Multi-Learning Techniques for Enhancing Student Engagement in Cybersecurity Education

Dr. Te-Shun Chou, East Carolina University

Dr. Te-Shun Chou is an Associate Professor in the Department of Technology Systems at ECU. He received his Bachelor degree in Electronics Engineering at Feng Chia University and both Master's degree and Doctoral degree in Electrical Engineering at Florida International University. He serves as the program coordinator of the Master program in Network Technology for the Department of Technology Systems and the lead faculty of Digital Communication Systems concentration for the Consortium Universities of the Ph.D. in Technology Management. He is also the point of contact of ECU National Centers of Academic Excellence in Cyber Defense Education (CAE-CDE). Dr. Chou teaches IT related courses, which include network security, network intrusion detection and prevention, wireless communications, and network management. His research interests include machine learning, wireless communications, technology education, and information security, especially in the field of intrusion detection and incident response.

Multi-Learning Techniques for Enhancing Student Engagement in Cyber Security Education

Abstract

Cybercrime is the utmost risk to every company in the world, causing un-estimated damage against companies. Hence, the mission of preparing students with sufficient knowledge and skills of cyber security has become extremely important and urgent. In this paper, we presented a cybersecurity learning system that provided a comprehensive training program to educate students in the field of cyber-attack and prevention. The system incorporated various learning techniques to not only deliver the contents clearly but also make the learning of cybersecurity interesting. The learning techniques included integrated learning, student-centric learning, problem-based learning, self-paced learning, and game-based learning. We expected the system to attract youngsters and prepare them to become the next generation of cyber security professionals.

Keywords: Cyber security, integrated learning, student-centric learning, problem-based learning, self-paced learning, game-based learning

1. Introduction

In the past, cyber-attacks on individuals, businesses, government agencies increased with incredible speed. According to a study from SecurityIntellgence, the global average cost of a data breach per compromised record was $148. In 2018, the average total cost of a breach ranged from $2.2 million (incidents with fewer than 10,000 compromised records) to $6.9 million (incidents with more than 50,000 compromised records). Overall, the total cost, per-capita cost and average size of a data breach (by number of records lost or stolen), have all increased year over year [1]. In order to protect infrastructures from cyber threats, cybersecurity education has become critically important to foster capable professionals.

Thus, we designed a comprehensive cyber security awareness system to educate students of cyber security knowledge and provide a platform for practicing hands-on activities. The learning system incorporated various learning techniques to assist students in understanding cyber security concepts and skills. The learning techniques were game-based learning, student-centric learning, integrated learning, self-pace learning, and problem-based learning.

An infrastructure was designed by using virtualization technology to emulate a realistic physical network. The infrastructure included multiple learning environments that were able to communicate with each other, which allowed students to conduct the cyber security activities simultaneously.

Nine CyberSec labs were included to introduce students the most important and current cybersecurity issues. Each lab included a pair of cyber-attack and defense sub-labs. The cyber-attack sub-labs demonstrated vulnerabilities exploitation and the methods to launch attacks against other students' virtual machines (VMs). The defense sub-labs showed students the implementations of the protection and prevention mechanisms against cyber-attacks on their VMs. For each attack/defense sub-lab, a three-stage process (learning, assessment, and engagement) was employed. This process not only delivered the principles and theory of cyber

security, but also equipped students with practical hands-on skills. This approach helped students turn abstract concepts into actual skills to solve real-world problems and challenges.

This paper is organized as follows: Section 2 illustrates conceptual framework. Section 3 describes game-based learning. Section 4 discusses problem-based learning. Section 5 deliberates integrated learning. Section 6 demonstrates student-centric learning. We then describe self-paced learning in Section 7 and evaluation plan in Section 8. Finally, we conclude our work in the last section.

2. Conceptual Framework

In this project, we built a learning system for cyber security education. It employed a variety of educational methods in order to make the learning of cyber security interesting and efficient. Figure 1 shows the conceptual framework.

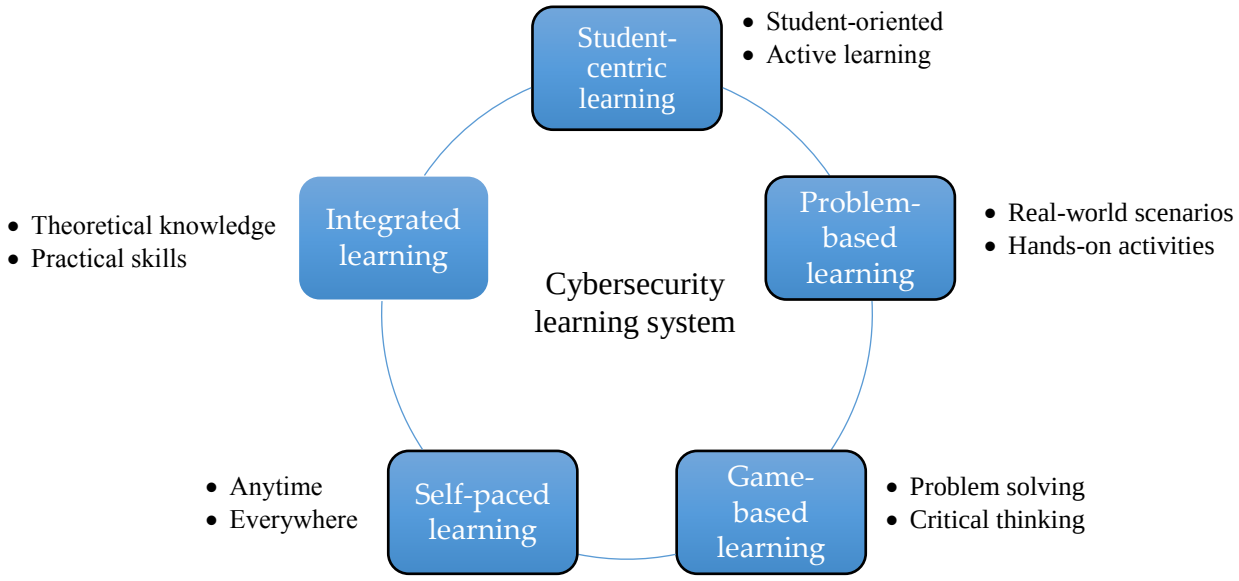

Figure 1. Conceptual Framework

3. Game-Based Learning

The major goal of this project was to design a system that can be used to train future cyber security professionals. To achieve this goal, a common approach was to prepare a game-based learning environment to educate learners [2], with gamification always facilitated through a competition model [3]. Typically, the competitions were clustered into four categories; they were network defense [4, 5], computer forensics [6, 7], penetration testing [8, 9], and capture the flag [10, 11]. At the competition, students were grouped into teams and each team was given an identical network. During the completion, students applied their knowledge and skills to solve real-world cyber security problems.

Most of the competitions only allowed teams to conduct activities in their own environments, which lacked interaction with each other. Also, the activities in the competitions were limited to on either attack or defense. Yet, we believed that cyber security learning should include both activities of offense and defense because they are equally important. With developed understanding of attackers' behavior, a good defense strategy can therefore be deployed. Therefore, in this project we built a game-based, multiplayer, and peer-to-peer cyber security infrastructure. Figure 2 shows the network infrastructure. It included a set of identical students' learning environments with each student having access to his/her own environment to conduct cyber security lab exercises. Since the environment was isolated, no sensitive information can be released outside of it.

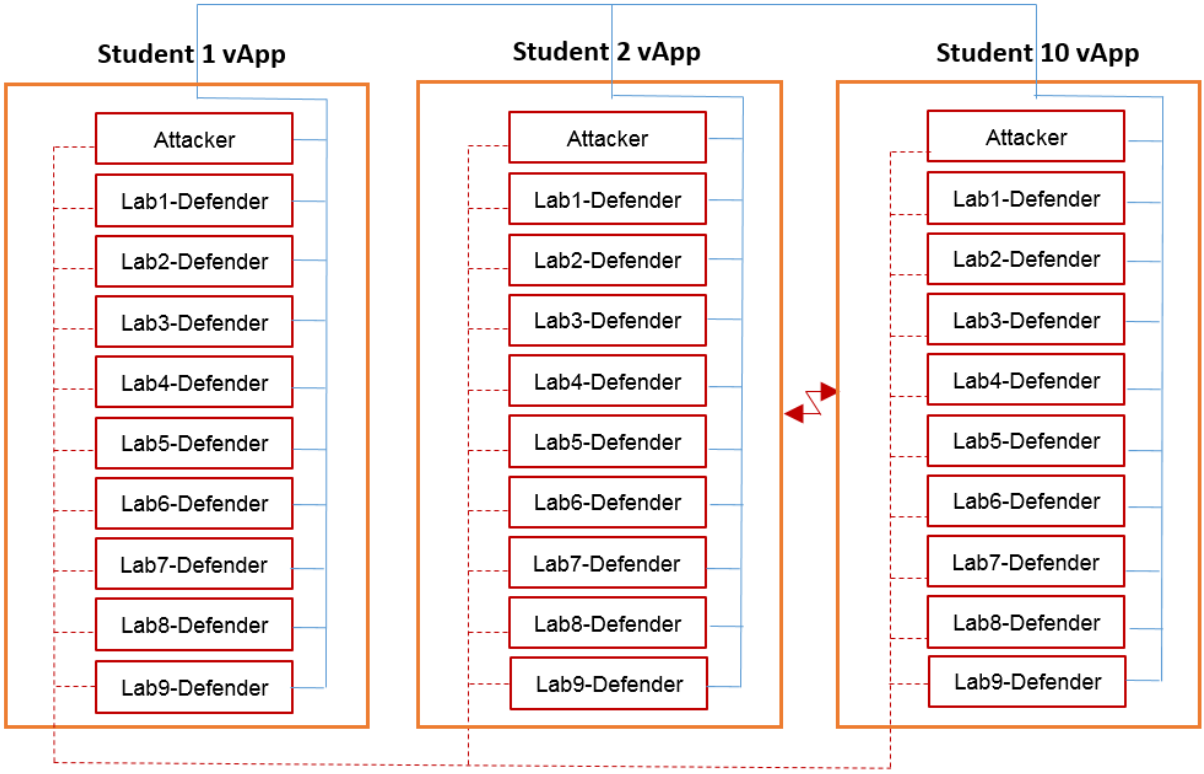

Figure 2. System Infrastructure

Virtualization technology was used to host multiple VMs in each learning environment. Each virtual application (vApp) was running VirtualBox hypervisor that contained a single Attack VM and Multiple Defense VMs (Defenders 1-9). The Attack VM was the Kali Linux that prepared students with a variety of penetration testing tools to initiate attacks and exploit system vulnerabilities on other students' defense VMs. Each defender was either a Windows Server or Linux machine that was configured specifically for its corresponding attack or defense sub-lab.

A Score and Message Board was designed to display the points students achieved. The student gained positive points when s/he successfully attacked someone's VM or configured his/her own defense VM; on the contrary, the student got negative points when s/he did not prevent an attack from others or failed to configure his/her own defense VM. During the competition, instant messages showing the real-time statuses of the attack/defense were displayed on the Board.

4. Problem-Based Learning

Problem-based learning is a student-centered pedagogy to help students learn a subject by engaging in complex and challenged real-world problems. The incentive to solve the problems directly drives students' motivation to learn and indirectly promotes the development of flexible knowledge, effective problem-solving skills, self-directed learning skills, effective collaboration skills, intrinsic motivation, and lifelong learning skills [12, 13].

In this project, real-world problems of cyber security were included in nine CyberSec labs. The labs provided students' with an opportunity to promote their critical thinking skills and problem-solving abilities. Table 1 shows the CyberSec labs.

Table 1. CyberSec Labs

Lab	Attacker's Goal	Defender's Goal
Remote Secure Login	Perform brute force attack and log in to change the password	Secure the host and the OpenSSH service
SQL Injection (SQLI)	Modify and delete the existing information throughout the website	Implement protection mechanisms on the MariaDB Server
Web Defacement	Use cross site scripting attack to inject malicious codes into the comment box to deface the webpage	Set up appropriate defense mechanisms on the Linux MariaDB Server
Patch Management	Scan the host to find vulnerable services	Patch outdated and vulnerable services
Honeypot	Change the honeypot architecture information	Configure the honeypot and install packages needed for the honeypot
FTP Server DoS Attack	Flood the FTP Server and prevent legitimate users from gaining access to it	Configure firewall and other parameters to protect against the attack
DHCP Starvation	Send Neighbor Solicitation packets to starve the address pool of the DHCP Server	Use the Server Manager tool to analyze the CPU usage and write rules to prohibit illegitimate incoming traffic
Backdoor	Install a persistent backdoor and retrieve files from the victim	Ensure protection of Server Message Block (SMB) file-sharing
Secure Plain Text Traffic	Sniff network packets and access FTP server with discovered credentials	Secure FTP access and transmission

In order to help students get familiar with different operating systems (OSs), three labs (DHCP Starvation, Backdoor, and FTP Server DoS) used Windows OS and six labs (Remote Secure Login, SQLI, Patch Management, Honeypot, Web Defacement, and Secure Plain Text Traffic) used Linux OS as defense hosts. Also, both IPv4 and IPv6 address families were included, which

DHCP Starvation and Backdoor labs used IPv6 address schemes and the rest of labs used IPv4 address.

5. Integrated Learning

In the system, challenges in cyber security education that should be addressed were identified. The system introduced different types of cyber threats and their corresponding prevention and countermeasure techniques. It helped students understand the fundamental concepts of cyber-attack techniques and defense mechanisms. However, theory alone was not sufficient to prepare students to detect and respond to live cyber intimidations in the real-world scenarios. Therefore, integrated learning was incorporated with hopes of connecting theory and practice so that the knowledge and skills learned in the class room can be applied to solve real-world issues. The system required students to immerse themselves in the cyber security discipline by conducting multiple, hands-on experiments. Students were required to take a series of necessary actions to attack network systems as well as protect the network from attacks. A three-stage, logical, step-by-step, process was designed to help students master both theoretical knowledge and practical skills of the CyberSec labs. The three-stage learning process is depicted in Figure 3. It outlines the logical links among three major stages when conducting a lab activity.

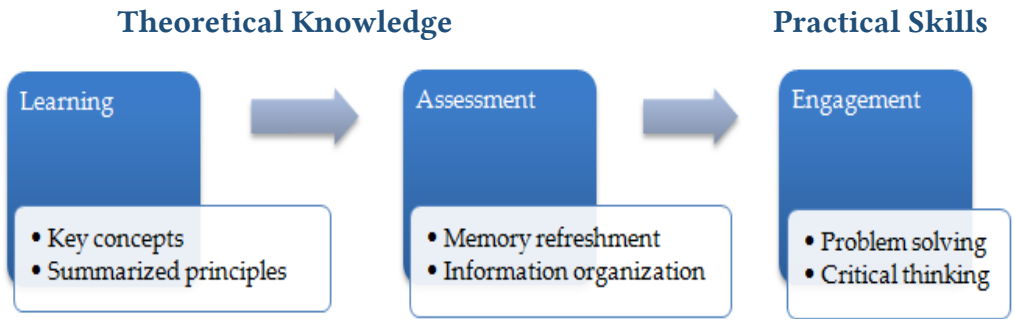

Figure 3. Three-Stage Learning Process

For a cyber-attack sub-lab, students learned about the attack technique by studying the provided reference materials. The relevant learning resources of a cyber threat were identified and described in detail in the first stage. This stage involved introducing students to the fundamental concepts, theories, and skills regarding a specific type of cyber-attack and system vulnerability. Examples were presented to help students quickly acquire subject knowledge. For example, the introduction of DoS attacks included the following questions with corresponding answers: What are DoS attacks? Is there a three-way handshake that establishes a connection between the attack host and target machine's destination port in the beginning of the attack? What are the attack techniques to launch DoS attacks and any countermeasures to the attacks?

After reading the introduction, students moved to the second stage where they must successfully pass a multi-question quiz in order to move on to next stage. The quiz was used to assess student learning with questions that were designed to reinforce important topics. The quiz compelled students to refresh their memory and organize information that they have learned 1414].

Students were required to successfully pass the quiz with 80% or higher before proceeding to the exercise of launching the cyber-attack in the third stage. Detailed guidance in attacking was provided in this stage. Instructions were illustrated to show how to carry out the attack activities in a logical, step-by-step fashion. This practice enabled a deeper understanding of the subject and helped students to develop broader experimental and problem-solving skills 1515].

Each cyber-defense sub-lab had a similar introduction and quiz components before starting the defense actions. Students were also required to successfully pass the quiz before proceeding to the walkthrough of mitigating the corresponding attack in the third stage. In this stage, students were required to implement proper cyber security mechanism to protect their hosts.

6. Student-Centric Learning

The traditional learning model was course- and teacher-focused [16]. In the model, teachers are in the principal role of helping students learn knowledge by giving out lectures, assigning homeworks, and creating exams to test students' comprehension of materials within a time-frame. This approach does not take into consideration the reality that students require different amounts of time to digest materials and grasp the key concepts and principles.

The student-centric approach places the student in the center of the learning process and provides students with opportunities to learn independently [17]. It allows the student to learn materials at his/her own pace and requires them to follow a competency method that s/he only moves ahead after demonstrating mastery of the content [16]. Studies have shown that student-centered learning approaches have demonstrated measurable improvements on academic performance, attitudes toward learning, and persistence in programs [18, 19].

In this project, the student completed the CyberSec labs anytime and from anywhere. Students may access the learning environment multiple times and complete the required lab tasks at his or her own pace. This personalized learning experience was a student-centric approach which allowed the student to be an active participant in the learning process instead of passively absorbing information from lectures. This self-guided approach made learning enjoyable and was effective in improving student learning and understanding [4, 5].

7. Self-Paced Learning

With self-paced learning, students proceed from one topic to the next at their own discretion. This type of student-centered learning approach allows students to learn at their own pace and choose their own learning sequence based upon mastery of the instructional materials. Studies have shown that this approach will enhance the performance of student learning, with benefits including no time pressure, effectively improves memory performance, suitable for different learning styles, no need for a schedule to absorb information, and efficiently meet learning objectives [20, 21]. Self-paced learning has become increasingly popular as the education world shifts from the classroom to the internet. [22]

In our project, the system was accessible through a secure Internet connection. Therefore, time and location were no longer accessibility issues to the system. This approach gave students time

to absorb the theoretical knowledge and practice CyberSec lab exercises at their own pace, anytime, from anywhere. This was a self-paced learning approach, in which students decide their own learning path on when to study and how long to study. The self-regulated learning method effectively improved students learning efforts and achievement in education [23].

8. Evaluation Plan

The lab walkthroughs of nine-pairs of attack/defense labs and the GUI have been developed. We are now focusing on the development of the Score and Message Board and anticipate the entire system will be completed by the end of the spring semester 2019. Once the design of the system is finished, we will ask the members of the Information and Computer Technology (ICT) program Advisory Board to review the system. Through their feedback, we will then revise the system to improve its overall quality.

In addition, a workshop will be held in the summer of 2019. Twenty community college instructors will be invited to use the learning environment and take a survey. The effectiveness and appropriateness of the project will be evaluated to determine whether or not the project goals and objectives have been met. In the future, the learning environment will be continuously used and assessed by students in classes.

9. Conclusions

In this project, we implemented a unique learning system to promote cyber security awareness training. Virtualization technology was used to create and scale the learning system. The system treated each student environment as a network in the real-world so the individual network was capable of interacting with other peers' networks.

Five different learning techniques were incorporated in the system: integrated learning, student-centric learning, problem-based learning, self-paced learning, and game-based learning. The integrated learning was a combination of both cyber security theory and hands-on practice. The game-based learning made learning interesting by assigning winning or losing points to students. Real-world cyber security issues were discussed in nine CyberSec labs. Students were allowed to complete the lab activities at their own pace, anytime, and from anywhere. Each activity acted as a learning development for students to raise a level of knowledge to a certain cyber-attack and defense. With successful completion of all the labs, students advanced their skills and understanding in the field of cyber security.

Acknowledgements

This research is based upon work supported by the Secure &Trustworthy Cyberspace (SaTC) Program of the National Science Foundation under Grant Number 1723650. The authors are grateful to the support of Department of Technology Systems in the College of Engineering and Technology at East Carolina University.

References

1. L. Ponemon, L, "Calculating the Cost of a Data Breach in 2018, the Age of AI and the IoT," 2018. Retrieved from https://securityintelligence.com/ponemon-cost-of-a-data-breach-2018/
2. A. Nagarajan, J. M. Allbeck, A. Sood, and T. L. Janssen, "Exploring game design for cybersecurity training," *2012 IEEE International Conference on Technology in Automation, Control, and Intelligent Systems (CYBER)*, pp. 256–262, Bangkok, Thailand, May 2012.
3. K. Boopathi, S. Sreejith, and A. Bithin, "Learning Cyber Security Through Gamification," *Indian Journal of Science and Technology*, vol. 8, no. 7, pp. 642–649, 2015.
4. National Collegiate Cyber Defense Competition. Retrieved from https://www.nationalccdc.org/
5. AFA CyberPatriot. Retrieved from https://www.uscyberpatriot.org/
6. Digital Forensics & Incident Response Challenge. Retrieved from https://digital-forensics.sans.org/community/challenges
7. RED. Retrieved from https://csaw.engineering.nyu.edu/RED
8. Collegiate Penetration Testing Competition. Retrieved from https://nationalcptc.org/
9. Global CyberLympics Security Competition. Retrieved from https://www.cyberlympics.org/
10. DEF CON CTF Qualifier. Retrieved from https://ctftime.org/ctf/1
11. DEF CON CTF. Retrieved from https://ctftime.org/ctf/2/
12. B. J. Duch, S. E. Groh, and D. E. Allen, *The power of problem-based learning*, Sterling, VA: Stylus, 2001.
13. C. E. Hmelo-Silver, "Problem-based learning: What and how do students learn?," *Educational psychology review*, vol. 16, no. 3, pp. 235-266, 2004.
14. B. J. Tewksbury and R. H. Macdonald," Assessing Student Learning," Course Design Tutorial. Retrieved from http://serc.carleton.edu/NAGTWorkshops/coursedesign/tutorial/assessment.html
15. E. F. Redish, *Teaching Physics with the Physics Suite*, John Wiley & Sons, Inc., 2003.
16. D. Schaffhauser, "New Report Offers Tech Blueprint for Student-Centric Learning," 2016. Retrieved from https://thejournal.com/articles/2016/05/05/new-report-offers-tech-blueprint-for-student-centric-learning.aspx
17. J. Froyd and N. Simpson, "Student-centered learning addressing faculty questions about student centered learning," *Course, Curriculum, Labor, and Improvement Conference*, Washington DC, August 2008.
18. J. Handelsman, D. Ebert-May, R. Beichner, P. Bruns, A. Chang, R. DeHaan, and et al. "Scientific teaching," *Science*, vol. 304, no. 5670, pp. 521–522, 2004.
19. S. F. H. S. Zain, F. E. M. Rasidi, and I. I. Z. Abidin, "Student-centred learning in mathematics-constructivism in the classroom," *Journal of International Education Research*, vol. 8, no. 4, pp. 319-328, 2012.
20. "Self-paced Learning meaning," LMS Knowledge Center. Retrieved from https://www.easy-lms.com/knowledge-center/lms-knowledge-center/self-paced-learning-definition/item10384
21. J. Patterson, "5 Reasons Why Self-Paced Training Is Highly Effective," KnowledgeWave, 2012. Retrieved from https://www.knowledgewave.com/blog/self-paced-training
22. W. Dick, and L. Carey, *The Systematic Design of Instruction*, Allyn & Bacon; 6 Edition, 2004.
23. J. Dunlosky and K. W. Thiede, "What makes people study more? An evaluation of factors that affect people's self-paced study and yield "labor-and-gain" effects," *Acta Psychologica*, pp. 37–56, 1998.