Criminal Investigations: An Interactive Experience to Improve Student Engagement and Achievement in Cybersecurity Courses

John Grady Hall
jhall170@uncc.edu
University of North Carolina at Charlotte
Charlotte, NC, USA

Abhinav Mohanty
amohant1@uncc.edu
University of North Carolina at Charlotte
Charlotte, NC, USA

Pooja Murarisetty
pmuraris@uncc.edu
University of North Carolina at Charlotte
Charlotte, NC, USA

Ngoc Diep Nguyen
nnguye62@uncc.edu
University of North Carolina at Charlotte
Charlotte, NC, USA

Julio César Bahamón
jbahamon@uncc.edu
University of North Carolina at Charlotte
Charlotte, NC, USA

Harini Ramaprasad
hramapra@uncc.edu
University of North Carolina at Charlotte
Charlotte, NC, USA

Meera Sridhar
msridhar@uncc.edu
University of North Carolina at Charlotte
Charlotte, NC, USA

ABSTRACT

This paper presents *Criminal Investigations*, a gamified, scalable web-based framework for teaching and assessing *Internet-of-Things* (IoT) security skills. Criminal Investigations is packaged as a series of stackable IoT security activities; the current version uses React for the front-end development and Python for the back-end, and is deployed as a web application on a university server. Criminal Investigations promotes student engagement and learning by incorporating gamification concepts such as storytelling, experience points, just-in-time learning content delivery and checkpoints into activity design. This paper presents a pilot deployment of Criminal Investigations' first, fully-deployed, prototype activity "Reverse Engineering and Analyzing IoT Firmware". The results of the pilot deployment indicate that Criminal Investigations provides an engaging, user-friendly, accessible environment, and helps students achieve the learning objectives of the prototype activity.

CCS CONCEPTS

• **Applied computing** → **Education**; **Interactive learning environments**; • **Security and privacy** → *Software reverse engineering*.

KEYWORDS

education, teaching, interactive, achievement, engagement, gamification, security, reverse-engineering

ACM Reference Format:
John Grady Hall, Abhinav Mohanty, Pooja Murarisetty, Ngoc Diep Nguyen, Julio César Bahamón, Harini Ramaprasad, and Meera Sridhar. 2022. Criminal Investigations: An Interactive Experience to Improve Student Engagement and Achievement in Cybersecurity Courses. In *Proceedings of the 53rd ACM Technical Symposium on Computer Science Education V. 1 (SIGCSE 2022), March 3–5, 2022, Providence, RI, USA.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3478431.3499417

SIGCSE 2022, March 3–5, 2022, Providence, RI, USA

ACM ISBN 978-1-4503-9070-5/22/03…$15.00
https://doi.org/10.1145/3478431.3499417

1 INTRODUCTION

As more organizations and governments make digital transformation a priority, the adoption of IoT technology increases. The number of IoT devices grew from 7 billion in 2018 to 31 billion in 2020 [49]. As IoT becomes widely popular, attacks are equally widespread. According to Nokia's threat intelligence report, internet-connected, or IoT, devices now make up roughly 33% of all the infected devices [45]. With the increasing number of attacks related to IoT devices, IoT security education gains importance both for awareness and improving the workforce. There are several gaps to be filled in advanced cybersecurity education in order to strengthen the nation's cybersecurity workforce [57]. For example, there is a severe lack of gender and ethnic diversity in the cybersecurity industry, something that is desperately needed to meet the growing demand and to foster innovation and creativity in problem solving [3, 15, 27, 34]. To address the above, it is important to deliver IoT security educational content in an engaging, inclusive way.

Prior work suggests that *gamification* [21] — the application of game-design elements and game principles in non-game contexts — in classroom activities is likely to increase student engagement and enhance learning [11]. Games in cybersecurity education enhance

engagement, promote active learning and generally aid in delivering educational content, inspiring interest in computer security and motivating participants to explore the field further (cf., [33]). To the best of our knowledge, ours is the first framework that incorporates principles of gamification, universal design and inclusivity to teach and assess advanced IoT software security topics.

In this paper, we introduce *Criminal Investigations*, a gamified, scalable web-based framework to teach and assess *Internet-of-Things* (IoT) security skills. We envision Criminal Investigations as a consolidated package of stackable IoT security activities, each activity teaching students skills critical for the next. Starting with an introduction to basic IoT firmware components through an IoT firmware reverse engineering and analysis activity, Criminal Investigations will span activities related to vulnerability discovery, and simple and advanced firmware attacks. We present Criminal Investigations, with a fully-deployed first prototype activity "Reverse Engineering and Analyzing IoT Firmware".

Criminal Investigations features several game design and development principles, including: (i) a narrative or story, (ii) *knowledge checkpoints* [52], (iii) rewards such as *eXperience Points* (XP) [23, 47], and (iv) challenge [14]. Criminal Investigations includes a *Practice Mode* to allow students to solve ungraded module challenges with simpler inputs / contexts and a *Test* mode that presents more difficult challenges and a graded quiz. Criminal Investigations also reinforces key concepts via *just-in-time* learning content delivery while the student is engaged in the activity. Criminal Investigations uses React [20] for the front-end and Python for the back-end, and is deployed as a web application on a university server.

For the "Reverse Engineering and Analyzing IoT Firmware" activity, we provide the student with an IoT firmware image and a virtual machine image with the required analysis tools pre-installed. The goal is to reverse-engineer the firmware using a tool named `binwalk` [24], and identify information such as the type and version of the firmware kernel, the type and version of the firmware bootloader, compression schemes used, the hardware architecture, etc. Identifying this information is the foundation of firmware security analysis and is used in decompressing firmware data, identifying pre-existing vulnerabilities, and creating *proof-of-concept* exploits to demonstrate the consequences of the vulnerabilities.

We design the "Reverse Engineering and Analyzing IoT Firmware" activity as a narrative featuring a detective and a college professor, addressed to a student from the cybersecurity department (who is completing the activity), regarding an ongoing investigation of compromised IoT devices on campus. As part of the investigation, the campus police has seized the laptop of a suspect in the case. The narrative leads the student through the analysis of the firmware files found on the laptop, which will help identify details about the compromised devices. Before beginning the activity, the student must read related learning content and pass a Knowledge Checkpoint quiz that assesses the student's preparation to attempt the activity. Auditing the learning content and reaching the Knowledge Checkpoint is critical since the information from the readings is required to solve the activity challenges.

We report on student feedback on Criminal Investigations, obtained through a pilot deployment during the Spring 2021 semester.

The main contributions of this paper are: **(1)** the design, development, and deployment of Criminal Investigations, a gamified, scalable web-based framework to teach and assess IoT firmware security skills; **(2)** Criminal Investigations's fully deployed first activity "Reverse Engineering and Analyzing IoT Firmware"; **(3)** results from a pilot deployment that obtains student feedback on the framework, student engagement and learning.

Roadmap: Section 2 presents our pedagogical goals and strategies. Section 3 discusses the high-level design of Criminal Investigations. Section 4 outlines details about the prototype activity. Section 5 discusses framework implementation and deployment. Section 6 presents our pilot study results. Section 7 briefly discusses related work. Section 8 presents conclusions and future work plans.

2 PEDAGOGICAL GOALS AND STRATEGIES

We have three primary educational goals, as outlined below.

G1: Promote student learning and engagement. A teacher is no longer just a source of *information*, but a *facilitator* who helps students develop and hone higher-order cognitive skills [30]. The focus is on engaging students in discussions / activities, helping them think critically and enabling them to be lifelong learners. We aim to incorporate strategies to improve student learning and their engagement with the course material, each other and instructors.

G2: Motivate students to explore advanced topics in cybersecurity. Cyberattacks' threat to national security is real. Currently, there is a national shortage of skilled cybersecurity workforce [27, 57]. We aim to motivate students to be interested in advanced cybersecurity topics such as IoT security and to maintain and grow this interest in the years ahead.

G3: Promote inclusivity, accessibility and broader dissemination. Bringing multiple perspectives through a diverse workforce is key to inspire creativity and innovation in a field like cybersecurity [3] where new types of security vulnerabilities and attacks arise all too frequently. There is an unfortunate lack of diversity in the cybersecurity workforce [15] and the cybersecurity higher-education pipeline. We aim to make advanced cybersecurity topics accessible to a diverse and broad body of students.

Our primary strategy to increase student engagement and learning (**G1**) and to motivate students to explore advanced topics in cybersecurity (**G2**) is to employ an interactive, gamified approach to teach and assess IoT security skills. Gamification has been shown to increase student engagement and motivation [11, 56].

To promote inclusivity, accessibility and broader dissemination (**G3**), we (1) design Criminal Investigations as a web-based application that is available online and easily accessible through any web browser; (2) incorporate diverse examples and avoid stereotypes that are prevalent in the field of cybersecurity within our narrative; (3) adhere to guidelines for universal design in our user interface.

3 DESIGN

The key idea behind the design of Criminal Investigations is to promote student learning and engagement in topics related to IoT security by incorporating elements of gamification [11] into hands-on activities. These activities will be used as part of cybersecurity course materials. They are intended to enhance learning of material featured in the course curriculum.

Criminal Investigations presents an activity in the form of a narrative (Fig. 1) to improve student engagement and incorporates knowledge checkpoints (Fig. 2) to assess student preparedness for the activity. We award eXperience Points (XP) at checkpoints throughout the activity to keep students motivated. We integrate *just-in-time* learning content delivery to reinforce key concepts while students are engaged in the activity. Criminal Investigations also features a *Practice Mode* for activities. Criminal Investigations is deployed as a web-based framework. We also provide students with a virtual machine image, pre-packaged with all software and tools required for a given hands-on activity. Used in conjunction with core learning content, this framework is intended to make difficult concepts more approachable and accessible for students of varying backgrounds and experience levels.

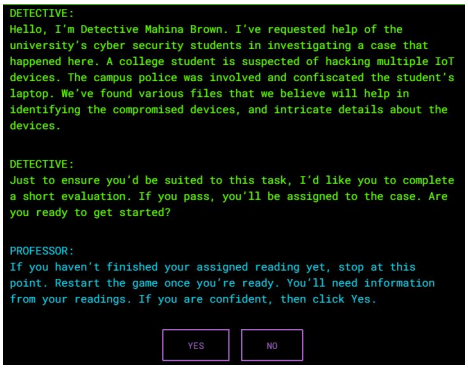

Figure 1: Activity as a narrative

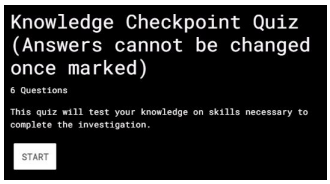

Figure 2: Knowledge Checkpoint in Criminal Investigations

3.1 Activity Gamification

We refer to past works that establish the success of gamification concepts in Computer Science education [11, 56]. The key idea behind gamification is to understand which mechanics keep gamers motivated to come back to play and apply those constructs to non-game environments to encourage similar engagement. Our goals are to increase student engagement in IoT security education, while also making the content accessible to a diverse audience. Based on prior research that establishes *interaction* as an important element in making games and activities engaging, a key focus in our design is interactivity [14, 47]. We achieve this by transforming a traditional assignment into a narrative-based interactive activity that incorporates gamification concepts such as XP and checkpoints.

3.2 Game Modes

As shown in Fig. 3, the framework supports Practice and Test modes.

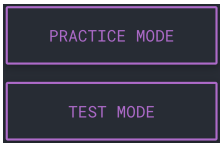

Figure 3: Game modes in Criminal Investigations

Practice Mode: The purpose of the Practice Mode is to give students an opportunity to get accustomed to the activity's environment and practice the skills required to successfully complete the activity, with inputs / configurations chosen specifically for practice mode. Students may use unlimited attempts in the Practice Mode.

Test Mode: Students use the Test Mode to complete an activity as part of a graded assessment within a course. The Test Mode can be configured to limit students to a specific number of attempts (e.g., two attempts) for an activity. Since the Test Mode has a restricted number of attempts, when students begin this mode, they are asked to first complete a *Knowledge Checkpoint* quiz to ensure that they are adequately prepared for the activity. The Knowledge Checkpoint has a minimum XP threshold that must be achieved.

3.3 Just-in-Time learning content delivery

Criminal Investigations is expected to be used in addition to learning content such as lecture videos, readings, tutorials, etc. rather than as a replacement. However, as seen in Fig 4, we incorporate snippets of learning content right into the narrative and activity to reinforce key concepts while students are engaged in the activity.

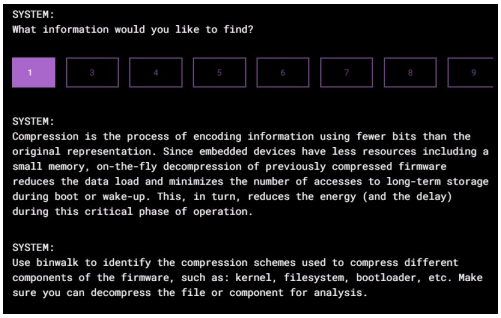

Figure 4: Just-in-Time learning

3.4 Ease of Access

Criminal Investigations is developed as an interactive web-based application using React [20] for the user interface (UI) or front-end, Python Flask [46] library for the backend and MongoDB [41] as the backend database. We provide all the tools and files that are required to complete a given activity as part of a pre-built virtual machine (VM) image. Criminal Investigations is easily accessible from a standard web browser.

4 PROTOTYPE ACTIVITY

In the prototype activity —*Reverse Engineering and Analyzing IoT Firmware*— the student's goal is to reverse engineer an IoT firmware image using `binwalk` [24] and extract and identify various components of the firmware. Students are required to identify firmware

components that include compression schemes used for the filesystem or elsewhere, kernel, bootloader, filesystem, user apps, web apps, and CPU endianness, architecture, and processor type (32-bit/64-bit). Identifying these components is critical for further analyzing the firmware image and diagnosing pre-existing security issues. For example, if the firmware uses an outdated kernel or bootloader containing known vulnerabilities, an attacker can exploit the vulnerabilities to hijack the IoT device. Information such as CPU architecture and endianness assists in constructing *proof-of-concept* exploits since every architecture type has a different set of instructions, opcodes syntax, count, and types of registers. This reverse engineering and analysis activity is foundational background for learning about advanced exploits and defenses for IoT firmware.

In this activity we incorporate the various design features that we introduced in Section 3:

Narrative Style. As seen in Fig 1, the activity begins with an introductory narrative featuring a detective and a college professor, addressed to a student (who is completing the activity), regarding an ongoing investigation of compromised IoT devices on campus. An unknown entity has compromised specific university IoT devices, and as part of the investigation the campus police has seized the laptop of a suspect in the case. The laptop contains firmware files that the police believe are from the compromised IoT devices, and the cybersecurity department has to assist the police department in analyzing the files. Once the introductory dialog ends, the student can choose to proceed or come back later to begin the core activity.

Practice and Test Modes. We provide students with the firmware image and the required analysis tools to complete the activity. Students can access the prototype activity in both *Practice* and *Test Modes*. The Test Mode starts with a Knowledge Checkpoint quiz. Once the student achieves a pre-defined XP threshold in this quiz, they can access the core activity components, where they are required to reverse engineer and analyze the assigned firmware and answer questions based on the analysis to help solve the case.

Reward System. To keep students motivated throughout the activity, Criminal Investigations provides instant feedback in the form of encouraging dialog and XP for correct answers.

Activity Requirements. As seen in Fig. 5, students need to complete nine activity tasks. The tasks are non-sequential and are accompanied by a short summary and security relevance information. To fulfill a requirement, students must perform a particular analysis task, such as finding the compression scheme used to compress the firmware file system and answer an analysis based question.

Virtual Environment. We provide students with a VM image that has `binwalk` and its dependencies pre-installed and accessible from the terminal. For the pilot deployment, the VM was exported using the Open Virtualization Format [17] and the size of the associated Virtual Machine Disk was 3.76 Gigabytes.

5 IMPLEMENTATION AND DEPLOYMENT

Criminal Investigations' implementation and deployment include three major aspects: **(1)** designing and developing the front-end or UI for the framework using React JS (open-source JavaScript library) [20] ; **(2)** designing and developing the back-end using Python's Flask library [46] in combination with MongoDB [41] for the database ; and **(3)** deploying a prototype of Criminal Investigations on a university server.

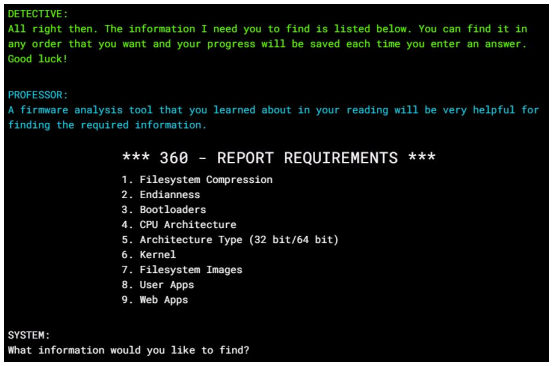

Figure 5: Tasks in prototype activity

5.1 Implementation

Front-end. We use React JS [20], a JavaScript library for building responsive and stateful UI components, for our front-end. React follows a component-based approach to support modularity. We develop components of a web page (e.g., header, navigation bar, etc.) individually and combine them to form different views. We use simple views for each state in the activity, and React efficiently updates only the required components when the data changes.

Quiz component. Criminal Investigations includes a quiz engine (e.g., for Knowledge Checkpoint quizzes, activity quizzes, etc.), built on top of *react-quiz-component* [58], an open-source React component that simulates a simple quiz engine. Quizzes are stored as JavaScript Object Notation (JSON) objects [28].

Database. Since the quizzes and narrative dialogs are stored as JSON objects, we use MongoDB [41] as our datastore due to the ease of storing and retrieving JSON objects from MongoDB.

Back-end. We use the Python Flask library [46] for our back-end. The back-end is responsible for packaging and delivering the UI and for connecting with the MongoDB datastore.

Accessibility. The UI follows universal design and accessibility guidelines to allow users of diverse abilities to navigate and use it. There is a high color contrast ratio between colors for better readability. The layout and typography are compliant with accessibility principles. There is a deliberate delay when rendering dialogs to help students easily follow the story, and a default scroll to bottom so that it is easier for students to view the current task.

Engagement and Motivation. A status bar at the top displays the amount of XP acquired (Fig. 6). To keep students motivated, the XP updates immediately after they complete a quiz / task. Students also receive congratulatory messages to reinforce the gamification principle of rewards.

5.2 Deployment

We have currently deployed Criminal Investigations on a university server that runs Ubuntu 18.04 LTS and is accessible to students. The

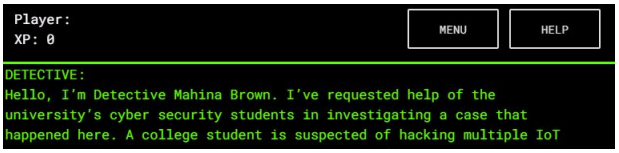

Figure 6: eXperience Points

front- and back-end are deployed as micro-services using Docker containers. We use NGINX, an open-source web server, which besides serving the static files of Criminal Investigations, also listens for HTTP/HTTPS traffic and transfers requests to the back-end. It also redirects traffic from HTTP to HTTPS.

6 PILOT STUDY

We deployed our prototype activity — *Reverse Engineering and Analyzing IoT Firmware* — as part of an extra credit module in one section of an undergraduate / early graduate game design and development class and three sections of an undergraduate operating systems and networking class in Spring 2021. The module included short pre- and post-surveys, learning content, the prototype activity detailed in Section 4, a quiz and a voluntary student feedback survey.

Thirty six students completed at least one task in the activity and the student feedback survey. Of those, twenty three completed all nine tasks. Sixteen questions in our survey used a five-point Likert Scale ranging from "Strongly Disagree" to "Strongly Agree". In our results, we group "Strongly Disagree" / "Disagree" into a "Negative" category, "Neither Agree nor Disagree" into a "Neutral" category, and "Agree" / "Strongly Agree" into a "Positive" category. Five questions asked for free responses. We categorize these responses into "Negative", "Neutral", and "Positive" based on the content of the response. We do this using the Python library *Natural Language Toolkit* (NLTK) with its *Vader* sentiment analyzer [44].

Table 1 shows our Likert Scale questions and their response classification. Table 2 shows our free response questions and response classification for them. We summarize our results (from quantitative and qualitative data) along three main dimensions, namely User Interface and Accessibility, Student Learning and Student Engagement and discuss additional feedback.

User Interface and Accessibility. Most students had positive responses to the User Interface and accessibility aspects of the framework. A few students suggested we speed up animations.

Student learning. Approximately 40 - 75% of the students had positive responses to questions related to the content and concepts. However, a significant number of students had neutral or negative reactions, some of whom reported that some instructions were not clear enough or that more learning content was required.

Student engagement. Over 50% of the students had positive responses to all but one question related to engagement, indicating that they found the activity style, narrative, XP and level of challenge to be engaging / motivating. Several students were neutral while a small number of students had negative reactions.

Additional feedback. Most students were able to complete the module within the expected time of 1 to 2 hours, but a few took longer due to installation issues. We also asked students to provide suggestions for improvement. The majority of the responses focused on aspects of the activity or the UI that could be enhanced, but were not critical to students' ability to complete the activity successfully. These were classified as Neutral or Positive by the NLTK. The negative responses focused on suggestions geared toward improving aspects that were confusing, cumbersome and in general problematic for the completion of the activity.

Discussion. Overall, the feedback we obtained from the pilot deployment is very encouraging and gives us valuable suggestions to improve the Criminal Investigations framework. We have begun to refactor our software framework to use a more flexible MERN (MongoDB, ExpressJS, ReactJS, NodeJS) stack and a more modular design, making it easier to add instructions, learning content, narrative and quiz components to our existing activity and to incorporate new activities. We are also fixing smaller issues that students pointed out with instructions, content and framework and adding support for multiple animation speed choices.

7 RELATED WORK

7.1 Gamification

Gamification is not a new concept in cybersecurity education / training; it has been applied in multiple areas of the field [16, 39, 48, 54]. Numerous works establish the benefits of gamification in making cybersecurity education more engaging and enjoyable (cf., [33]). However, not a lot of work focuses on gamification of activities that teach skills related to IoT firmware. Ashgar et al. discuss an approach to teach reverse engineering in a classroom environment but their focus is on reversing the code for a mobile app [4]. We focus on reverse engineering and analysis of IoT firmware, which is very different from reverse engineering a mobile app.

Gamified activities have been shown to increase student engagement and learning [11]. An example is a set of "wargames" created by the OverTheWire community [13]. Watson et al. [56] found that once students reach a certain level of engagement in a gamified activity, they are likely to continue to optional, ungraded levels.

We utilize game design principles to ensure the delivery of experiences that are meaningful and engaging [47]. A key aspect is the idea of games posing a challenge to the players; for example, the need to overcome an obstacle or manage a key resource to successfully achieve the game's objectives [14]. Furthermore, well-designed games often tell compelling stories and enable the audience to be active participants in an interactive experience [14, 37, 47]. Games typically also include sophisticated rule systems and rewards mechanisms, designed to promote specific activities and discourage or prevent others [29, 47]. We leverage these characteristics of game design to create a framework that enables the delivery of engaging experiences. Players are presented with scenarios built around specific learning objectives, supported by hands-on activities conducted in an interactive environment [37, 38], to emphasize key concepts or essential skills.

7.2 Education

Over the last several years, there has been a large body of research on pedagogical strategies to help students develop higher-order thinking skills [30], to improve student engagement and to support

Question	Negative	Neutral	Positive	*N*
User Interface and accessibility				
The application design is attractive (graphics, interface, layout)	0 (0%)	4 (11.11%)	32 (88.89%)	36
The text font (size & style) and colors are clear and consistent.	2 (5.56%)	1 (2.78%)	33 (91.67%)	36
Student learning				
The learning content was sufficient to help me understand relevant concepts and do the activity smoothly.	12 (33.33%)	7 (19.44%)	17 (47.22%)	36
The content and structure of the activity helped me gain confidence in the concepts.	8 (22.22%)	12 (33.33%)	16 (44.44%)	36
The contents of the activity are relevant to my interests.	7 (19.44%)	6 (16.67%)	23 (63.89%)	36
It is clear to me how the contents of the activity are related to the targeted concepts.	2 (5.56%)	7 (19.44%)	27 (75%)	36
The activity helped me reinforce relevant concepts.	6 (16.67%)	9 (25%)	21 (58.33%)	36
This activity is an adequate teaching method for the included concepts.	10 (27.78%)	9 (25%)	17 (47.22%)	36
Student engagement				
Earning eXperience Points (XP) motivated me to do well in the activity.	6 (16.67%)	11 (30.56%)	19 (52.78%)	36
The story / narrative at the beginning of the activity was interesting and captured my attention.	6 (16.67%)	8 (22.22%)	22 (61.11%)	36
I found the activity to be fun / highly engaging (i.e., it does not become monotonous or boring).	8 (22.22%)	8 (22.22%)	20 (55.56%)	36
Completing the individual tasks of the activity gave me a satisfying feeling of accomplishment.	7 (19.44%)	10 (27.78%)	19 (52.78%)	36
I was so involved in the activity that I lost track of time.	18 (50%)	6 (16.67%)	12 (33.33%)	36
This activity is appropriately challenging for me.	7 (19.44%)	10 (27.78%)	19 (52.78%)	36
I would recommend this activity to others.	10 (27.78%)	8 (22.22%)	18 (50%)	36
I prefer learning with this style of activity to other styles that I have experienced.	6 (16.67%)	10 (27.78%)	21 (55.56%)	36

Table 1: Likert scale questions and responses

Question	Negative	Neutral	Positive	*N*
If you faced issues with the gameplay length or activity setup, please note them below.	7 (36.84%)	11 (57.89%)	1 (5.26%)	19
If you noticed any gameplay issues or bugs, please list them here.	5 (27.78%)	11 (61.11%)	2 (11.11%)	18
Please list two strong aspects of the activity.	0 (0.00%)	5 (17.86%)	23 (82.14%)	28
Please give two suggestions to improve the activity.	5 (17.86%)	8 (28.57%)	15 (53.57%)	28
If you have any additional feedback not covered in the previous questions and sections, please note it here.	2 (28.57%)	3 (42.86%)	2 (28.57%)	7

Table 2: Free response questions and responses

inclusivity. A central idea that helps achieve these goals is active learning [9, 22, 40]. Gamification is one approach to improve student engagement and increase motivation [11, 56]. Manifestations of active learning may be found in team-based learning [32, 35], the Flipped Classroom [6–8, 36], and Process-Oriented Guided Inquiry Learning (POGIL) [1, 2, 25, 26, 31, 42, 43].

7.3 IoT Software Security Education

The closest works to ours in IoT security are two advanced IoT security training courses/workshops that include firmware extraction, emulation and analysis, and building exploits for ARM and MIPS architectures [5, 51]. Another training course/workshop covers broader topics such as secure architecture, infrastructure, policies, mobile and cloud vulnerabilities and briefly touches upon firmware analysis [53]. However, we plan to incorporate activities in Criminal Investigations that teach how to use *Address Sanitizer* [50] and American Fuzzy Lop (AFL) [59] to identify vulnerabilities in IoT firmware and writing advanced exploits for ARM and x86 that can bypass memory protections. Other vendors such as Udemy [55] and EdX [18] explore limited introductory IoT security topics [10, 19], such as identifying and analyzing IoT security and privacy risks, understanding conceptual designs for secure hardware and software, knowledge of security architectures, etc. However, these do not address IoT firmware security and are not gamified.

Chothia introduces a course that focuses on basic end-to-end penetration testing techniques for IoT devices and includes a basic IoT firmware security (simple buffer overflows) module [12]. In contrast, our course will discuss firmware analysis and security in depth, including firmware extraction, reversing, analysis and fuzzing, using tools such as AddressSanitizer to identify memory-corruption vulnerabilities and writing advanced exploits that can bypass memory-level protections.

8 CONCLUSION AND FUTURE WORK

In this work, we present Criminal Investigations, an interactive, gamified framework to teach and assess IoT security skills. Our goal is to provide students with an enjoyable and engaging environment to learn these skills. Criminal Investigations currently features a prototype "Reverse Engineering and Analyzing IoT Firmware" activity. We deployed our framework in three sections of an operating systems and networking course and one section of a game design and development course in the Spring 2021 semester. Student feedback indicates that our framework is engaging and accessible. In future work, we plan to add several enhancements to our framework, including activities with increasing levels of complexity and progression requirements, the ability for students to earn incentives and unlock challenge levels based on earned XP, and increase in randomization and adaptivity of the activities using concepts of Artificial Intelligence.

ACKNOWLEDGMENTS

This research was supported by NSF award NSF-DGE #1947295.

REFERENCES

[1] [n.d.]. Process Oriented Guided Inquiry Learning. https://pogil.org/.
[2] [n.d.]. Process Oriented Guided Inquiry Learning. http://cspogil.org/Home.
[3] [n.d.]. The Need for Diversity in Cybersecurity. https://medium.com/diversity-unscripted/the-need-for-diversity-in-cybersecurity-1ec1c14e1770.
[4] Muhammad Rizwan Asghar and Andrew Luxton-Reilly. 2018. Teaching Cyber Security Using Competitive Software Obfuscation and Reverse Engineering Activities. In *Proceedings of the 49th ACM Technical Symposium on Computer Science Education*. 179–184.
[5] Attify. [n.d.]. Offensive IoT Exploitation. https://www.attify.com/iot-security-exploitation-training. Accessed: 2020-1-13.
[6] Jonathan Bergmann and Aaron Sams. 2012. *Flip your classroom: Reach every student in every class every day*. International society for technology in education.
[7] J. Bergmann and A. Sams. 2014. *Flipped Learning: Gateway to Student Engagement*. International Society for Technology in Education.
[8] Jacob Lowell Bishop and Matthew A Verleger. 2013. The flipped classroom: A survey of the research. In *ASEE National Conference Proceedings, Atlanta, GA*, Vol. 30. 1–18.
[9] Charles C Bonwell and James A Eison. 1991. *Active Learning: Creating Excitement in the Classroom. 1991 ASHE-ERIC Higher Education Reports*. ERIC.
[10] Brian Russel and Sunil Gupta. [n.d.]. Securing IoT: From Security to Practical Pentesting on IoT. https://www.udemy.com/course/securing-iot-from-security-to-practical-pentesting-on-iot/. Accessed: 06-07-2019.
[11] Patrick Buckley and Elaine Doyle. 2016. Gamification and student motivation. *Interactive Learning Environments* 24, 6 (2016), 1162–1175. https://doi.org/10.1080/10494820.2014.964263
[12] Tom Chothia and Joeri de Ruiter. 2016. Learning From Others' Mistakes: Penetration Testing IoT Devices in the Classroom. In *USENIX Workshop on Advances in Security Education (ASE 16)*.
[13] OverTheWire (community). [n.d.]. Wargames. http://overthewire.org/wargames/.
[14] Chris Crawford. 2003. *Chris Crawford on Game Design*. New Riders Publishing, USA.
[15] DataUSA. [n.d.]. INFORMATION SECURITY ANALYSTS. https://datausa.io/profile/soc/151122/#demographics. Accessed on 04-22-2019.
[16] Tamara Denning, Adam Lerner, Adam Shostack, and Tadayoshi Kohno. 2013. Control-Alt-Hack: The Design and Evaluation of a Card Game for Computer Security Awareness and Education. In *Proceedings of the ACM SIGSAC Conference on Computer & Communications Security (CCS)*. 915–928.
[17] Distributed Management Task Force (DMTF). [n.d.]. Open Virtualization Format. https://www.dmtf.org/standards/ovf. Accessed on 01-14-2021.
[18] edx. [n.d.]. Cybersecurity and Privacy in the IoT. https://www.edx.org/course/cybersecurity-and-privacy-in-the-iot. Accessed: 2019-5-7.
[19] edX-Curtin University. [n.d.]. Cybersecurity and Privacy in the IoT. https://www.edx.org/course/cybersecurity-and-privacy-in-the-iot. Accessed: 06-07-2019.
[20] Facebook Inc. [n.d.]. React—A JavaScript library for building user interfaces. https://reactjs.org/. Accessed on 08-26-2020.
[21] Zachary Fitz-Walter. 2020. What is Gamification? https://www.gamify.com/what-is-gamification.
[22] Scott Freeman, Sarah L Eddy, Miles McDonough, Michelle K Smith, Nnadozie Okoroafor, Hannah Jordt, and Mary Pat Wenderoth. 2014. Active learning increases student performance in science, engineering, and mathematics. *Proceedings of the National Academy of Sciences* 111, 23 (2014), 8410–8415.
[23] GiantBomb.com. 2020. Experience Points. https://www.giantbomb.com/experience-points/3015-39/.
[24] Craig Heffner. 2010. Binwalk: Firmware analysis tool. (2010).
[25] Helen H. Hu and Clifton Kussmaul. 2012. Promoting Student-centered Learning with POGIL. In *Proceedings of the 43rd ACM Technical Symposium on Computer Science Education (SIGCSE '12)*. 579–580.
[26] Helen H Hu and Tricia D Shepherd. 2014. Teaching CS 1 with POGIL activities and roles. In *Proceedings of the 45th ACM technical symposium on Computer science education*. ACM, 127–132.
[27] $(ISC)^2$. [n.d.]. *Cybersecurity Professionals Focus on Developing New Skills as Workforce Gap Widens: $(ISC)^2$ CYBERSECURITY WORKFORCE STUDY, 2018*. Technical Report. Accessed on 04-22-2019.
[28] json.org. [n.d.]. Introducing JSON. https://www.json.org/json-en.html. Accessed on 01-14-2021.
[29] Jesper Juul. 2011. *Half-real: Video games between real rules and fictional worlds*. MIT press.
[30] David R. Krathwohl. 2002. A Revision of Bloom's Taxonomy: An Overview. *Theory Into Practice* 41, 4 (2002), 212–218.
[31] Clifton Kussmaul. 2012. Process oriented guided inquiry learning (POGIL) for computer science. In *SIGCSE*.
[32] Celine Latulipe, N. Bruce Long, and Carlos E. Seminario. 2015. Structuring Flipped Classes with Lightweight Teams and Gamification. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education* (Kansas City, Missouri, USA) *(SIGCSE '15)*. ACM, New York, NY, USA, 392–397.
[33] Chengcheng Li and Rucha Kulkarni. 2016. Survey of Cybersecurity Education through Gamification. In *Proceedings of the ASEE Annual Conference & Exposition*.
[34] Peter Loshin. [n.d.]. McAfee CISO explains why diversity in cybersecurity matters. https://searchsecurity.techtarget.com/feature/McAfee-CISO-explains-why-diversity-in-cybersecurity-matters. Accessed on 04-22-2019.
[35] Stephen MacNeil, Celine Latulipe, Bruce Long, and Aman Yadav. 2016. Exploring Lightweight Teams in a Distributed Learning Environment. In *Proceedings of the 47th ACM Technical Symposium on Computing Science Education* (Memphis, Tennessee, USA) *(SIGCSE '16)*. ACM, New York, NY, USA, 193–198.
[36] Mary Lou Maher, Celine Latulipe, Heather Lipford, and Audrey Rorrer. 2015. Flipped Classroom Strategies for CS Education. In *Proceedings of the 46th ACM Technical Symposium on Computer Science Education (SIGCSE '15)*. 218–223.
[37] Michael Mateas and Phoebe Sengers. 1998. Narrative Intelligence. In *The Proceedings of AAAI Fall Symposium*.
[38] M Mateas and A Stern. 2003. Fa{ç}ade: An experiment in building a fully-realized interactive drama. In *The Proceedings of Game Developers Conference, Game Design track*. Citeseer.
[39] Matt Trobbiani. [n.d.]. Hacknet Labyrinths. https://store.steampowered.com/app/521840/Hacknet__Labyrinths/. Accessed on 08-25-2020.
[40] Chet Meyers and Thomas B Jones. 1993. *Promoting Active Learning. Strategies for the College Classroom*. ERIC.
[41] MongoDB, Inc. [n.d.]. MongoDB—The database for modern applications. https://www.mongodb.com/. Accessed on 01-13-2021.
[42] Rick Moog. 2014. *Process oriented guided inquiry learning*. Washington University Libraries.
[43] Richard S Moog, James N Spencer, and Andrei R Straumanis. 2006. Process-oriented guided inquiry learning: POGIL and the POGIL project. *Metropolitan Universities* 17, 4 (2006), 41–52.
[44] NLTK Project. [n.d.]. Natural Language Toolkit. https://www.nltk.org/. Accessed on 08-11-2021.
[45] Nokia. 2020. Nokia Threat Intelligence Report warns of rising cyberattacks on internet-connected devices. https://nokia.ly/3azsLiV.
[46] Pallets. [n.d.]. Flask—web development, one drop at a time. https://flask.palletsprojects.com/en/1.1.x/. Accessed on 08-26-2020.
[47] Katie Salen and Eric Zimmerman. 2003. *Rules of Play: Game Design Fundamentals*. The MIT Press.
[48] Z. Cliffe Schreuders and Emlyn Butterfield. 2016. Gamification for Teaching and Learning Computer Security in Higher Education. In *Proceedings of the USENIX Workshop on Advances in Security Education (ASE 16)*.
[49] Security Today. 2020. The IoT Rundown For 2020: Stats, Risks, and Solutions. https://securitytoday.com/Articles/2020/01/13/The-IoT-Rundown-for-2020.aspx?Page=2.
[50] Konstantin Serebryany, Derek Bruening, Alexander Potapenko, and Dmitriy Vyukov. 2012. AddressSanitizer: A Fast Address Sanity Checker.. In *Proceedings of the USENIX Annual Technical Conference*. 309–318.
[51] Tactical Network Solutions. [n.d.]. IoT Firmware Exploitation. https://www.tacnetsol.com/store/aRyibNKX. Accessed: 2020-1-13.
[52] TeachThought Staff. 2020. 12 Examples Of Gamification In The Classroom. https://www.teachthought.com/the-future-of-learning/12-examples-of-gamification-in-the-classroom/.
[53] Tonex. [n.d.]. IoT Security Training. https://www.tonex.com/training-courses/iot-security-training-iot-security-awareness/. Accessed: 2020-1-13.
[54] Trend Micro: The fugle company. [n.d.]. Targeted Attack: The Game. http://targetedattacks.trendmicro.com/. Accessed on 08-25-2020.
[55] Udemy. [n.d.]. Fundamentals of IoT Security. https://www.udemy.com/fundamentals-of-iot-security. Accessed: 2019-5-7.
[56] Stacey Watson and Heather Richter Lipford. 2019. Motivating Students Beyond Course Requirements with a Serious Game. In *Proceedings of the 50th ACM Technical Symposium on Computer Science Education, SIGCSE*. Association for Computing Machinery, 211–217.
[57] William Crumpler. 2019. The Cybersecurity Workforce Gap. https://bit.ly/2IZ5snw.
[58] wingkwong on Github. [n.d.]. react-quiz-component. https://github.com/wingkwong/react-quiz-component. Accessed on 08-26-2020.
[59] Michal Zalewski. 2010. American Fuzzy Lop: a security-oriented fuzzer. (2010).