Journal of Information Systems Education

Volume 34
Issue 4
Fall 2023

Teaching Tip
What You Need to Know about Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges

J.B. (Joo Baek) Kim, Chen Zhong, and Hong Liu

Recommended Citation: Kim, J. B., Zhong, C., & Liu, H. (2023). Teaching Tip: What You Need to Know about Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges. *Journal of Information Systems Education*, 34(4), 387-405.

Article Link: https://jise.org/Volume34/n4/JISE2023v34n4pp387-405.html

Received: July 22, 2022
First Decision Made: September 10, 2022
Accepted: December 30, 2022
Published: December 15, 2023

ISSN: 2574-3872 (Online) 1055-3096 (Print)

Teaching Tip
What You Need to Know about Gamification Process of Cybersecurity Hands-on Lab Exercises: Lessons and Challenges

J.B. (Joo Baek) Kim
Chen Zhong
John H. Sykes College of Business
University of Tampa
Tampa, FL 33606, USA
jkim@ut.edu, czhong@ut.edu

Hong Liu
School of Sciences
Indiana University Kokomo
Kokomo, IN 46902, USA
hlius@iu.edu

ABSTRACT

Cybersecurity education is becoming increasingly important in modern society, and hands-on practice is an essential element. Although instructors provide hands-on labs in their cybersecurity courses, traditional lab exercises often fail to effectively motivate students. Hence, many instructors desire to incorporate gamification in hands-on training to engage and motivate cybersecurity students, especially beginner learners. Given the dearth of guiding examples, this paper aims to describe the holistic process of converting traditional cybersecurity hands-on lab exercises to gamified lab exercises in an undergraduate network security course. We find that the gamified cybersecurity lab promotes students' engagement, learning experience, and learning outcomes. The results show the positive acceptance of gamification by students as well as instructors. While gamification has been used in competitions and training, the success in the classroom and students' desire for more gamification show that further investment in gamification will be more important in the classroom. We expect this paper to help instructors who are interested in gamification 1) convert traditional lab exercises to gamified labs; 2) estimate the extra workload and potential benefits; and 3) plan resources for implementation. This process is applicable to any cybersecurity courses with hands-on assignments.

Keywords: Cybersecurity, Gamification, Game-based learning, Teaching tip

1. INTRODUCTION

Over recent decades, with the rapid development and popularization of information technology, cybersecurity has become a part of people's lives. Cybersecurity skills are considered essential across every industry and organization (IBM, 2021). It is thus important to engage college students and improve their cybersecurity knowledge (Qusa & Tarazi, 2021). However, for various reasons, many cybersecurity course instructors find it difficult to engage students and achieve desired learning outcomes. Previous studies have found that traditional training methods such as lab work, are limited in engaging and motivating cybersecurity students (Schreuders & Butterfield, 2016).

Gamification is a new technique that can be effective in education and business training. As defined by Deterding et al. (2011, p. 10), gamification is "the use of game design elements in non-game contexts." Because younger generations are familiar with games and seek fun when learning and working, gamification is a suitable method to teach them various skills. Gamification is already being used widely in various education and business training contexts to take advantage of its engagement and motivational capabilities (Faria, 1998; Faria & Wellington, 2004). Many cybersecurity competitions and camps also employ gamification to draw participants' interest. Although designing gamified cybersecurity lab exercises can help gain more attention from students and enhance their motivation in the learning process (Demmese et al., 2020), instructors in higher education may hesitate to implement gamification in their classes because of two major concerns: (1) the difficulty of predicting and managing the extra work that is needed to create and implement gamified course activities; and (2) the uncertainty of the benefits in return for the cost.

Several previous studies have reported the effectiveness of gamified cybersecurity training methods (Adams & Makramalla, 2015; Demmese et al., 2020; Karagiannis & Magkos, 2021; Ros et al., 2020; Wolfenden, 2019), but their scopes and approaches were limited and their outcomes mixed. Most of the past literature on gamification in cybersecurity education focused on cybersecurity competitions, such as Capture-The-Flag (CTF), which is more effective in providing students with the opportunity to apply cybersecurity skills already developed from lectures or exercise labs (Demmese et al., 2020). However, there is a lack of attention to the cybersecurity skill development process through gamification, which consequently causes a lack of affordable existing gaming platforms for cybersecurity labs. Given that little previous work demonstrates a holistic process of building gamified cybersecurity lab exercises in a college course, it is necessary to provide instructors with a guide for gamifying labs based on existing teaching materials.

To address the problem, we describe the workflow that includes general tasks of converting a traditional cybersecurity lab session into a gamified lab exercise. The workflow has been tested in an undergraduate cybersecurity course in the College of Business at a mid-sized university in the United States. To provide useful information to guide instructors who are considering implementing gamified labs, we summarize the lessons and challenges from the study in this paper. The paper makes two main contributions to the field: (1) the proposed workflow can be used by instructors to estimate and manage the extra workloads in implementing gamified labs; and (2) the lessons and challenges summarized from our study can be used as a resource guide.

The rest of the paper is organized as follows. Section 2 reviews previous literature and theories related to gamification in cybersecurity. Section 3 describes the existing course and lab exercises. Section 4 presents the overall process of converting the existing lab exercises into gamified lab exercises. Section 5 then reports students' feedback on and learning outcomes from engaging in the gamified lab exercises. We discuss in Section 6 the findings and takeaways from our experience of gamifying cybersecurity lab exercises and make suggestions for integrating gamification into future cybersecurity courses. Finally, Section 7 summarizes the paper and draws conclusions.

2. RELATED WORK

Incorporating games in non-entertaining contexts has recently been gaining attention in higher education and business training. Especially as younger, tech-savvy generations familiar with digital games undertake higher education, gamification will become an increasingly important educational tool (Donovan & Lead, 2012). In this regard, gamification is considered effective because of various elements, including situated cognition, assimilation/accommodation, and engagement. Situated cognition refers to the capability of games to provide a meaningful and relevant context, which allows learners to understand the subject matter more effectively and in a more convenient manner (Van Eck, 2006). According to Piaget's (1952) theory of cognitive development, an individual's intelligence matures through the continuous cycle of assimilation and accommodation, which gamified learning tools help learners experience. Games are also considered effective in engaging and motivating learners (Garris et al., 2002; Lepper & Malone, 1987; Malone, 1981; Parker & Lepper, 1992; Rieber, 1996).

Cybersecurity is gaining much attention from researchers and practitioners as a domain for applying gamification to enhance the effectiveness and efficiency of educating students and training workforces (Wolfenden, 2019). Karagiannis and Magkos (2021) investigated the values of digital game-based learning in cybersecurity education and found it was accepted by students as a sufficient learning method. Adams and Makramalla (2015) identified various gamification training solutions in the cybersecurity discipline from several different perspectives, namely, awareness, defensive strategy, offensive strategy, and attacker centricity. Coenraad et al. (2020) found that, as of Fall 2018, there were 181 cybersecurity games available in the market; they provided a comprehensive overview of these games categorized by their attributes, such as platform, developer, playtime, audience, visual realism, camera view, anthropomorphism, a game story, game actions, and presentation of cybersecurity content. Capture-The-Flag (CTF) is one of the popular gamified methods identified as effective in teaching cybersecurity skills in various studies (Demmese et al., 2020). Beuran et al. (2016) suggested a framework that incorporates the skill, environment, and cost aspects required for cybersecurity training activities and matches them with appropriate types of cybersecurity training methodologies.

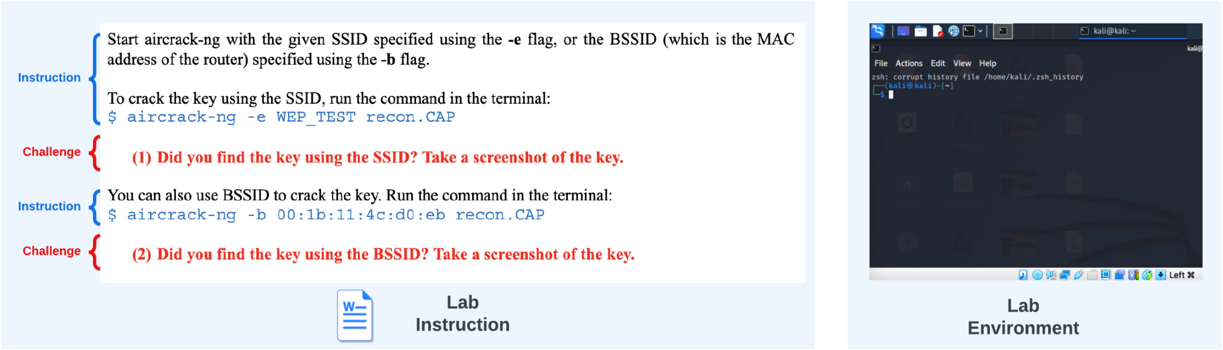
Tioh et al. (2019) identified the advantages of gamified learning compared to traditional hands-on training. They concluded that game-based learning accounts for many advantages, including cost-effectiveness, low risk, standardized assessments, high engagement, individually tailored pace, and immediate feedback, whereas traditional training and hands-on training only partially provide these advantages.

In the cybersecurity education/training domain, there have been several studies on using game-based learning methods in teaching cybersecurity skills and principles. Omar et al. (2021) identified several types of game-based learning methods, including mobile-based gaming applications, puzzle games, web-based games, mini-games, and narrative gameplay. These game-based learning methods cover various topics in cybersecurity, including spam, malware, cyber-attacks, scams, password cracking, identity theft, phishing, brute-force attacks, and SQL injection; they also target various audiences, including children aged 9-12 years old and high school, university, and graduate students.

3. STUDY BACKGROUND AND MOTIVATION

3.1 Target Subjects

The course we sought to improve through gamification is an undergraduate course of the cybersecurity major in a nationally ranked college of business at a mid-sized university in the southeastern United States. The course name is Network Security, and its topics include cryptography, firewall, intrusion detection, wireless systems, remote connectivity, and common attack types. The prerequisites of this course include an introductory network course and an information security basics course. The students enrolled in this course are typically junior and senior undergraduates with a cybersecurity major.



Start aircrack-ng with the given SSID specified using the **-e** flag, or the BSSID (which is the MAC address of the router) specified using the **-b** flag.

To crack the key using the SSID, run the command in the terminal:

```
$ aircrack-ng -e WEP_TEST recon.CAP
```

(1) Did you find the key using the SSID? Take a screenshot of the key.

You can also use BSSID to crack the key. Run the command in the terminal:

```
$ aircrack-ng -b 00:1b:11:4c:d0:eb recon.CAP
```

(2) Did you find the key using the BSSID? Take a screenshot of the key.

```
zsh: corrupt history file /home/kali/.zsh_history
┌──(kali㉿kali)-[~]
└─$ 
```

Figure 1. Example of the Non-Gamified Lab Instruction and Lab Environment

3.2 The Original (Non-Gamified) Lab Exercises

The original design of the course emphasizes reinforcing concepts with hands-on lab-based exercises. One lab exercise may contain multiple tasks, and each task consists of a set of instructions and challenges. In our study, the original lab instructions were provided in Word documents that guided students through the challenges. Students were asked to follow the instructions and complete the tasks in a virtual machine environment and report results in an answer sheet. Figure 1 shows a short extract of these instructions in the original lab, illustrating what students were asked to report.

The lab we used for gamification is a wireless security lab that contains four tasks. Table 1 describes the tasks and their learning objectives. The first three tasks have different learning objectives: Task 1 emphasizes understanding wireless network security protocols; Task 2 asks students to configure a wireless network based on their understanding gained in Task 1; and Task 3 helps students understand Media Access Control (MAC) addresses. Task 4 is similar to Task 1 and aims to assess whether students can apply what they have learned to a new problem. Instructions in the original lab were developed to guide students to complete the tasks and report the outcome (Figure 1).

3.3 Motivation of Gamifying Lab Exercises

The original cybersecurity lab exercises have some problems. First, some students lack self-motivation to address complex problems when not provided with detailed instructions; conversely, students given detailed instructions cannot always connect the lab exercises to learning objectives because critical thinking and reflection are lacking. Second, students may work on lab exercises at different speeds, making it hard for instructors to maintain all students' attention when addressing a problem or reviewing an exercise. The challenge here is how to engage students when they prefer to complete exercises at their own pace.

4. THE APPROACH TO GAMIFYING A CYBERSECURITY LAB

Given that little previous work provides a holistic process for building gamified cybersecurity lab exercises in a college course, it is necessary to provide instructors with a guide for gamifying labs based on the existing teaching materials. Therefore, we integrate the major game elements in the existing cybersecurity labs and lay out the process of gamification as a workflow.

	Challenges in Task	Learning Objectives
Task 1*	• Analyze captured network packets using Wireshark • Find the network ID, BSS ID, whether WEP is used • Use aircrack-ng to crack the network key	• Explain the stage of reconnaissance • Practice using Wireshark for packet analysis • Explain why WEP is not secure • Employ tool to crack WEP network
Task 2	• Configure wireless setting • Configure wireless security setting	• Apply good practice in wireless network configuration • Compare wireless security protocols
Task 3	• Find MAC address of a given device • Track geolocation using the records of a connected wireless network	• Explain why MAC address is the physical address of a device
Task 4	• Analyze network packet capture • Identify the security protocol of the network • Use aircrack-ng to crack the password	• Same as Task 1

*Task 1 is adapted from the Secknitkit project (Security Knitting Kit, www.secknitkit.org; https://www.nsf.gov/awardsearch/showAward?AWD_ID=1140864).

Table 1. Task Description and Learning Objectives of the Wireless Security Lab

4.1 Game Elements

Several previous works have identified various elements required for designing effective gamification (Adams &

Makramalla, 2015; Kapp, 2012), including game mechanics, player control, problem-solving, and story. Zichermann and Cunningham (2011) also suggested game design elements, including point systems, levels, badges or trophies, leaderboards, challenges and quests, onboarding, and engagement loops. The major game elements used in the lab include game storytelling, game rewards, a leaderboard, and badges. The rationales for including these elements are as follows:

- *Game storytelling*: The learning objectives of each task can be written in the form of a mission description for the game scenario. We believe storytelling helps students understand the learning objectives.
- *Game rewards*: Reward points are offered for solving a challenge successfully so that students are motivated to continue playing the game, especially when solving a challenge requires effort.
- *Leaderboard*: Because students play our game individually, the leaderboard allows them to compare their performance against that of their peers.
- *Badges*: Badges are provided when students perform well on a task. Earning a badge indicates that a student achieved the task's learning objectives. Students should be motivated to collect badges as demonstrations of the knowledge and skills they have developed.

4.2 Gamification Workflow

For gamifying the aforementioned wireless security lab, the workflow of gamification is described in Figure 2, showing four major stages. Stage 1 allows an instructor to review the existing order of tasks (described in Section 3.2) and reorder them if necessary. If an instructor wants to include storytelling, story scenarios can be described according to the task order in this stage. Stage 2 mainly focuses on developing the game rules. The lab contents are added to the gamified lab in Stage 3 with the implementation of the contents and game elements. The final gamified lab is reviewed in Stage 4. The detailed steps in each stage are described below.

4.2.1 Stage 1: Game Structure. An existing lab exercise may contain multiple tasks, and each task is identified as a set of lab instructions and challenges with the same objectives. A course instructor may need to re-order the tasks according to the instructor's teaching plan. The tasks and challenges form the main body of the game structure, which needs to be reviewed before progressing. Once the structure is fixed, story scenarios can be added to describe students' missions in the game scenario. We learned that our students prefer real-life scenarios, so a popular mission is to play a cybersecurity professional role. The following is an example of the scenario of Task 1 in the wireless security lab.

> *As a newly hired intern at the Orange Cafe, you notice that the company is still using WEP. Knowing the dangers of WEP and the exploits within it, you attempt to bring the issue up to your supervisor. Your supervisor allows you to compile a presentation on the matter which you will present at the next company meeting in a few days.*

4.2.2 Workload Analysis. Given the original lab exercises, the steps of identifying and ordering tasks do not require much effort, but extra work is needed in the storytelling step. However, we found it easy to define missions in a relevant scenario by referring to some real-world cases. In addition, storytelling can be created by student assistants because it does not require domain expertise.

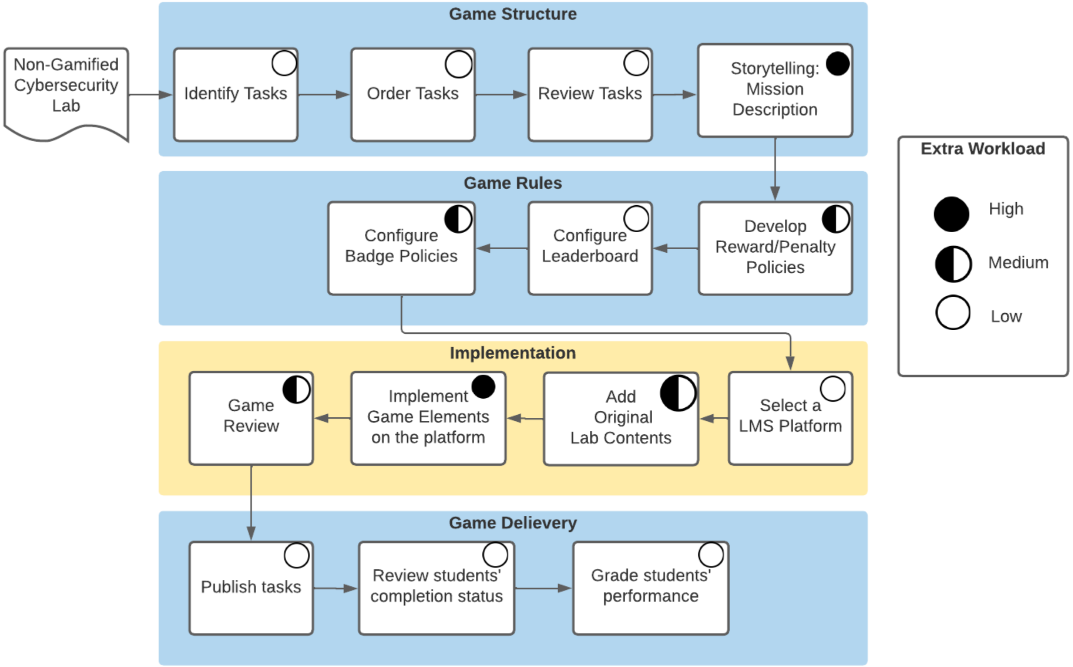
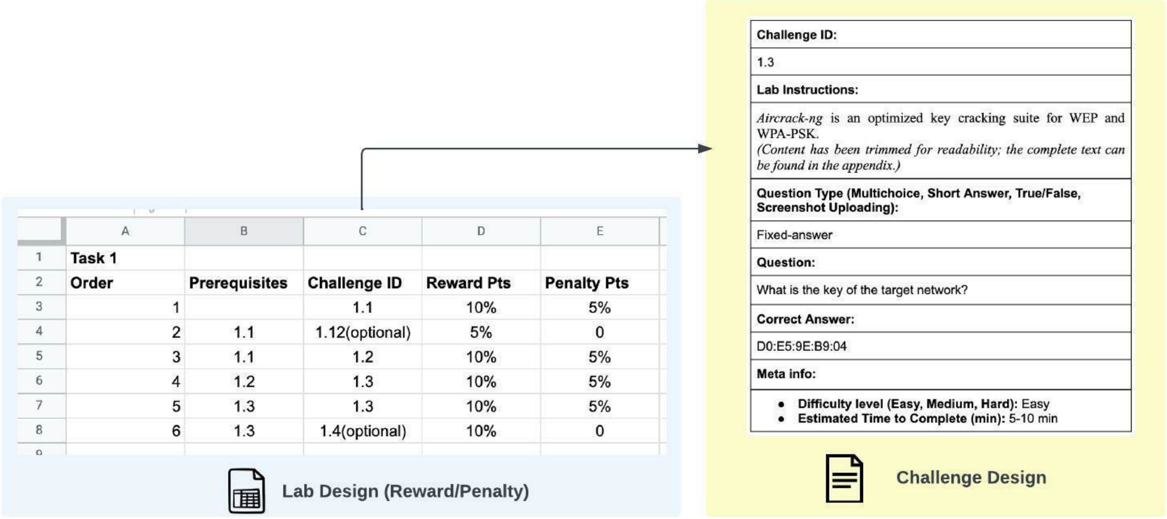

Game Structure
Non-Gamified Cybersecurity Lab
Identify Tasks ○
Order Tasks ○
Review Tasks ○
Storytelling: Mission Description ●
Game Rules
Configure Badge Policies ◐
Configure Leaderboard ○
Develop Reward/Penalty Policies ◐
Implementation
Game Review ◐
Implement Game Elements on the platform ●
Add Original Lab Contents ◐
Select a LMS Platform ○
Game Delievery
Publish tasks ○
Review students' completion status ○
Grade students' performance ○
Extra Workload
● High
◐ Medium
○ Low

Figure 2. The Workflow of Transforming a Traditional Lab to a Gamified Lab (The Level of Extra Workload Is Estimated by the Course Instructor in Our Study)



	A	B	C	D	E
1	Task 1				
2	Order	Prerequisites	Challenge ID	Reward Pts	Penalty Pts
3	1		1.1	10%	5%
4	2	1.1	1.12(optional)	5%	0
5	3	1.1	1.2	10%	5%
6	4	1.2	1.3	10%	5%
7	5	1.3	1.3	10%	5%
8	6	1.3	1.4(optional)	10%	0

Challenge ID:
1.3
Lab Instructions:
Aircrack-ng is an optimized key cracking suite for WEP and WPA-PSK. *(Content has been trimmed for readability; the complete text can be found in the appendix.)*
Question Type (Multichoice, Short Answer, True/False, Screenshot Uploading):
Fixed-answer
Question:
What is the key of the target network?
Correct Answer:
D0:E5:9E:B9:04
Meta info:
• **Difficulty level (Easy, Medium, Hard):** Easy • **Estimated Time to Complete (min):** 5-10 min

Figure 3. An Example of Lab Design and Challenge Design (The Design Templates and a Full-Content Challenge Example Are Available in Appendix C)

4.2.3 Stage 2. Game Rules. Once the game structure is fixed, the second stage is to design the game rules, including the reward/penalty, leaderboard, and badge policies. The reward/penalty policies can be determined based on the original course assessment strategy. For instance, instructors may offer more points to students who can address a more complex challenge. The leaderboard and badges can be further set up based on the reward points. We configured the leaderboard to show the top 10 players and awarded badges when a player finished a task and earned a certain number of points.

4.2.4 Workload Analysis. Moderate extra work is required to design the game rules. We first divided the workload using templates in Google Docs and Spreadsheet. As it is shown in Figure 3, a lab is made up of a sequence of challenges laid out in a Google Spreadsheet that come with rewards and penalties. Every challenge was created using a template that contained the challenge ID, lab instructions, question type, correct response, and metadata. Metadata were added for consideration of rewards, such as difficulty level and estimated completion time. Other components of a challenge, including lab instructions, question type, and question, can be directly copied from the original lab. There are two major advantages of using these templates: (1) It separates the design and implementation. Instructors can divide the work by challenges and tasks. If student assistants are available, the work can be assigned accordingly; and (2) it is easy to make changes to reward/penalty policies of challenges.

4.2.5 Stage 3: Implementation. The design of the gamified lab can be completed after Stages 1 and 2. The next stage implements the game elements and lab contents that can be delivered to students. Many universities have adopted Learning Management Systems (LMS) for instructors to integrate and manage learning materials, such as Blackboard and Canvas. To reduce workload, instructors can directly use the gamification features provided by an available LMS if the LMS supports gamification. Because of the lack of gamification support from the available LMS, we used a third-party gamification LMS named *Gametize* to implement the instructions and challenges of gamified labs. The next step is to add the original lab instructions to the LMS according to the tasks and challenges designed in the Game Structure stage. Figure A4 in Appendix D shows an example of the lab instructions presented in web format. After filling in the contents, game elements can be implemented according to the policies designed in the Game Rules stage. Finally, a gamified lab needs to be reviewed and tested before being delivered in classes.

We gamified the aforementioned wireless security lab (Section 3.2). Some examples of gamification elements are demonstrated in Appendix D, Figure A4. The lab starts with an introduction, followed by a brief story scenario that provides the context and the player's role in the exercise (Figure A4a). Each specific challenge is given with detailed instructions, according to the sequence determined in the design process (Figure A4b). Players earn points by completing the challenge or selecting the correct answer to questions after reading and following the instructions (Figure A4c). There are many different types of challenges, such as multiple-choice questions and questions with a fixed answer (Figure A4d). They receive instant feedback on their actions in the lab (Figure A4e) and can also access the leaderboard at any time to compare their performance against that of other students in the class, which promotes competition (Figure A4f). Special badges are given to players for various achievements, such as being among the first to complete a specific task (Figure A4g).

4.2.6 Workload Analysis. The Implementation stage has the greatest workload. However, instructors can anticipate the amount of work in the Game Structure and Game Rules stages. In addition, an easy-to-use LMS that supports gamification can greatly reduce the workload. We chose to use a third-party LMS because the original LMS adopted by the university does not support gamification. As a result, moderate efforts were required to convert the original lab instruction in Word format to another format (webpage) that is required by the LMS. In addition, the workload of implementing the game elements depends greatly on how well the LMS supports gamification.

Tasks	Timeline
Task 0 (Game Tutorial): How to play the game Read learning objectives Read how the tasks are organized Read how to locate instructions Practice submitting answers using the platform Practice reviewing reward points and leaderboard **Task 1: Crack the passcode of a wireless network (Same as Task 1 described in Section 3.2)** **Task 2: Configure a secure wireless network (Same as Task 2 described in Section 3.2)** **Task 3: Search for geolocation using MAC address (Same as Task 3 described in Section 3.2)** **Task 4: Practice cracking passcode (Same as Task 4 described in Section 3.2)**	**Day 1:** First class was given (2 hours) **Tasks 0, 1, 2, and 3 were released to students** Day 2: No class Tasks 0, 1, 2, and 3 remained available **Day 3:** Second class was given (2 hours) Tasks 0, 1, 2, and 3 remained available **Task 4 was released to students.** Days 4-8: No class All tasks remained available **Day 8 was the deadline to complete the lab**

Table 2. Task Description and Experiment Timeline

An easy-to-use LMS (e.g., Gametize) allows instructors to define rules for rewarding/penalty, offering badges, and ranking on leaderboards so that no manual work is needed afterward.

4.2.7 Stage 4: Game Delivery. The gamified lab was delivered to two classes of the Network Security course in Spring 2021 and two classes in Fall 2021. In addition to the tasks included in the original non-gamified lab described in Section 3.2, a new task was added that teaches the students how to use the gamification platform. The contents of other tasks are identical to the original tasks. Table 2 demonstrates the timeline of our study. In total, 8 days were allowed to complete the lab. Day 1 was when the first class meeting was held in the week and Day 3 was when the second class meeting was held. The instructor used half of the time in each class (1 hour) to deliver the course contents and let the students work on the lab tasks in the remaining time. Students could also complete the tasks after class if they could not complete them in class. Tasks 0, 1, 2, and 3 were released on Day 1 and Task 4 was released on Day 3.

4.2.8 Workload Analysis. The delivery and management of the lab are very easy once the gamified lab is implemented. First, gamification allows instructors to assess student performance in real time. When students are working in the lab, an instructor is able to review the leaderboard and each student's challenge completion status. This capability allows an instructor to gauge overall class progress and offer help if needed when students are working at their own pace. Additionally, the grading time can be significantly reduced in gamified labs. The implementation of multiple-choice and short-answer challenges is similar to online quizzes because short answers have been provided. Therefore, students' answers can be automatically graded in real time. After the lab is completed, the instructor can review the final reward points received by students and the time used for completion and grade student performance accordingly. However, we noticed that considering completion time in grading may discourage some students from reading instructions and critical thinking. Therefore, we used only the reward points to grade student performance.

5. EVIDENCE

This section details the outcomes of the gamifying cybersecurity lab exercise we designed and conducted. In particular, we collected activity reports, including join time, completion time, points, and comments. Students were also asked to complete a post-lab survey to evaluate the effectiveness and practicality of gamifying cybersecurity labs for students. We conducted the study in Spring 2021 and Fall 2021. The gamified lab was completed by 76 students in total, and 35 of them participated in surveys.

5.1 Learning Outcomes

All students were asked to answer questions in a test after completing the lab that assessed their understanding of the concepts outlined in Table 1. The percent accuracy of students' answers was used to assess their performance. The first plot in Figure 4 demonstrates that the students had a strong performance after completing the gamified labs in the semesters of Spring 2021 and Fall 2021 (n = 76). We found that 65.8% of students were able to answer 100% of the questions correctly, and 93.4% of students managed to score over 80%. In comparison, we referred to the performance of the students who completed non-gamified labs in the previous semester of Fall 2020 (n = 37). We discovered a smaller percentage of students (86.5%) who scored above 80%. However, the data were gathered throughout a number of semesters that were taught in various contexts, taking into account the use of hybrid teaching in the Fall 2020 semester. To draw statistically significant comparative conclusions, we plan to gather more data by running both gamified and non-gamified labs in future semesters.

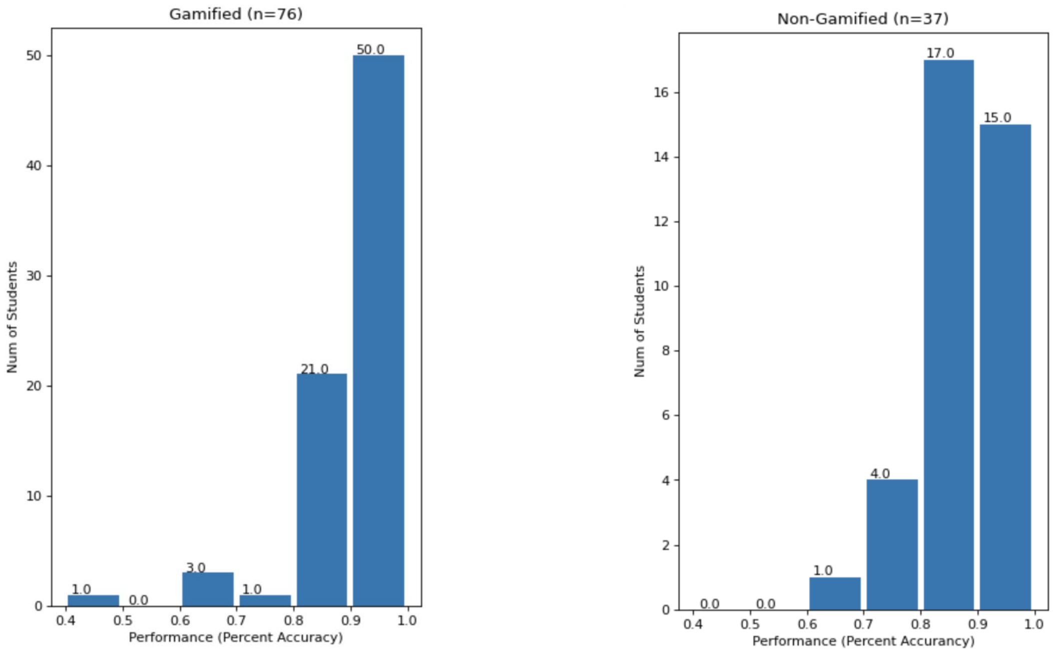
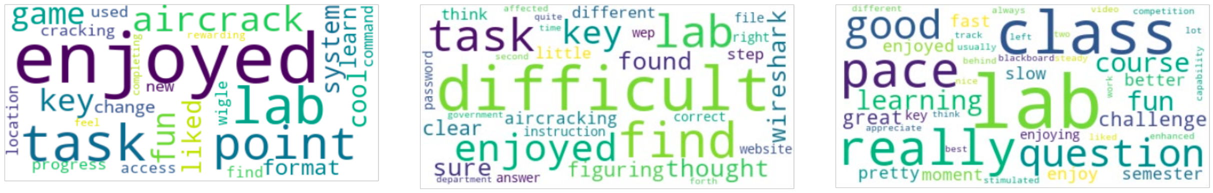


Figure 4. Students' Performance in Answering the Review Questions Testing Their Understanding of Cybersecurity Concepts

	Mean	Standard Deviation	Min	1st Quartile	Median	3rd Quartile	Max
Appropriate Challenge	4.42	0.46	3.43	4.14	4.43	4.79	5.00
Intrinsic Motivation	4.04	0.70	2.29	3.64	4.00	4.57	5.00
Extrinsic Motivation	4.46	0.80	1.00	4.00	4.67	5.00	5.00
Career Interests	4.22	0.73	1.67	3.83	4.50	4.67	5.00
Learning Outcome	4.58	0.61	2.50	4.25	5.00	5.00	5.00

Table 3. Results of Student Responses to the Post-Lab Survey



(a) Q1: Which part of the lab did you enjoy the most?

(b) Q2: Which part of the lab did you find the most difficult?

(c) Q3: What other questions/thoughts/comments do you have?

Figure 5. Word Cloud of Student Comments to Open-Ended Questions in the Post-Lab Survey

5.2 Student Engagement

In the post-survey, students were asked a series of questions to assess the effectiveness of the gamifying lab, including a 5-point Likert question section and an open-ended question section. Given the students' survey responses (n = 35), we calculated the average Likert question score (from 1 to 5) for each student based on the five categories of questions, and the results are summarized in Table 3.

At the end of the post-survey, we presented three open questions regarding the participants' experience with the gamification labs and asked their suggestions for improvements as follows: Q1) Which part of the lab did you enjoy the most? Q2) Which part of the lab did you find the most difficult? Q3) What other questions/thoughts/comments do you have? To summarize the participants' answers, we first cleaned the text to use text mining techniques, including removing special symbols and stop words, converting them to lowercase letters, and stemming and then visualized the popular words from the responses to each question in word clouds based on frequency and relevance. The results are shown in Figure 5. We found that most participants enjoyed using aircrack to crack passwords, while some found it difficult to address Task 4 without stepwise instructions. Answering Q3, most participants reported the gamification labs to be highly innovative (e.g., "*different from what we usually do*"), instructive (e.g., "*help me understand what we are learning*"), and entertaining (e.g., "*pretty fun*"). In addition, most indicated that they gained knowledge in the lab, that the game system is easy to use, and that the game elements can promote competition and efficiency. Some example quotes from the students are as follows: "*I enjoyed the point system of the game. It inspired me to push myself to do the best that I can and feel rewarded afterwards.*" "*I enjoyed it being in the game format because it made it more fun to learn this way.*" "*The point system was pretty cool and I liked how the different steps of the lab were broken down. I felt like I was accomplishing something.*" "*I like the competition aspect a lot. Really enjoy doing labs and learning.*" "*I really enjoyed this lab and I would enjoy doing more labs like this! I feel like my learning capabilities were enhanced and stimulated through this.*" Furthermore, students also suggested increasing the number of labs, adding challenges of various difficulty levels, and allowing multiple attempts.

Based on the activity reports and post-lab survey data, we could infer that students acquired the learning objectives we intended to teach through an experiential learning process. The intended learning objectives include having the capability to explain and apply wireless security techniques which are described in Table 1 in more detail.

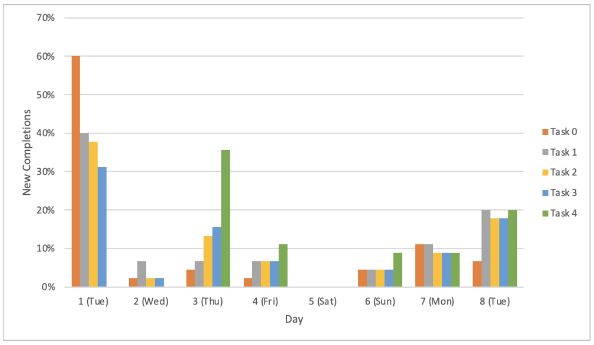


Figure 6. Percentage of Students Who Completed the Tasks on Each Day

Figure 6 shows how students progressed in completing each task over the 8 days of the experiment. Tasks 0, 1, 2, and 3 were completed on Day 1 (the same day they were released) by 60%, 40%, 38%, and 31% of students, respectively. Task 4 was completed by 36% of students on the day of its release (Day 3). By the end of Day 4, the percentages of students who had completed Tasks 0, 1, 2, 3, and 4 were 68%, 61%, 60%, 53%, and 47%, respectively. Day 8 was the deadline for the assignment. Only 7% of students completed every task on the day each was released; 84% of students completed all the tasks before the deadline. The completion reports enabled the instructor to review how well each student had performed on specific tasks and to understand the obstacles students encountered during the assignment.

6. DISCUSSION

6.1 Students' Motivation and Learning Outcomes

Overall, we found the gamified lab exercises help students be motivated to learn the course materials better. According to the survey results, participating students perceived that gamification increased their interest and engagement. As previous gamification research has revealed, we provided an easily accessible leaderboard so that students are engaged and motivated through competition. Badges are given at different levels to recognize students' achieving milestones, encouraging them between the beginning and the finish line. As a result, the task completion reports show that by the end of Day 4, 56% of students had completed Tasks 0, 1, 2, and 3, while 47% of students had also completed Task 4. In total, 84% of students managed to complete the lab within 8 days. In the prior semester, students were asked to complete the original non-gamified lab in 2 weeks, and the instructor found that more than half of the students could not finish the lab in the first week. The introduction of the gamified labs made a more condensed time window, yet more students were able to finish the lab before the deadline. It is a promising finding that gamification better motivates students more than traditional labs do to complete the lab early.

Moreover, instant feedback played an important role in engaging students. The gamification platform automatically checked students' answers to the questions and let them know instantly whether their answer was correct or not. Unlike the traditional lab exercises, students do not have to wait several days until their work is graded to receive feedback from the instructor. We believe that instant feedback helps students assess their knowledge quickly and motivates them to acquire the necessary knowledge to solve the questions.

Another benefit we found in students' learning experience was that the gamified lab exercises could dissect a large chunk of exercise into smaller tasks and provide a separate task screen for each of them. While some students may be overwhelmed by the large, consolidated document-based traditional lab exercises, they could easily manage the small tasks that are properly connected in a series of visualized screens backed by the storyline. A storyline that mimics real-world situations was embedded in the game so students could understand the context and be better engaged than in the traditional labs. Students can also easily navigate between tasks on the gamified platform, which helps them locate instructions and submit their work easily.

6.2 Benefits for Instructors

We found there are several apparent benefits that instructors can gain from gamifying lab exercises. First, gamified labs free up instructors' time so they may spend more time interacting with the students. After implementing the gamified lab exercises, the instructors were able to address questions or other issues while students were working on tasks in the experiment. We also observed that students raised fewer questions reflecting failure to properly review lab instructions or reading materials compared with previous classes using traditional labs. This demonstrates that students were more inclined to carefully read lab materials provided in the context of gamified challenges.

Second, gamified labs make it easier for instructors to check and understand the student's learning progress. The completion reports are easily accessible in the gamification platform and enable the instructor to monitor the progress of the class, thereby gaining a better understanding of student's learning progress in the lab. For example, the instructor was able to identify a challenge that several students found difficult by tracking the time spent on it and the number of unsuccessful attempts until they got a successful outcome.

Third, grading in the gamified labs is much quicker and more accurate. Although the instructor has to spend time setting the correct answers in the gamified lab design and development phase, the grading process is quick and much easier than with traditional labs because the students' completion reports are automatically generated by the gamification platform.

6.3 Additional Workload for Instructors

The gamification process demonstrated in Figure 3 shows that some extra work is necessary to develop the gamified lab. One of the objectives of this paper is to share our experience with gamifying traditional labs to help instructors estimate and manage the extra workload required for gamification. From our experience with gamifying the cybersecurity lab exercises, we found the most time-consuming phases were as follows. First, we needed to review various gamification platforms that are currently available and select the best platform based on our needs and budget. Depending on the needs and the budget an instructor has, the amount of extra work may vary. To help instructors make this decision, we conducted a comprehensive investigation of existing platforms and provided guidelines based on our findings, which are available in Appendix A. Second, significant efforts were needed to develop stories as well as mission descriptions within the story scenario. Because storytelling is an essential part of students' acceptance and engagement in the gamified lab, we recommend instructors spend enough time and effort to develop appropriate stories and mission descriptions. It would be helpful to build a storytelling database for instructors to customize as the basis of their labs. Third, we spent considerable time configuring the game rules, such as deciding how reward points would be allocated, designing badges, and locking tasks to control the flow. Instructors should expect this process to be done in several iterations. We did several refinements until we developed the final game rules.

6.4 Suggestions

Based on our observations and reflections on the lab, as well as the feedback and suggestions from students, we make the following suggestions for the instructors who are preparing gamified cybersecurity lab exercises. First, it is important to form a very solid plan in the early stage, allowing a substantial amount of time for each preparation and implementation step. Instructors may have to put in extra work because converting a traditional lab to a gamified one and setting up the process requires various efforts by the instructor as described in our example. Our paper should help them estimate the approximate time and effort needed for the preparation and design process. The comprehensive process depicted in Figure 3 can be customized based on the instructor's needs.

Second, instructors should allow sufficient time for implementation before they start to use the gamified lab. The implementation time can be estimated by referring to our gamification process (Figure 3) and controlled by the instructor based on how many gamification elements are to be included. Once the gamified lab is ready, the instructor can decide when to use it in class as when using traditional labs. The gamified labs can be used for reviewing the lecture content or alternatively for introducing students to the new content. Regarding the timeline, we found starting the gamified lab after students have learned the basic concepts of wireless network and security protocols is best so they can reinforce the knowledge from the class through the gamified labs.

Students should also be given sufficient time to complete the lab tasks. We suggest using gamified labs as an independent class activity, such as homework assignments. If a gamified lab is combined with other class activities and/or not properly emphasized, students may not pay enough attention to playing the game. In addition, the instructor should clearly explain to students the gamified lab elements, including the game background, system, rules, and rewards, so that students can clearly understand the overall gamified activity. If the gamified lab is run as an in-class activity, it is helpful to keep the lab accessible after class. We found that advanced students in cybersecurity may want to complete more challenging tasks; therefore, optional/bonus tasks may be added to increase practice and difficulty. A reflection task could also be added to the lab, giving students the opportunity to reflect on their experiences and show their understanding of the topics.

There are still several points to be improved in our current gamified lab. Since the current game process used in this study follows a linear flow, it can be improved by creating a flexible game flow and assigning follow-up tasks based on the previous tasks. Also, more metadata information can be added to the game, for instance concerning challenge difficulty level. We believe the metadata will help instructors when they need to revise the existing game or add more tasks to the game. Finally, at present all the exercises are designed to be played by individual students. Because working as a team is a significant element in cybersecurity education, in the future teamwork tasks could be added to the lab to improve students' collaboration skills.

Last, it is noteworthy that the gamification process we have followed and shown above was focused on teaching a technical subject, namely, network security. Hence, we believe the instructors who are considering creating gamified exercises in such a technical course will get direct benefits from our teaching tip article. We also believe that instructors who teach non-technical courses may find useful information because the fundamental principles we adopted for gamifying processes, such as leaderboard, badging, and award announcement can be applied to gamifying any other subjects. In addition, the platform we used to gamify the lab exercises is being used for various purposes. This article can make a good case for such a gamification platform.

7. CONCLUSIONS

This paper describes in detail an overall process for gamifying cybersecurity labs. Although this is complex and requires significant time and effort from the instructor, we found that using a gamified cybersecurity lab as a pedagogic technique can effectively motivate students and enhance their learning experience. Our paper thus makes an innovative and enlightening contribution to cybersecurity education. For instructors who consider converting traditional lab exercises to gamified ones, this paper offers a better understanding of the conversion process, including its benefits and pitfalls.

8. REFERENCES

Adams, M., & Makramalla, M. (2015). Cybersecurity Skills Training: An Attacker-Centric Gamified Approach. *Technology Innovation Management Review*, 5(1), 5-14.

Beuran, R., Chinen, K.-i., Tan, Y., & Shinoda, Y. (2016). Towards Effective Cybersecurity Education and Training. *Research Report* (School of Information Science, Graduate School of Advanced Science and Technology, Japan Advanced Institute of Science and Technology), IS-RR-2016(003), 1-16.

Coenraad, M., Pellicone, A., Ketelhut, D. J., Cukier, M., Plane, J., & Weintrop, D. (2020). Experiencing Cybersecurity One Game at a Time: A Systematic Review of Cybersecurity Digital Games. *Simulation & Gaming*, 51(5), 586-611.

Demmese, F., Yuan, X., & Dicheva, D. (2020). Evaluating the Effectiveness of Gamification on Students' Performance in a Cybersecurity Course. *Journal of The Colloquium for Information Systems Security Education*, 8(1), 1-6.

Deterding, S., Dixon, D., Khaled, R., & Nacke, L. (2011). From Game Design Elements to Gamefulness: Defining Gamification. *Proceedings of the 15th International Academic MindTrek Conference: Envisioning Future Media Environments* (pp. 9-15).

Donovan, L., & Lead, P. (2012). *The Use of Serious Games in the Corporate Sector: A State of the Art Report*. Dublin: Learnovate Centre.

Faria, A. J. (1998). Business Simulation Games: Current Usage Levels—An Update. *Simulation & Gaming*, 29(3), 295-308.

Faria, A. J., & Wellington, W. J. (2004). A Survey of Simulation Game Users, Former-Users, and Never-Users. *Simulation & Gaming*, 35(2), 178-207.

Garris, R., Ahlers, R., & Driskell, J. E. (2002). Games, Motivation, and Learning: A Research and Practice Model. *Simulation & Gaming*, 33(4), 441-467.

IBM. (2021). IBM Cybersecurity. https://www.ibm.com/academic/technology/security

Kapp, K. M. (2012). *The Gamification of Learning and Instruction: Game-Based Methods and Strategies for Training and Education*. John Wiley & Sons.

Karagiannis, S., & Magkos, E. (2021). Engaging Students in Basic Cybersecurity Concepts Using Digital Game-Based Learning: Computer Games as Virtual Learning Environments. In *Advances in Core Computer Science-Based Technologies* (pp. 55-81). Springer.

Lepper, M., & Malone, T. (1987). Intrinsic Motivation and Instructional Effectiveness in Computer-Based Education. In R. E. Snow & M. J. Farr (Eds.), *Aptitude, Learning, and Instruction* (vol. 3, pp. 255-286).

Malone, T. W. (1981). Toward a Theory of Intrinsically Motivating Instruction. *Cognitive Science*, 5(4), 333-369.

Omar, N. S., Foozy, C. F. M., Hamid, I. R. A., Hafit, H., Arbain, A. F., & Shamala, P. (2021). Malware Awareness Tool for Internet Safety Using Gamification Techniques. *Journal of Physics: Conference Series* (vol. 1874, no. 1, p. 012023). IOP Publishing.

Parker, L. E., & Lepper, M. R. (1992). Effects of Fantasy Contexts on Children's Learning and Motivation: Making Learning More Fun. *Journal of Personality and Social Psychology*, 62(4), 625-633.

Piaget, J. (1952). The Third Stage: The "Secondary Circular Reactions" and the Procedures Destined to Make Interesting Sights Last. In J. Piaget & M. Cook (Trans.), *The Origins of Intelligence in Children* (pp. 153-209). W. W. Norton & Co.

Qusa, H., & Tarazi, J. (2021). Cyber-Hero: A Gamification Framework for Cyber Security Awareness for High School Students. [Paper presentation]. *The 2021 IEEE 11th Annual Computing and Communication Workshop and Conference* (CCWC). NV, USA (virtual).

Rieber, L. P. (1996). Seriously Considering Play: Designing Interactive Learning Environments Based on the Blending of Microworlds, Simulations, and Games. *Educational Technology Research and Development*, 44(2), 43-58.

Ros, S., Gonzalez, S., Robles, A., Tobarra, L., Caminero, A., & Cano, J. (2020). Analyzing Students' Self-Perception of Success and Learning Effectiveness Using Gamification in an Online Cybersecurity Course. *IEEE Access*, 8, 97718-97728.

Schreuders, Z. C., & Butterfield, E. (2016). Gamification for Teaching and Learning Computer Security in Higher Education. [Paper presentation]. *The 2016 USENIX Workshop on Advances in Security Education*. Austin, TX.

Tioh, J.-N., Mina, M., & Jacobson, D. W. (2019). Cyber Security Social Engineers An Extensible Teaching Tool for Social Engineering Education and Awareness. [Paper presentation]. *The 2019 IEEE Frontiers in Education Conference* (FIE). Covington, KY.

Van Eck, R. (2006). Digital Game-Based Learning: It's Not Just the Digital Natives Who Are Restless. EDUCAUSE Review, 41(2), 16-30.

Wolfenden, B. (2019). Gamification as a Winning Cyber Security Strategy. Computer Fraud & Security, 2019(5), 9-12.

Zichermann, G., & Cunningham, C. (2011). *Gamification by Design: Implementing Game Mechanics in Web and Mobile Apps*. O'Reilly Media.

AUTHOR BIOGRAPHIES

J.B. (Joo Baek) Kim is an assistant professor in the John H. Sykes College of Business at the University of Tampa (UT) in Tampa, Florida. Before he joined UT, he worked at Worcester Polytechnic Institute in Worcester, Massachusetts. He received his Ph.D. from Louisiana State University. His work/interest encompasses serious games in business contexts, business simulation games, gamification, and online user reviews and interactions. His research work has been published in peer-reviewed journals such as *Information Technology and People* (ITP) and the *Asia Pacific Journal of Information Systems* (APJIS), and in various conference proceedings.

Chen Zhong is an assistant professor of Cybersecurity in the John H. Sykes College of Business at The University of Tampa. She received her doctoral degree in Information Sciences and Technology from Pennsylvania State University in 2016. Her current research interest includes network security, intrusion detection, artificial intelligence, and cybersecurity education. Dr. Zhong has published in the refereed journals and conference proceedings, such as *Computers & Security*, *IEEE Systems Journal*, *IEEE Conference on Cognitive and Computational Aspects of Situation Management* (CogSIMA).

Hong Liu is an associate professor of computer science in the School of Sciences at Indiana University Kokomo. She earned her Ph.D. from Oklahoma State University. Her research spans various computer science domains, encompassing data cleaning, quality management, artificial intelligence, cybersecurity, and innovative approaches in computing education. Dr. Liu applies advanced technologies to bolster these fields, connecting theoretical principles with practical implementations. Additionally, she actively engages in education, consistently fostering curiosity and encouraging the pursuit of learning in her students.

APPENDICES

Appendix A. Gamifying Platform

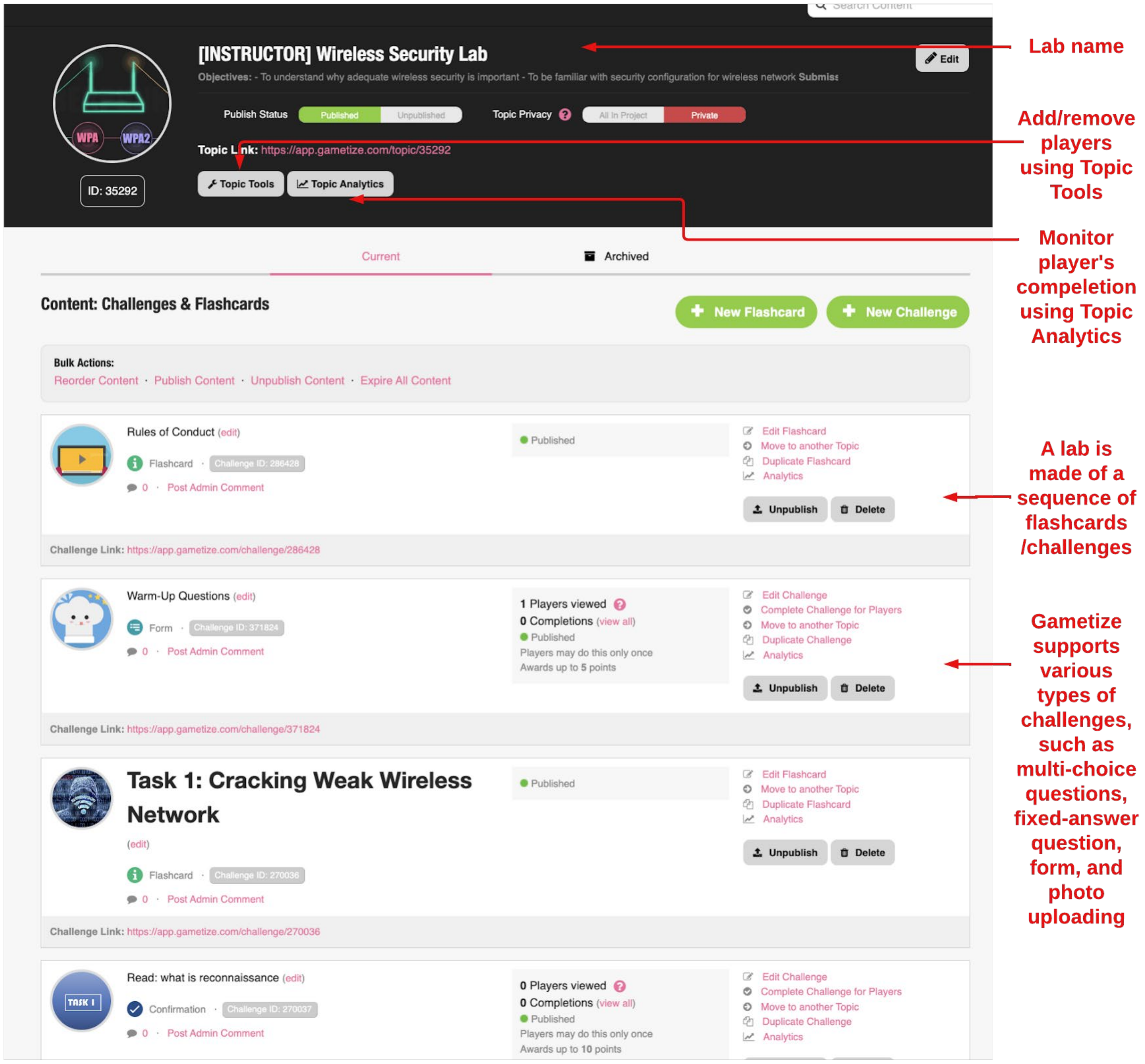
Before implementing the converted labs in a gamification platform, we extensively explored multiple options for gamified lab implementation, including integrating the gamification functions into a learning management system (LMS) and using stand-alone gamification platforms. First, we considered using a leaderboard and badge function plug-in that could be installed on the university's LMS (Blackboard). However, this would have required a technical configuration supported by the university's IT department involving a long process of verifying security and evaluating the university-wide impact. We therefore sought an alternative way to implement the gamified labs.

We considered a wide variety of gamification platforms available in the market and narrowed them down to several candidates, which we then extensively evaluated to find the best platform for our purpose. The capabilities and features of these gamification platforms are summarized in Table A1. Based on the information and the short hands-on experience, we went through the evaluation process among the gamification project team. The evaluation criteria included (among others) cost, customizability, user interface, support for graphics/videos, and degree of "gamishness."

Gamification Platform	Gametize (https://gametize.com)	Influitive (https://influitive.com/)	The Training Arcade (https://thetrainingarcade.com/)	Bunchball Nitro (https://www.biworldwide.com/gamification/bunchball-nitro/)
Features	Variety of Interactive Challenge Types Achievements Awardable Actions Bonus Points Teams Rewards Store Analytics web and mobile app	Analytics Automatic Notifications CRM Integration Geofencing Instant Message Leaderboards Loyalty Program Mobile Application Social Media Integration Widgets	Player-to-Player Challenges Team Tournaments Daily Mini-Games Level-Up and Achievements Systems individual game leaderboards Global Leaderboard	Teams Collaboration Engage Service & Support Teams Training, Learning & Development Activate Online Community
Devices Supported	Windows Linux Android iPhone/iPad Mac Web-based	Windows Android iPhone/iPad Mac Web-based	Web-based	Windows Linux Android iPhone/iPad Mac Web-based
Deployment	Cloud Hosted On-Premise	Cloud Hosted	Cloud Hosted	Cloud Hosted
Pricing Model	Monthly payment Annual Subscription Price starts from $100 per month	Quote-based	Annual Subscription Price starts from $7499 per year	Quote-based
Available Support	Training	Training	Training	Training

Table A1. Summary of Gamification Platform Features

Eventually, we decided to implement the gamified lab on a commercial gamification platform named *Gametize* (https://gametize.com), which has provided a simple but efficient gamification platform since 2012. Various enterprises and organizations have been using Gametize to engage their employees, customers, and students; the Gametize platform has provided more than 20 million challenges, completed by 500,000 registered users (https://gametize.com/about). Compared with other gamification platforms, Gametize allows us to organize tasks and challenges in a clear and linear way, ensuring that students can easily navigate across tasks without confusion. In addition, Gametize supports HTML content, which makes it easy to display screenshots and codes.



[INSTRUCTOR] Wireless Security Lab

Objectives: - To understand why adequate wireless security is important - To be familiar with security configuration for wireless network Submiss

Topic Link: https://app.gametize.com/topic/35292

Content: Challenges & Flashcards

Rules of Conduct (edit)
Flashcard · Challenge ID: 286428
0 · Post Admin Comment
Published
Challenge Link: https://app.gametize.com/challenge/286428

Warm-Up Questions (edit)
Form · Challenge ID: 371824
0 · Post Admin Comment
1 Players viewed
0 Completions (view all)
Published
Players may do this only once
Awards up to 5 points
Challenge Link: https://app.gametize.com/challenge/371824

Task 1: Cracking Weak Wireless Network
(edit)
Flashcard · Challenge ID: 270036
0 · Post Admin Comment
Published
Challenge Link: https://app.gametize.com/challenge/270036

Read: what is reconnaissance (edit)
Confirmation · Challenge ID: 270037
0 · Post Admin Comment
0 Players viewed
0 Completions (view all)
Published
Players may do this only once
Awards up to 10 points

Lab name

Add/remove players using Topic Tools

Monitor player's compeletion using Topic Analytics

A lab is made of a sequence of flashcards /challenges

Gametize supports various types of challenges, such as multi-choice questions, fixed-answer question, form, and photo uploading

Figure A1. An Example Lab Implemented on Gametize, Including a Sequence of Flashcards and Challenges

Users may learn more about Gametize’s features by watching the several training videos available at https://corp.gametize.com/video-guides/. Most videos are between 3 and 5 minutes long. A teacher must first develop a project and then implement a lab within the project. Figure A1 shows a sample lab that has been created on Gametize that consists of a sequence of challenges and flashcards. A flashcard is a webpage that contains information only, while a challenge is a webpage with information and a question for players to answer. Gametize supports various types of challenges, such as multiple-choice questions, fixed-answer questions, forms, and photo uploading.

The instructor can decide which tasks and challenges to make available at which time. The instructor can also lock some challenges to add restrictions, for example, by preventing students from accessing a challenge before reading the introductory paragraph. When students are working on the lab, an instructor is able to review students’ completion status of challenges to gauge overall class progress. After the lab is completed, the instructor can review the reports of students’ activities and complete grading. Developing the gamified lab may reduce the grading workload; Section 6.2 discusses this further.

Appendix B. How to Play the Game

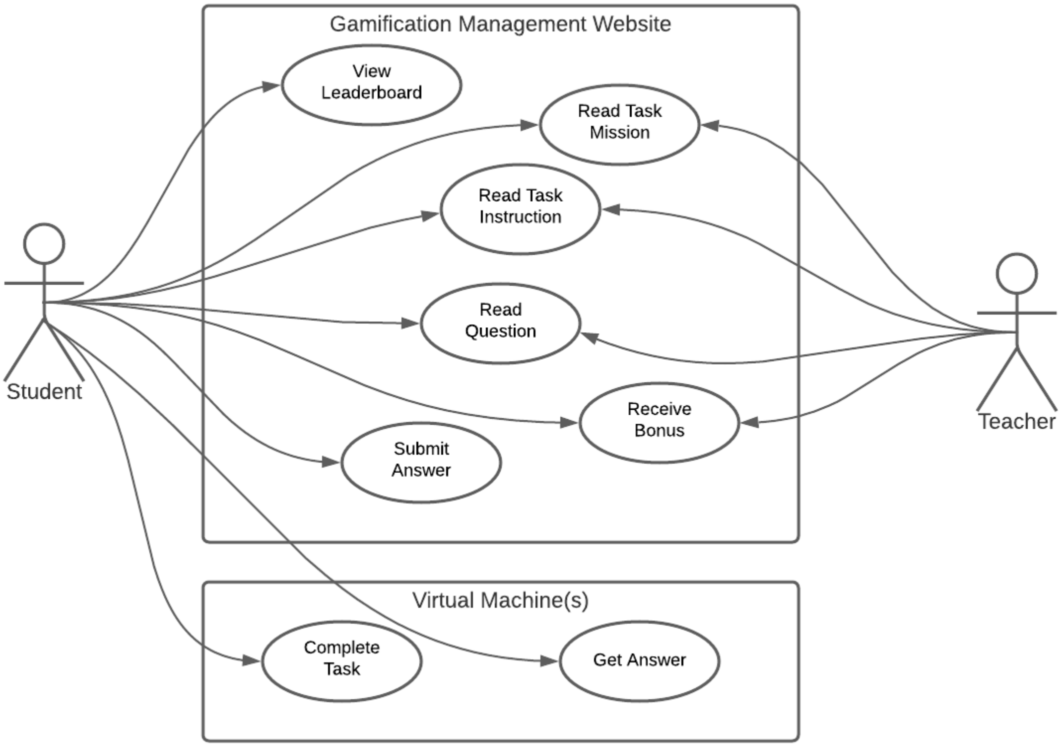
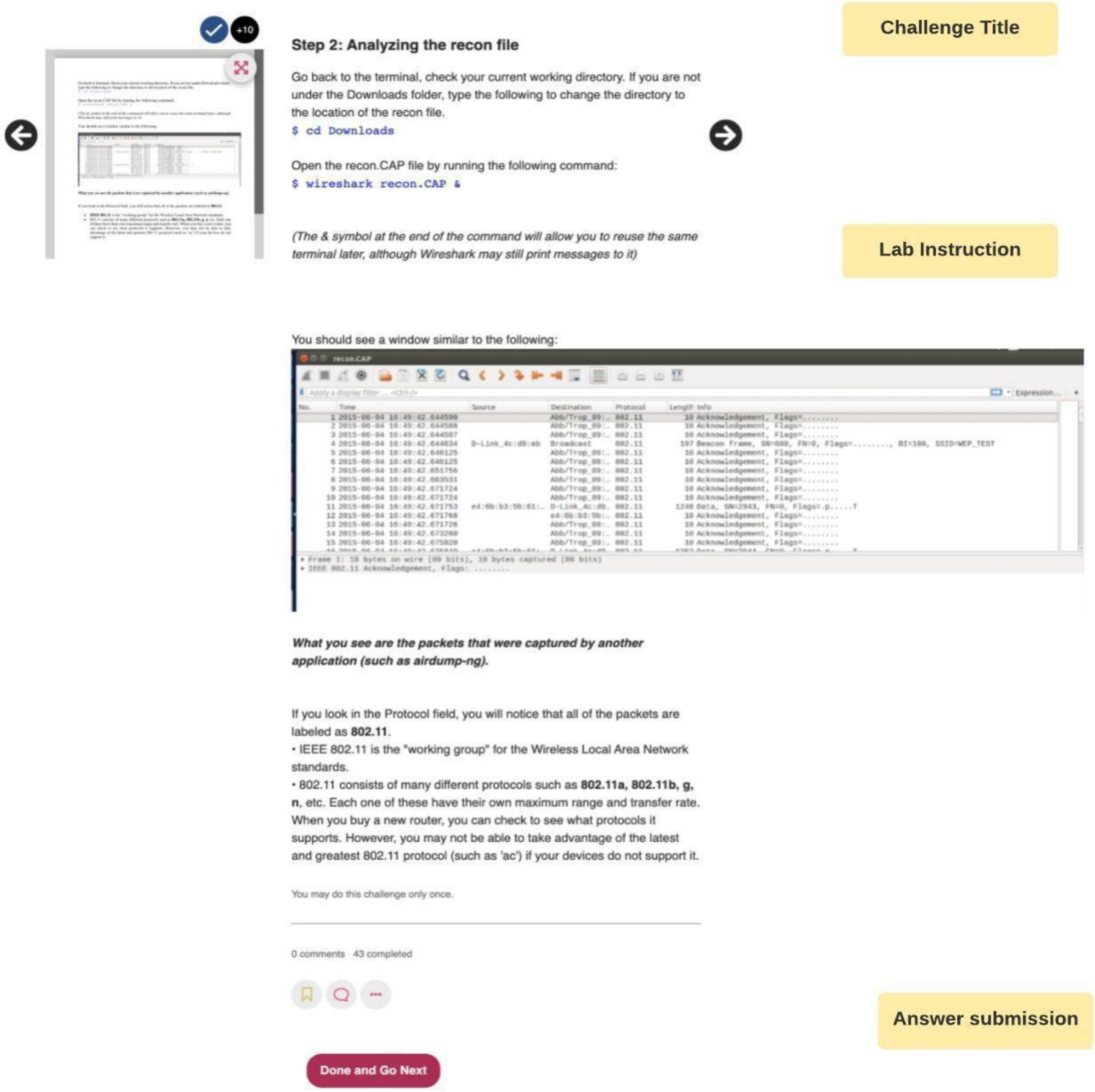


Figure A2. A Case Diagram of a Gamified Lab

Figure A2 demonstrates the use case of the gamification system. The lab contents and game elements are hosted on the Gametize website. Students followed the lab instructions and completed tasks on a virtual machine set up on their local computer. Instructors can manage the game via Gametize by reviewing students' completion status and assigning bonus points.

The gamified lab is structured as a sequence of tasks, each containing a scenario, mission description, lab instructions, and challenges. An example of a challenge is displayed in Figure A3.



Step 2: Analyzing the recon file

Go back to the terminal, check your current working directory. If you are not under the Downloads folder, type the following to change the directory to the location of the recon file.

```
$ cd Downloads
```

Open the recon.CAP file by running the following command:

```
$ wireshark recon.CAP &
```

(The & symbol at the end of the command will allow you to reuse the same terminal later, although Wireshark may still print messages to it)

You should see a window similar to the following:

```
recon.CAP
Apply a display filter ... <Ctrl-/>                                                     Expression...
No.   Time                        Source             Destination    Protocol  Length Info
    1 2015-06-04 16:49:42.644590                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
    2 2015-06-04 16:49:42.644588                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
    3 2015-06-04 16:49:42.644587                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
    4 2015-06-04 16:49:42.644634  D-Link_4c:d0:eb    Broadcast      802.11      197 Beacon frame, SN=680, FN=0, Flags=........, BI=100, SSID=WEP_TEST
    5 2015-06-04 16:49:42.646125                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
    6 2015-06-04 16:49:42.646125                     Abb/Trop_08:.. 802.11       10 Acknowledgement, Flags=........
    7 2015-06-04 16:49:42.651756                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
    8 2015-06-04 16:49:42.663531                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
    9 2015-06-04 16:49:42.671724                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
   10 2015-06-04 16:49:42.671724                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
   11 2015-06-04 16:49:42.671753  e4:6b:b3:5b:61:..  D-Link_4c:d0.. 802.11     1246 Data, SN=2943, FN=0, Flags=.p.....T
   12 2015-06-04 16:49:42.671768                     e4:6b:b3:5b:.. 802.11       10 Acknowledgement, Flags=........
   13 2015-06-04 16:49:42.671726                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
   14 2015-06-04 16:49:42.673260                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
   15 2015-06-04 16:49:42.675820                     Abb/Trop_09:.. 802.11       10 Acknowledgement, Flags=........
▸ Frame 1: 10 bytes on wire (80 bits), 10 bytes captured (80 bits)
▸ IEEE 802.11 Acknowledgement, Flags: ........
```

What you see are the packets that were captured by another application (such as airdump-ng).

If you look in the Protocol field, you will notice that all of the packets are labeled as **802.11**.
- IEEE 802.11 is the "working group" for the Wireless Local Area Network standards.
- 802.11 consists of many different protocols such as **802.11a, 802.11b, g, n**, etc. Each one of these have their own maximum range and transfer rate. When you buy a new router, you can check to see what protocols it supports. However, you may not be able to take advantage of the latest and greatest 802.11 protocol (such as 'ac') if your devices do not support it.

You may do this challenge only once.

0 comments   43 completed

Done and Go Next

Figure A3. Example of a Task Challenge

Appendix C. Gamified Lab Design Template

(1) Template for a Lab (containing multiple challenges)

Order	Story Telling	Challenge ID	Reward Pts	Penalty Pts	Lock (Y/N)	Badge
1						
2						
3						
: :						

(2) Template for an individual challenge

Challenge ID:
Lab Instructions:
Question Type (For example, multi-choice questions, fixed answer, or open-ended question:
Question:
Correct Answer:
Challenge Attributes:
● **Difficulty level (Easy, Medium, Hard):** ● **Estimated Time to Complete (min):**

(3) An example of challenge designed using the template

Challenge ID:
1.3
Lab Instructions:

Crack the password of the wireless network

Aircrack-ng is an optimized key cracking suite for WEP and WPA-PSK. Using this suite, we will be able to determine the key of our target network. First, we need to install the aircrack-ng software in the VM by running the command in the terminal:

```
$ sudo apt-get install -y aircrack-ng
```

Start aircrack-ng with the given SSID specified using the **-e** flag, or the BSSID (which is the MAC address of the router) specified using the **-b** flag. To crack the key using the SSID, run the command in the terminal:

```
$ aircrack-ng -e TEST recon.CAP
```

Question Type (Multichoice, Short Answer, True/False, Screenshot Uploading):

Fixed-answer

Question:

What is the key of the target network?

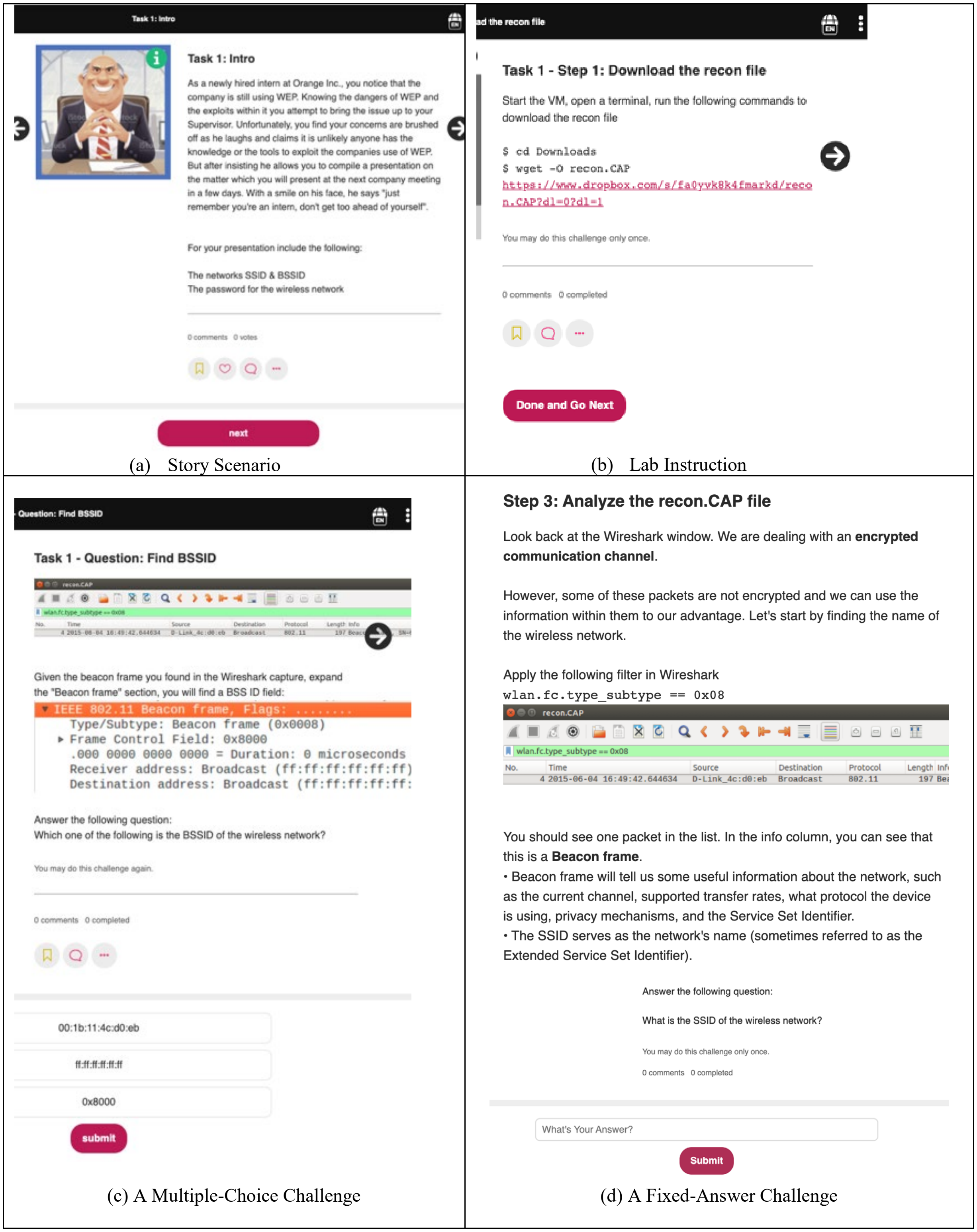
Correct Answer:

D0:E5:9E:B9:04

Meta info:

- **Difficulty level (Easy, Medium, Hard):** Easy
- **Estimated Time to Complete (min):** 5-10 min

Appendix D. Gamified Lab Example Screenshots



Task 1: Intro

As a newly hired intern at Orange Inc., you notice that the company is still using WEP. Knowing the dangers of WEP and the exploits within it you attempt to bring the issue up to your Supervisor. Unfortunately, you find your concerns are brushed off as he laughs and claims it is unlikely anyone has the knowledge or the tools to exploit the companies use of WEP. But after insisting he allows you to compile a presentation on the matter which you will present at the next company meeting in a few days. With a smile on his face, he says "just remember you're an intern, don't get too ahead of yourself".

For your presentation include the following:

The networks SSID & BSSID
The password for the wireless network

(a) Story Scenario

Task 1 - Step 1: Download the recon file

Start the VM, open a terminal, run the following commands to download the recon file

```
$ cd Downloads
$ wget -O recon.CAP
https://www.dropbox.com/s/fa0yvk8k4fmarkd/recon.CAP?dl=0?dl=1
```

You may do this challenge only once.

(b) Lab Instruction

Task 1 - Question: Find BSSID

recon.CAP
wlan.fc.type_subtype == 0x08
No. Time Source Destination Protocol Length Info

```
4 2015-06-04 16:49:42.644634 D-Link_4c:d0:eb Broadcast 802.11 197 Beac
```

Given the beacon frame you found in the Wireshark capture, expand the "Beacon frame" section, you will find a BSS ID field:

```
▼ IEEE 802.11 Beacon frame, Flags: ........
    Type/Subtype: Beacon frame (0x0008)
  ▶ Frame Control Field: 0x8000
    .000 0000 0000 0000 = Duration: 0 microseconds
    Receiver address: Broadcast (ff:ff:ff:ff:ff:ff)
    Destination address: Broadcast (ff:ff:ff:ff:ff:
```

Answer the following question:
Which one of the following is the BSSID of the wireless network?

You may do this challenge again.

○ 00:1b:11:4c:d0:eb
○ ff:ff:ff:ff:ff:ff
○ 0x8000

(c) A Multiple-Choice Challenge

Step 3: Analyze the recon.CAP file

Look back at the Wireshark window. We are dealing with an **encrypted communication channel**.

However, some of these packets are not encrypted and we can use the information within them to our advantage. Let's start by finding the name of the wireless network.

Apply the following filter in Wireshark
`wlan.fc.type_subtype == 0x08`

```
No.  Time                        Source           Destination  Protocol  Length  Info
   4 2015-06-04 16:49:42.644634  D-Link_4c:d0:eb  Broadcast    802.11       197  Bea
```

You should see one packet in the list. In the info column, you can see that this is a **Beacon frame**.

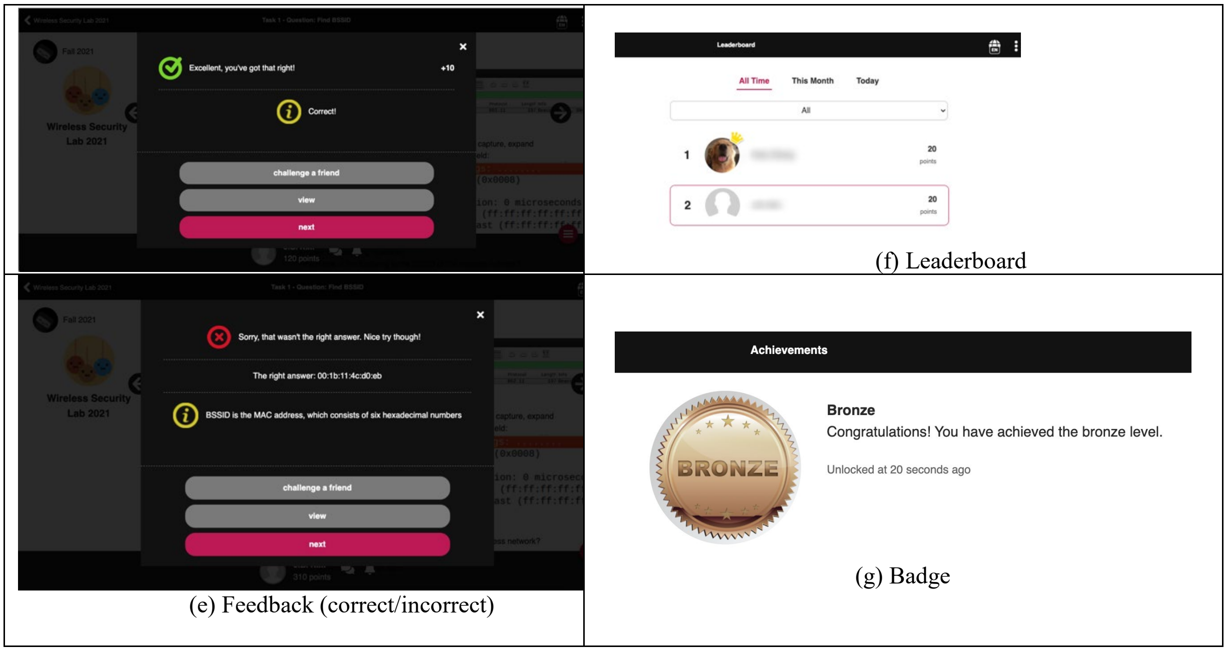
- Beacon frame will tell us some useful information about the network, such as the current channel, supported transfer rates, what protocol the device is using, privacy mechanisms, and the Service Set Identifier.
- The SSID serves as the network's name (sometimes referred to as the Extended Service Set Identifier).

Answer the following question:

What is the SSID of the wireless network?

You may do this challenge only once.

(d) A Fixed-Answer Challenge



Excellent, you've got that right! +10

Correct!

Sorry, that wasn't the right answer. Nice try though!

The right answer: 00:1b:11:4c:d0:eb

BSSID is the MAC address, which consists of six hexadecimal numbers

(e) Feedback (correct/incorrect)

1	[redacted]	20 points
2	[redacted]	20 points

(f) Leaderboard

Bronze

Congratulations! You have achieved the bronze level.

Unlocked at 20 seconds ago

(g) Badge

Figure A4. Gamified Lab Example Screenshots

Information Systems & Computing Academic Professionals

Education Special Interest Group

STATEMENT OF PEER REVIEW INTEGRITY

All papers published in the ***Journal of Information Systems Education*** have undergone rigorous peer review. This includes an initial editor screening and double-blind refereeing by three or more expert referees.

ISSN: 2574-3872 (Online) 1055-3096 (Print)