An Attack-Defence Tree of e-Exam System

https://doi.org/10.3991/ijet.v14i23.11088

Yusep Rosmansyah (✉)
Bandung Institute of Technology, Bandung, Indonesia
yusep@stei.itb.ac.id

Mora Hertanto Ritonga, Ariq Bani Hardi
National Cyber and Crypto Agency, Jakarta, Indonesia

Abstract—Not only does the electronic-examination (e-exam) system transform the paper-based into the electronic-based examination, but it also brings about security challenges that must be resolved to guarantee the trust of its users. This paper aims at analysing security challenges of an e-exam system and proposing a solution using Attack and Defence Tree method. The attack tree scheme was defined by risk assessment methods and then evaluated by penetration test experiments against a server running the e-exam application. A proposed defence tree scheme against the identified attack tree was presented as the main contribution of this research. This contribution can be used as a guideline to plan similar e-exam systems and can be served as a starting point for future research towards a comprehensive attack-defence tree of the secure e-exam system.

Keywords—e-exam, attack-defence tree, penetration testing

1 Introduction

As information technology evolves, more and more researchers and organizations deploy electronic examination (e-exam) systems. As stated in [1], an organization that operates the e-exam must concern about security to guarantee information confidentiality, integrity, and availability, and to keep the reputation of the institution. Research about secure e-exams can be found in many studies such as in [2] and [3]. The secure e-exam is also implemented by several e-exam website providers [4], [5], and [6]. One of the e-exam service providers offers several secure e-exam features that are interesting to discuss [6]. The features include secure browser implementation; remote proctoring using the camera on the client device; data encryption using SSL; and audit log.

A study about the design of the Secure Exam Management System (SEMS) was proposed by Kaiiali et al. [3]. The paper provides seven main functions in securing the examination process. These are:

- Distribution of secure and random exam questions
- Turbo mode assessment

- Exam without supervision by proctor
- Anti-impersonation by using face recognition
- Anticipation of changing devices during the exam
- Establishment of secure communication between server and client
- Audit

The research underlying this paper adhered to the SEMS [3] while addressing all challenges that already existed in e-exam, then expanded the attack analysis using the attack tree method.

Security analysis based on the attack tree has been widely discussed in various studies, such as in [7], [8], [9], [10], and [11]. In this paper, the attack tree method was applied to an e-exam system. The attack tree is a collection of all possible actions of an attacker to damage the system. The attack tree scheme can be defined by identifying the possible attack goals of the system first. For every attack goal, there is a separate tree with subtrees and nodes [12]. In this paper, the scheme of the attack tree on an e-exam system was based on SEMS Design [3] and NIST SP 800-30 Revision 1 Document about Conducting Risk Assessments [13]. The modeled attack tree was then verified as a practical penetration test on a demonstration server e-exam. Finally, this paper proposed a good security approach for each branch of the attack tree, as a corresponding defence tree.

The main contribution of this paper is useful as consideration for system managers to improve the security level of their e-exam systems.

2 Attack-Defence Tree Model

2.1 NIST SP 800-30 Risk Assessment

The risk assessment process consists of 9 steps, starting from System Characterization; Threat Identification; Vulnerability Identification; Control Analysis; Likelihood Determination; Impact Analysis; Risk Determination; Control Recommendations; and Results Documentation [13]. This paper presents the result of a risk assessment process in Table 1, which shows only medium and high risk.

Table 1. Medium and High Risk Event

No	Risk	Likelihood	Impact	Risk Level	Information
1	Server failure	1.0 (High)	100 (High)	100 (High)	The system/exam cannot run online/offline because all data is on the server.
2	There is no security on sensitive data	1.0 (High)	100 (High)	100 (High)	Data leakage and insecurity lead to system distrust and uselessness.
3	Poor supervision so cheating occurs	1.0 (High)	Medium= 50	50(Medium)	Cheating is a major risk when supervision/system does not work properly

2.2 Defining Attack-Defence Tree Model

The attack tree model on this paper focuses on several attack goals that are considered to be harmful to the e-exam system. There are 6 identified e-exam attacks from the results of the risk assessment which can be objects of the attack tree model, as follows:

- Server attack
- Cheating attack
- Software attack, it can be errors in the application
- Client device attack, it can be divided into two attack branches, namely network device attack, and client device attack
- Officer attack, it can happen to proctor so that another attack can be done
- Examinee attack

While creating an attack tree, the main goal to achieve is how to do countermeasure, which is called an attack-defence tree. In this paper, the attack tree and attack-defence tree were combined into one attack-defence tree diagram, see Fig. 1 (at the end of the paper). The more detailed description discusses one by one in the following subsections.

Server Attack-Defence Tree: This is related to server availability. Server attack can damage the server and cause sensitive data leakage. It can harm the e-exam assets because sensitive data are located on the server. If the server is not available, the e-exam cannot be performed. This condition is severe, so that the server attack becomes the main attack goal and is placed as a root node of the e-exam attack tree.

Further, the server attack root node can be divided into 4 branches that are very likely to be attacked, specifically:

1. Web application attacks, which are weaknesses or serious vulnerabilities that allow hackers to gain direct access to the database to obtain sensitive data. Elaborated further, these attacks consist of four types, namely:

   a) SQL Injection attack, which can be anticipated using SQL defined queries so that the database recognizes a valid SQL code. Moreover, the implementation of Web Application Firewall (WAF) can monitor the network traffics and block the possible attacks.
   b) Cross-Site Scripting (XSS) attack, which can be anticipated carefully when entering untrusted data.
   c) Denial of Services (DoS) attack, which can be anticipated using frequency hopping techniques to prevent the channel jamming attack. Furthermore, ingress filtering techniques can be implemented to prevent the smurfing attack. Likewise, the flooding attack can be anticipated by SYN cookies.
   d) Cross-site request forgery (CRSF) attack, which can be counter measured by a web application firewall.

2. Malware and spam attacks, which are malicious programs created by hackers with the aim of damaging computer system, stealing sensitive information, or accessing

computer confidential data. Malware and spam attacks can be anticipated by the anti-malware and anti-spam implementation.

3. Social engineering attacks. There are five major parts. These parts are as follows:

   a) Scareware, the most common example of a scareware technique is a pop-up that appears when using a web browser.
   b) The watering hole is an attack technique that injects malicious code into one or more public websites where one or all of the websites is a site that is often accessed by victims.
   c) Phishing, usually uses email, social media, short messages, and other communication intermediaries to cheat/manipulate victims to get important information.
   d) Pretexting, usually the attacker pretends to be someone else who is trusted by the victim. After being deceived, the attacker can lead the victim further so that the victim voluntarily provides important information.
   e) Baiting, by utilizing the curiosity that humans have, the attacker will install a 'trap' that is intentionally installed in a public place.

The social engineering attacks can be anticipated by measuring the policies and procedures; provide information security awareness training to staff; and prevention control and technical determination.

4. Infrastructure attacks. According to [14] infrastructure is the biggest target of attacks in the year 2018. These attacks can consist of:

   a) Physical attack, which can be anticipated by carrying out extra physical security and making backups
   b) Network failure, which can be anticipated by a good configuration system and arranging backups
   c) Natural disasters, which can be anticipated by back up and distant mirroring

Cheating Attack-Defence Tree: There are 7 types of e-exam cheating attacks [15], which are as follows:

a) Impersonation
b) Assistance/collaboration
c) Plagiarism
d) Using aids not allowed for the exam
e) Time violations
f) Lying to proctors
g) Smuggling out the exam questions after the exam

Countermeasures of the cheating attacks in e-exam can be performed with the following steps, as stated in [15] and [16]:

1. Mixed seating, especially in exam classes that are a combination of several classes
2. Nonuniform 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 number of questions between one student and another

3. Moving calculators and books into the exam system
4. Arrange strictly the question/answer sequence, make or display one question at a time, this reduces the chance of participants to remember or ask other participants;
5. Automated plagiarism checking by utilizing existing tools
6. Biometric authentication, using face, voice recognition or keystroke dynamics
7. Installing a firewall and anti-virus
8. Implementing security management (ISM)
9. Improving authentication, authorization, confidentiality, and accountability
10. Using digital rights management and cryptography
11. Security professional training, this is more to improve the professionalism of the officers (proctors)

Software Attack-Defence Tree: Software is one of the biggest causes of a system's failure. To prevent the software attack, secure coding and software security must be applied at all stages in every layer of implementation.

Network Device Attack-Defence Tree: The network device attack can occur if the installation of the devices is insecure or they do not meet network device configuration standards. To avoid this attack: adopt standardized devices, installation, and configuration; prepare failover scenarios.

Proctor Attack-Defence Tree: The human attack on the e-exam system can occur to the proctors. The attack is done to enable cheat during the exam. There are two types of attack: offline and online proctor attack. The offline proctor attack can paralyze the proctor physically, such as intimidation or murder. The professional security training and awards system [16] can anticipate this attack. Meanwhile, the online proctor attack attempts to interact with the proctor. Securing the proctor identity that can be used to protect against this attack.

Examinee Attack-Defence Tree: The examinee attack is executed as such so that the examinee is unable to take the exam at the specified time and venue. A straightforward solution is exam rescheduling.

3 Case Study

This research performed a case study to simulate the attack and defence tree scheme. The tool used was Acunetix [18]. It scanned the e-exam system vulnerabilities based on Acunetix Threat Level 2 profiles (medium).

The initial results (shown in Table 2) of the black-box penetration test were presented as a list of identified vulnerabilities of the e-exam system. Alerts generated by scanning for each classification follow the Common Vulnerability Scoring System (CVSS) [17].

Table 2. Alert types and their impacts on the server availability

No	Type of Alert	Availability Impact (CVSS2)	Availability Impact (CVSS3)
1	Apache server-info enabled	none	none
2	Apache server-status enabled	none	none
3	Application error message	none	none
4	HTML form without CSRF protection	none	none
5	Test CGI script leaking environment variables	n/a	n/a
6	User credentials are sent in clear text	none	none
7	Clickjacking: X-Frame-Options header missing	partial	n/a
8	Cookie(s) without HttpOnly flag set	none	n/a
9	Cookie(s) without Secure flag set	none	n/a
10	TRACE method is enabled	none	n/a
11	Content Security Policy (CSP) not implemented	none	n/a
12	Password type input with auto-complete enabled	none	none

Referring to Table 2, the e-exam prototype implementation is considered secure. Looking closely at the table on row number 7, "Clickjacking: X-Frame-Options header missing alert" has an availability impact on the server. According to [18], the clickjacking method is included in the XSS blind attack type. An attacker can insert a malicious website into the website that is accessed. The motivation of the attacker is to disrupt the e-exam system. In future work, a proper countermeasure for this risk should be implemented.

4 Conclusion

The proposed attack-defence tree can be regarded as a starting point towards building a more comprehensive attack-defence tree. As technology develops, the kinds of attacks and their countermeasures will continue to grow.

5 References

[1] M. Al-Fayoumi and S. J. Aboud, "An Efficient E-Exam Scheme," International Journal of Emerging Technologies in Learning (iJET), vol. 12, no. 4, pp. 153-162, 2017. https://doi.org/10.3991/ijet.v12i04.6719

[2] M. Yağci and M. Ünal, "Designing and Implementing an Adaptive Online Examination System," Procedia - Social and Behavioral Sciences, vol. 116, pp. 3079-3083, 21 February 2014. https://doi.org/10.1016/j.sbspro.2014.01.711

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

[4] Kryterion Global Testing Solutions, "Kryterion Global Testing Solutions," [Online]. Available: https://www.kryteriononline.com. [Accessed 2 April 2019].

[5] PSI Services LLC, "PSI Online One Stop Solution for Test Takers," [Online]. Available: https://home.psiexams.com/. [Accessed 2 April 2019].

[6] Splashgain Technology Solutions Pvt Ltd, "Online Examination System | Online Exam Software | Online Exam Free trial | AI Based Auto Remote Proctoring | Eklavvya," [Online]. Available: https://www.eklavvya.in/Default.aspx. [Accessed 15 March 2019].

[7] M. Houmer, M. L. Hasnaoui and A. Elfergougui, "Security Analysis of Vehicular Ad-hoc Networks based on Attack Tree," in 2018 International Conference on Selected Topics in Mobile and Wireless Networking (MoWNeT), Trainger, 2018. https://doi.org/10.1109/mownet.2018.8428905

[8] V. K. Saini and Q. Duan, "Attack Tree-Based Security Analysis for MyProxy Online Credential Repository," 15 September 2015. [Online]. Available: https://www.researchgate.net/publication/239796589_Attack_Tree-Based_Security_Analysis_for_MyProxy_Online_Credential_Repository. [Accessed 23 April 2019]. https://doi.org/10.1109/hpdc.2001.945181

[9] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System," in 2014 ACM SIGSAC Conference on Computer and Communications Security, Scottsdale, 2014. https://doi.org/10.1145/2660267.2660315

[10] M. Fraile, M. Ford, O. Gadyatskaya, R. Kumar, M. I. A. Stoelinga and R. Trujillo-Rasua, "Using attack-defence trees to analyze threats and countermeasures in an ATM: A case study," in 9th IFIP WG 8.1 Working Conference on The Practice of Enterprise Modeling (PoEM), Berlin, 2016. https://doi.org/10.1007/978-3-319-48393-1_24

[11] R. Kumar, Truth or dare: quantitative security risk analysis via attack trees, Enschede: University of Twente, 2018. https://doi.org/10.3990/1.9789036546256

[12] B. Schneier, "Modeling security threats," December 1999. [Online]. Available: https://www.schneier.com/academic/archives/1999/12/attack_trees.html. [Accessed January 2019].

[13] Computer Security Division of National Institute of Standards and Technology, "Guide for Conducting Risk Assessments," Gaithersburg, 2012.

[14] Positive Technologies, "Cybersecurity threatscape 2018: trends and forecasts," 18 March 2019. [Online]. Available: https://www.ptsecurity.com/ww-en/analytics/cybersecurity-threatscape-2018/. [Accessed 7 May 2019].

[15] G. Sindre and A. Vegendla, "E-exams versus paper exams: A comparative analysis of cheating-related security threats and countermeasures," in Conference: Norsk Informasjonssikkerhetskonferanse (NISK), Finse, 2015.

[16] Y. Chen and W. He, "Security Risks and Protection in Online Learning: A Survey," The International Review of Research in Open and Distributed Learning, vol. 14, no. 5, pp. 1-9, 2013.

[17] FIRST.org, Inc., "Common Vulnerability Scoring System SIG," FIRST.org, Inc., [Online]. Available: https://www.first.org/cvss/. [Accessed 16 April 2019].

[18] Acunetix, "ClickJacking and Blind XSS," Acunetix, 24 March 2014. [Online]. Available: https://www.acunetix.com/blog/articles/clickjacking-blind-xss/. [Accessed 16 April 2019].

6 Authors

Yusep Rosmansyah received a B.S. degree from Bandung Institute of Technology, Indonesia, and both the M.S. and Ph.D. degrees from the University of Surrey, U.K. He has been a researcher and faculty member at the School of Electrical Engi-

neering and Informatics, Bandung Institute of Technology, Indonesia. His current research interest includes mobile learning technologies and cybersecurity.

Mora Hertanto Ritonga is a master’s student at the School of Electrical Engineering and Informatics, Bandung Institute of Technology. He received a scholarship from the National Cyber and Crypto Agency. His research interest includes cybersecurity and e-learning (mora.hertanto@bssn.go.id).

Ariq Bani Hardi is a master’s student at the School of Electrical Engineering and Informatics, Bandung Institute of Technology, Indonesia. He received a scholarship from the National Cyber and Crypto Agency. His main research interests are related to the design and development of security of the mobile application, cybersecurity, and applied cryptography (ariq.bani@bssn.go.id).

Article submitted 2019-06-21. Resubmitted 2019-08-19. Final acceptance 2019-09-08. Final version published as submitted by the authors.

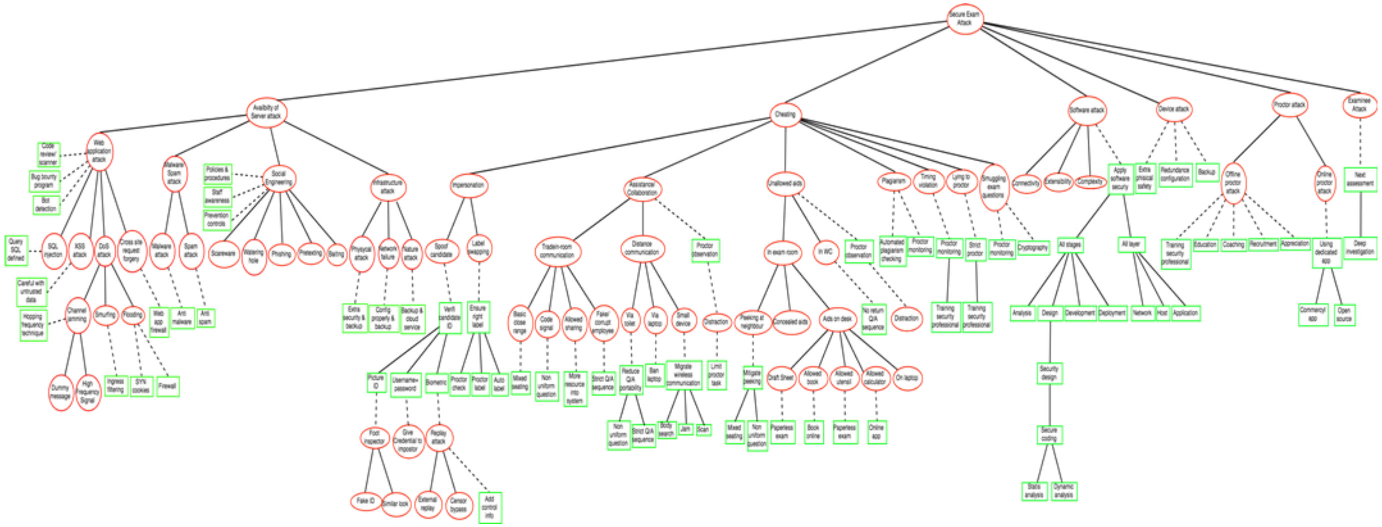

Fig. 1. Attack-defence tree on e-exam system