feb 2013.

[11] M. Kaiiali, A. Ozkaya, H. Altun, H. Haddad, and M. Alier, "Designing a Secure Exam Management System (SEMS) for M-Learning Environments," *IEEE Trans. Learn. Technol.*, vol. 9, no. 3, pp. 258–271, 2016. https://doi.org/10.1109/tlt.2016.2524570

[12] E. G. Agulla, L. A. Rifón, J. L. A. Castro, and C. G. Mateo, "Is My Student at the Other Side? Applying Biometric Web Authentication to E-Learning Environments," in *2008 Eighth IEEE International Conference on Advanced Learning Technologies*, 2008, pp. 551–553. https://doi.org/10.1109/icalt.2008.184

[13] Q. Gao, "Biometric Authentication to Prevent e-Cheating," *Int. J. Instr. Technol. Distance Learn.*, vol. 9, no. 2, p. 12, 2012.

[14] Y. Atoum, L. Chen, A. X. Liu, S. D. H. Hsu, and X. Liu, "Automated Online Exam Proctoring," *IEEE Trans. Multimed.*, vol. 19, no. 7, pp. 1609–1624, 2017. https://doi.org/10.1109/tmm.2017.2656064

[15] A. Ullah, H. Xiao, M. Lilley, and T. Barker, "Design, privacy and authentication of challenge questions in online examinations," *2013 IEEE Conf. e-Learning, e-Management e-Services, IC3e 2013*, pp. 46–50, Dec. 2013. https://doi.org/10.1109/ic3e.2013.6735964

[16] Y. Albayram, M. M. Hasan Khan, A. Bamis, S. Kentros, N. Nguyen, and R. Jiang, "Designing challenge questions for location-based authentication systems: a real-life study," *Human-centric Comput. Inf. Sci.*, vol. 5, no. 1, p. 17, Dec. 2015. https://doi.org/10.1186/s13673-015-0032-3

[17] A. Ullah, H. Xiao, and T. Barker, "A Dynamic Profile Questions Approach to Mitigate Impersonation in Online Examinations," *J. Grid Comput.*, vol. 17, no. 2, pp. 209–223, 2019. https://doi.org/10.1007/s10723-018-9442-6

7 Authors

Yusep Rosmansyah is a lecturer at the School of Electrical Engineering and Informatics, Bandung Institute of Technology, Bandung, Indonesia.

Ignatius Leo Sri Hendarto was a graduate student of the School of Electrical Engineering and Informatics, Bandung Institute of Technology, Bandung, Indonesia. leosh232@alumni.itb.ac.id

Demby Pratama was a graduate student of the School of Electrical Engineering and Informatics, Bandung Institute of Technology, Bandung, Indonesia. pratama.demby@gmail.com

Article submitted 2019-12-12. Resubmitted 2020-02-09. Final acceptance 2020-03-31. Final version published as submitted by the authors.