Engineering Educators Bringing the World Together
2025 ASEE Annual Conference & Exposition
Palais des congrès de Montréal, Montréal, QC • June 22–25, 2025 ASEE
Paper ID #48134

Extra Credit, Extra Security: Lessons Learned from a Bonus-Based IoT Security Class

Derin Cayir, Florida International University

Derin Cayir is pursuing her Ph.D. at Florida International University, Miami, FL USA, where she is currently a graduate research assistant in the Cyber-Physical Systems Security Lab. Her research interests include privacy/security systems for extended reality devices. Cayir received her bachelor's degree in electrical electronics engineering from Bilkent University, Ankara, Turkey. She also worked as a Machine Learning Researcher in Meta, Redmond WA.

Dr. Mark Allen Weiss, Florida International University

Mark Allen Weiss is Distinguished University Professor, Associate Dean for Undergraduate Education in the College of Engineering and Computing, and Associate Director in the School of Computing and Information Sciences at Florida International University

Prof. Selcuk Uluagac, Florida International University

Prof. Selcuk Uluagac is currently a Program Director at US NSF CISE/CNS as a rotator from his home institution Florida International University, where he is an Eminent Scholar Chaired Professor in the School of Computing and Information Science, leading the Cyber-Physical Systems Security Lab. Before, he was a Senior Researcher at Georgia Tech and Symantec. He holds a PhD from Georgia Tech and MS from Carnegie Mellon University. He received US National Science Foundation CAREER Award, US Air Force Office of Sponsored Research's Summer Faculty Fellowship, and Google's ASPIRE Research award in security and privacy, inter alia. He is an expert in the areas of cybersecurity and privacy. He has hundreds of publications in the most reputable venues as well as numerous patents. His research has been funded by numerous government agencies and industry. He has chaired/served on the of top-tier security conferences, e.g., NDSS, USENIX, ACM CCS, IEEE SP, and serving as the deputy editor in-chief of IEEE TIFS and associate editor of Elsevier COMNET journals. More information can be obtained from http://nweb.eng.fiu.edu/selcuk/.

Extra Credit, Extra Security: Lessons Learned from a Bonus-Based IoT Security Class

Abstract

The Internet of Things (IoT) devices and technologies are increasingly integral to the global market, enabling enhanced interaction and control over the physical world through networks of smart devices in homes, offices, and urban environments. However, pervasive security design flaws within these systems have become prime targets for hackers, increasing the risk of security breaches. This highlights the critical need for specialized education programs that prepare STEM students with the skills and knowledge to tackle these security challenges. This paper introduces a security class on IoT which is designed and taught at Florida International University, Miami, Florida, USA with the goal to address this gap by integrating hands-on projects that enable both graduate and undergraduate students to help them practice security concepts on real devices in tangible manners. This approach effectively helps bridge theoretical knowledge with practical applications. By implementing a bonus-based teaching approach, we aim to enhance learning outcomes. We also evaluate the course's effectiveness through student surveys conducted over four years, which indicate significant improvements in student expertise and satisfaction with the course content and bonus activities. We share our lessons and experiences from the course.

1 Introduction

The Internet of Things (IoT) has become increasingly integral in shaping a technology-driven lifestyle for consumers worldwide. IoT systems, characterized by interconnected sensors and devices[1,2], collect and transmit data through cloud servers to the Internet. This proliferation of smart network appliances and smart city environments, such as intelligent homes and vehicles, has been accompanied by a significant rise in cybersecurity vulnerabilities, often exploited at a rate that outpaces the development of effective countermeasures. Given the increasing frequency and severity of these security incidents, there is an urgent need for educational programs that prepare STEM students to learn how to tackle these challenges through specialized IoT security courses[3].

This paper outlines the design and implementation of a hands-on IoT security class which is offered in Florida International University that educates students about the fundamental concepts of IoT and the most common security threats. By exploring various attack vectors, the course aims to prepare students to develop generalized security solutions for these technologies.

The course structure is innovatively designed to include a combination of immersive homework

assignments, laboratory exercises, and a student project. Using a bonus-based grading system, the course aims to motivate students and enhance learning outcomes, as evidenced by improved academic performance throughout the course. The availability of various IoT devices in our laboratory, Cyber-Physical Systems Security Lab (CSL), provides a practical, hands-on learning experience for students, enabling them to create security applications in real-world scenarios.

By fostering a comprehensive understanding of IoT security challenges and solutions, this course serves as a critical component of STEM education, preparing students to contribute effectively to safeguarding modern digital ecosystems. Our experiences and course outcomes highlight the importance of adaptive and responsive education models that align with evolving technological landscapes and security requirements.

Contribtuions: Our contributions of the paper are as follows:

- We introduce a bonus-based grading system to enhance student engagement and performance, fostering a dynamic learning environment.
- Our course design integrates hands-on projects with laboratory exercises, enabling the practical application of theoretical knowledge in real-world scenarios.
- We provide a detailed and extensive curriculum that covers a broad spectrum of IoT security topics, ensuring a comprehensive understanding essential to tackle various security challenges.
- We measure the course's impact on student learning outcomes through student surveys and demonstrate our results.

Organization: Section 2 gives the related work and compares our work with the existing work. Section 3 presents our approach including the structure and design of class modules, homework assignments, laboratory exercises, final student projects, and bonus-based teaching method. Section 4 discusses the results of student surveys and presents our lessons learned and experience from the course. Finally, Section 5 concludes the paper.

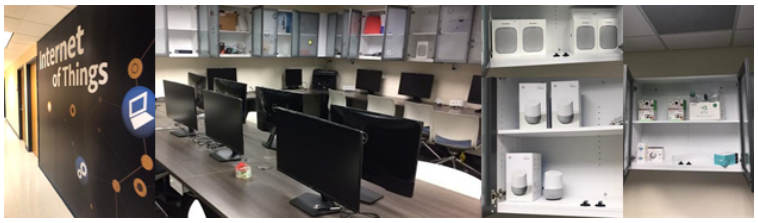

Figure 1: The IoT Security Laboratory where the labs are conducted.

2 Related Work

IoT redefines how people perform their everyday tasks with its rich integration of various functionalities[4,5]. IoT devices can be seen in various domains, from entertainment enhancement such as gaming, security of homes and properties to hospitality and healthcare[6,7,8,9]. These technologies has emerged as a key theme in combining theoretical aspects of computer science with real-world applications, integrating seamlessly into diverse educational environments[10,11]. As IoT systems grow in complexity and ubiquity, understanding their security vulnerabilities becomes crucial, especially given projections of cyberattack costs that reach $10. 5 trillion by 2025[12,13]. It is vital that educational programs prepare future engineers and developers with robust knowledge of these threats[14,15,16].

Several studies illustrate the integration of IoT into educational settings. Xia et al. describe an IoT architecture that facilitates the integration of objects from the real world into virtual academic communities (VAC), adapting existing architectural frameworks to educational needs[17]. Another study highlights the success of incorporating IoT into a humanities curriculum, significantly boosting student interest and understanding of IoT[18]. Furthermore, a workshop focusing on smart home security for the general public demonstrated the practical application of IoT security knowledge, significantly improving the awareness of participants and their ability to manage security risks in their homes[19]. The importance of hands-on laboratory exercises is emphasized in studies like Trabelsi's, which reported positive feedback on the effectiveness of practical labs in teaching IoT security within smart home contexts[20]. Another study introduces an example course focused on smart home security and privacy to illustrate how IoT education can be enhanced[21]. A recent study by Oliveira et al. highlights a "Capture the Flag" competition designed for IoT cybersecurity education, which demonstrated effective hands-on learning and engagement in cybersecurity practices for IoT systems[22]. The introduction of comprehensive lab kits and practical exercises has been met with enthusiasm, significantly enhancing hands-on learning and student engagement with real-world security challenges[23].

Differences from existing work: IoT devices are increasingly being integrated to our daily lives, making the need to secure them against threats and to protect user privacy more critical than ever[24,25,26,27]. It is especially crucial to introduce students to how vital it is to secure IoT technologies and how these technologies can be vulnerable. IoT cybersecurity classes are essential to improve the students' understanding of our technologies and how they should be secured. Despite these useful advancements, the availability of dedicated IoT courses remains limited, creating a knowledge gap among new graduates[28]. With this study, we expand the current

literature by detailing a structured IoT security course that incorporates bonus-based teaching - a novel approach in this field. This method has been shown to improve student engagement and performance, providing a more equitable learning environment. Furthermore, this work is distinctive in its longitudinal assessment spanning five years across seven academic semesters: Fall 2016, Fall 2017, Spring 2018, Fall 2018, Spring 2019, Spring 2021, and Fall 2021. This timeline offers valuable insight into the sustained impact of integrating project-based learning with IoT devices in an educational setting.

3 Approach

This section outlines the structure and design of our IoT security course, including class modules, homework assignments, laboratory exercises, and the final student projects. We also discuss the rationale behind the course design and the implementation of a bonus-based teaching system.

3.1 Class Design Overview

This course is offered to undergraduate and graduate students at Florida International University and is a key component of a bachelor's degree focusing on IoT. The syllabus was crafted with the consideration of current threats in IoT systems and evolving security measures. The course design was also guided by several goals aimed at deepening students' understanding of IoT security, from fundamental concepts to complex security solutions for state-of-the-art IoT devices. The class objectives aim to equip students with the following:

- A thorough understanding of basic and advanced security mechanisms in the IoT.
- Insights into software and hardware architectures of various IoT platforms.
- Competence in designing energy-efficient and secure IoT systems.
- Practical skills in programming and securing state-of-the-art IoT devices.

The content being taught in the class is divided into a total of 12 modules comprising topics ranging from security and confidentiality in IoT, to intrusion detection systems in IoT devices and digital forensic concepts in IoT devices. During each module, students are assigned and expected to complete a number of homework assignments related to the subject matter covered in that module. In addition to the assigned homework, through a set of curated laboratory exercises, students are given practical experience working in real-time with IoT devices, including microcontrollers and sensors. A final project is assigned to the students, where students are to devise their own idea relating to the content taught in the course, and implement that idea using the numerous IoT resources accessible to them throughout the duration of the course. Students are periodically tested on the knowledge gained and the material they have been taught throughout the course. This is administered in the form of two graded tests, a midterm test and a final test. The midterm evaluates students on the content taught in modules 1-6, while the final examination tests students in a cumulative fashion on the contents of all modules 1-12.

3.2 Overview of Class Modules and Content

In this subsection, the 12 class modules that make up the content taught in the class are described. Each module description includes the numerous subtopics that students are exposed to during its duration.

Module 1 - Introduction to IoT: Overview of IoT definitions, infrastructures and protocols.

Module 2 - IoT devices: Exploration of diverse IoT devices and their capabilities.

Module 3 - Security and confidentiality: Focus on confidentiality issues within IoT ecosystems.

Module 4 - Integrity in IoT: Discussion on data integrity and hashing mechanisms in IoT.

Module 5 - Authentication in IoT: Examine various IoT authentication strategies.

Module 6 - Access control and remote authentication: Analysis of remote authentication methodologies and access control mechanisms.

Module 7 - Key management in IoT: Critical key management strategies for secure IoT operations.

Module 8 - Preserving privacy: Application of encryption techniques, including homomorphic encryption within IoT devices.

Module 9 - Malicious software: Identification and mitigation of malware in IoT systems.

Module 10 - Intrusion detection in IoT: Strategies to detect and prevent intrusions in IoT devices.

Module 11 - Digital forensics: Forensic techniques applicable to IoT contexts.

Module 12 - Physical layer threats: Understanding and mitigating physical layer vulnerabilities in IoT devices.

3.3 Homework Assignments and Laboratory Exercises

Homework Assignments: Homework assignments are designed to bridge theoretical concepts with practical application, enabling students to engage deeply in contemporary research and cultivate skills crucial for academic and professional success in IoT security. The assignments are research-oriented, effectively merging coursework with scholarly inquiry to create an enriched learning environment[?] . Through these assignments, students gain practical experience in writing research papers and developing original ideas, which significantly enhances their academic writing skills.

Laboratory Exercises: A pivotal component of our course involves regular laboratory exercises that not only improve hands-on skills but also integrate theoretical concepts thought during the class with practical device applications. We have designed a series of exercises that provide students with hands-on experience with various IoT devices and technologies.

A brief description of each exercise follows:

Lab 1: In this initial laboratory, students establish an I2C connection between a Raspberry Pi 3 and a BME280 sensor, following a detailed wiring scheme provided by the instructor. Utilizing a basic sensor application, they read and print the sampled data, which are then transferred to a micro-web-service. This lab offers insights into secure communications, micro-web services, and JSON data formats, laying a foundational understanding of IoT system interactions.

Lab 2: Continuing from Labor 1, students investigate more deeply IoT applications by enhancing a secure smart home thermostat system. They configured an Android application to display sensor data on an emulated device screen in near-real time. Students manage a MongoDB database and a web service on an Ubuntu virtual machine to handle sensor data, building on their previous experience while introducing them to virtual machine usage and Android app integration.

Lab 3: This lab extends the use of sensor applications to include data transmission through ZigBee devices (XBee), utilizing a ZigBee USB explorer connected to the Raspberry Pi 3. Students analyze plaintext packet communications using Wireshark and employ the RZUSBstick with the Killerbee Framework to capture and decrypt encrypted traffic within a Samsung SmartThings ZigBee network. This scenario provides a practical exploration of wireless security vulnerabilities and data interception techniques.

Lab 4: In the final lab of the semester, students conduct static and dynamic analyzes of IoT enabled Android applications. The goal is to introduce students other real-world applications with which IoT technologies would interact. The students examine the source code of popular apps like ”Facebook” and ”Clash of Clans” to extract static features. Dynamic features are analyzed using Android Studio, which allows students to install and test a preconfigured Android application on their choice of mobile device. This exercise is crucial to understanding the security characteristics of mobile applications, distinguishing between benign and potentially malicious software.

3.4 Final Projects

In this subsection, we discuss various aspects of the final student projects such as the rationale for project assignments, the process of forming student groups, and potential project ideas.

Motivation Behind Final Projects: Project-based learning is crucial in engineering education, recognized for improving problem-solving skills and fostering teamwork[29,30]. To ensure a deep understanding of IoT security, it is crucial that students not only master the fundamental principles, but also develop proactive defense strategies against potential security threats[31].

Selection of IoT Devices: Students are required to select an IoT device for their projects from the devices available in our lab. The IoT devices available to students throughout the course are detailed in Table 1. The devices are chosen for their user-friendliness to ensure that students can manage and utilize them effectively across different project settings. The selection includes a broad spectrum of equipment to encourage hands-on experience with different types of technology, which is crucial to understanding and mitigating potential security risks. The assortment of devices provided includes the following:

- **Smart wearables/devices:** 8 different models that students can use to explore the security of wearable technology.

Table 1: List of Devices Available to Students

Device	Device Type
Sony Smart Watch-3	Smart Wearable/Device
Samsung Gear Live	Smart Wearable/Device
LG G Watch R	Smart Wearable/Device
Moto 360	Smart Wearable/Device
Asus Zen Watch	Smart Wearable/Device
Vuzix Smart Glass	Smart Wearable/Device
Google Nest Smart Thermostat	Smart Wearable/Device
Google Home	Smart Wearable/Device
Raspberry Pi 3 Model B	Development Board
Intel Galileo 2 Board	Development Board
Atmel AVR RZUSBstick	Transceiver/RF Module
XBee	Transceiver/RF Module
Microsoft Kinect	Sensor and Controller
Leap Motion Controller	Sensor and Controller
BME280	Sensor and Controller

- **Development boards:** 2 types, which offer students the opportunity to work with raw computing hardware.
- **Transceivers/RF modules:** 2 kinds, allowing experiments with wireless communications and signal security.
- **Sensors and controllers:** 3 varieties, allowing students to engage with fundamental sensor technology and control systems.

Engaging directly with these devices enables students to apply security techniques in real-time and understand the practical challenges of securing IoT environments.

Team-Based Pairing Based on Questionnaire Responses: In this course, the final project involves students working in teams. To optimize team dynamics, students are paired based on a preliminary questionnaire that assesses their programming skills. This ensures that teams are balanced and conducive to a collaborative learning environment. The details of the questionnaire are documented in Table 2.

Helping Students with Potential Project Ideas: We provided students with a variety of sample topics to inspire their projects, catering to varying levels of expertise and familiarity with IoT. These topics are intended as starting points to guide the students' project directions. Students are encouraged to explore and brainstorm their ideas, and they must obtain instructor approval to pursue their chosen topics. The development of these topics was guided by extensive research on current security trends and empirical needs to expose students to real world scenarios. Below are several sample topics focusing on different aspects of IoT security:

Table 2: Programming Experience Questionnaire

No.	Question
Q1	What is your experience with Java programming?
Q2	What is your experience with Android programming?
Q3	Experience with open source systems/tools/programs? (e.g., Linux)
Q4	Experience with scripting languages? (e.g., Python, Ruby, BASH)
Q5	Can you build an Android or iOS app?
Q6	Run open source programs from the CLI? (e.g., Linux)
Q7	Can you install a Linux OS from a distribution?
Q8	Configure open source tools? (e.g., firewall, IP Tables)
Q9	Install/use programs based on apropos and man pages? (e.g., Linux)
Q10	Modify and change OS system modules in Linux?
Q11	Can you modify the OS kernel in Linux systems?
Q12	Any other notes/comments/concerns? (e.g., group preferences)

1. *Asymmetric encryption implementation and performance evaluation:* Explore the ElGamal encryption algorithm, an alternative to RSA, which is based on the difficulty of computing discrete logs in a large prime modulus. Students will implement and evaluate the ElGamal encryption algorithm, focusing on encryption speed and overhead.
2. *Symmetric encryption implementation and performance evaluation:* Investigate the RC4 encryption algorithm, renowned for its speed of up to ten times faster than AES and its prevalence in commercial products. Students are tasked with implementing RC4 and analyzing its performance compared to other encryption algorithms such as homomorphic and asymmetric systems.
3. *Design of an anomaly-based intrusion detection system:* Design an intrusion detection system that identifies suspicious activity by differentiating normal from anomalous device behavior. This project will involve the use of an IoT device from Table 1 to develop and implement the detection mechanism.
4. *Design of an IoT honeypot:* Create a honeypot system designed to attract and deceive hackers to study malicious activities. This project will provide insight into attack methodologies and help students understand the necessary security measures to prevent breaches.
5. *Analysis of unintended data leakage:* Examine the consequences of data breaches from compromised IoT devices. Students will select a device from Table 1 and simulate data leakage to an external server, analyzing the impact on device functionality and security.

3.5 Bonus-Based Teaching System

This course also incorporates a bonus-based teaching method to enhance student engagement and performance in STEM, aligning with national educational policies that have emphasized such strategies since the 1980s[32]. Traditional student evaluations typically involve grading based on

performance; however, introducing bonus tasks offers an innovative way to further motivate students and improve academic results[33].

In this IoT security course, bonus questions are integrated into both homework assignments and examinations to provide students with opportunities to earn additional points. This method serves dual purposes: enhancing understanding of course material and offering a means to improve participation and provide flexibility, particularly for those who may not perform well on standard questions due to their other life expectations such as work, etc.

Homework Assignments Each of the homework assignments that come with the labs contain bonus questions. If students answer all regular and bonus questions correctly, the bonus points are carried over to the final exam. If a student fails to achieve 100 percent on the regular questions but answers the bonus questions correctly, these bonus points can compensate for the shortfall. Consequently, students have the potential to achieve full credit regardless of their initial scores on regular questions. Any excess points gained from bonus questions on assignments in which the student has already scored full marks are added to their final examination score.

Midterm Examination The midterm examination follows a similar structure, where bonus questions can significantly impact the positive attitude of the students and encourage them to have a great learning opportunity. During several semesters, this approach has demonstrably improved student performance, with detailed evidence and analysis provided in Section 4.

Course Grading The grading system incorporates bonus-based questions to also foster a friendly competitive environment within the course. The detailed final course classification system and the scale can be reviewed in Tables 3 and 4. As seen in Table 3, the class is designed with one mid-term, one final project and several lab-based assignments, focusing more on hands-on components.

Table 3: Course Grading Weights

Component	Weightage
Homeworks with Labs	30%
Midterm Exam	30%
Final Research Project	40%

Table 4: Grading Scale for the Final Course Grade

Grade	Range	Grade	Range	Grade	Range	Grade	Range	Grade	Range
A	95-100	B+	86-89	C+	76-79	D+	66-69	F	0-59
A-	90-94	B	83-85	C	73-75	D	63-65		
		B-	80-82	C-	70-72	D-	60-62		

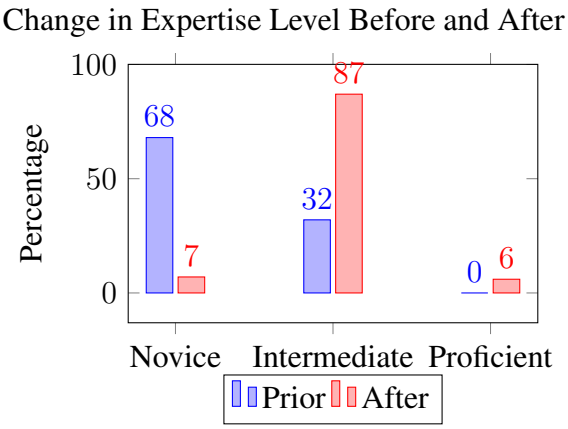

Figure 2: Comparison of student expertise level in IoT before and after the course.

4 Results and Lessons Learned

In this section, we present a preliminary evaluation of the IoT security course, focusing on its impact on student performance and expertise in IoT and network security domains.

To assess the impact, we surveyed both undergraduate and graduate level students who took the course to gauge their perceived level of IoT expertise before and after the course. Over five years when the class was taught, 75 students participated in this survey, which was meticulously designed to align with the objectives of the course. The questions, using a Likert scale from 1 (Strongly disagree) to 5 (Strongly agree), optional choices, and open questions, are detailed in Table 5.

Table 5: Survey Questions for IoT/CPS Security Course Evaluation

No.	Question
Q1	Before this class, my experience with the IoT and CPS devices was:
Q2	The class increased my interest in the IoT/CPS security field.
Q3	I was able to understand the basics of IoT/CPS devices.
Q4	I was able to understand the security concepts of IoT/CPS devices and applications.
Q5	Bonus-based teaching helped me do better in the class.
Q6	The homeworks in the class were instrumental.
Q7	Which optional Lab did you like the most?
Q8	What is your level of experience with IoT and CPS devices after this course?
Q9	Any additional comments?

Feedback collected over this period has been overwhelmingly positive. Students have expressed high levels of satisfaction with both the course content and the instructional approach. In particular, the implementation of a bonus-based teaching strategy was shown to be highly effective, significantly improving student performance across all metrics evaluated. We detail the comprehensive results obtained from our survey below:

Improvement in Perceived Expertise in IoT: As shown in Figure 2, the course significantly

advanced the students' understanding of IoT. Initially, 68% of the students identified as novices, which decreased to 7% after the course, while those who considered themselves competent or advanced increased to 87%. This marks a profound improvement in expertise, confirming the effectiveness of the course in deepening knowledge in this fast-evolving field.

Increase in Interest in IoT/CPS Security: The survey assessed how the course influenced students' interest in IoT and Cyber-Physical Systems (CPS) security. The data reveal a strong agreement on an increase in interest for the majority of students, with 48 participants reporting a significant enhancement in their interest levels. This substantial increase in interest highlights the effectiveness of the course in not only teaching technical skills but also in inspiring students to delve deeper into the security aspects of IoT and CPS.

Understanding Security Concepts: Students were also queried about their understanding of security concepts after completing the course. Most of the students (53) achieved an excellent understanding of security concepts, evidencing the course's success in conveying complex security topics effectively. The high ratings reflect that the educational strategies employed, possibly including bonus-based teaching and various lab activities, were successful in improving students' understanding of crucial security principles.

Bonus-Based Teaching Effectiveness: The effectiveness of the bonus-based teaching method in an IoT security course was evaluated based on student feedback. The results indicate a significant lean toward high effectiveness, with a majority of (47 out of 75 students) rating the bonus-based approach as highly effective. This suggests that the bonus-based elements of the course substantially improved student engagement and learning outcomes, corroborating the utility of integrating such motivational strategies in academic courses, particularly in fields requiring high levels of technical proficiency such as IoT security.

Labratory Exercises: Students were also surveyed about their preferences regarding various laboratory sessions offered throughout the course. Feedback highlighted diverse interests and experiences, demonstrating that each lab incorporated a different topic that aligned with various students' interests. However, it was seen that 8 out of 75 students did not participate in the optional labs, suggesting a potential need to encourage broader engagement or reassessing the optional components of the course to make them more appealing.

Valuable Hands-on Experience: The access to high-quality equipment and hands-on activities was highly appreciated, with one respondent highlighting, *"The availability of the items at the laboratory - very expensive items - was an amazing experience."* This sentiment was echoed by many, who found that the practical experience greatly enhanced their confidence and competence. Another student shared, *"The labs were also very fun to do as they gave us a way to learn more hands-on."*

Suggestions for Improvement: A few of the students also offered constructive suggestions about requests for more demonstrative sessions and workshops. One student noting, *"One suggestion would be to have a demo or workshop period to teach us about the CPS or IoT device we will be using for the homework assignments."* Additionally, the desire for more interactive and investigative labs was expressed, with another student proposing, *"A lab in which we can execute*

an attack on a device and then protect the device from that attack would be something a lot of students who want to advance in security will find enjoyable." We considered these valuable suggestions from the students and are planning to address some of the suggestions in the future teaching of the IoT Security class. Regarding the recommendation to include offensive security techniques, we intend to consult with the university's general counsel to ensure compliance with institutional guidelines and ethical standards.

Educational Content and Learning Opportunities The course's structured learning materials and assignments were deemed extremely helpful. The students praised the clarity and relevance of the shared slides and the variety of topics covered. *"There were some very helpful points in the shared slides such as the IoT platforms related to different companies and different examples of cyber attacks,"* mentioned one of the students.

Enhanced Interest and Career Aspirations Students expressed that the course significantly broadened their interest in IoT and even influenced their career paths. One student noted, *"The guest lecture series you put together was extremely informative and increased my interest in pursuing an IoT-related profession rather than just software engineering."* This reflects the course's success in not only delivering content but also inspiring students to explore specialized fields within technology.

Concluding Remarks: Overall, the results from our comprehensive evaluation indicate that the IoT security course has successfully met its educational objectives. It has not only enhanced students' technical expertise and interest in IoT security but has also fostered a robust understanding of essential security principles. Future iterations of the course will look to build on these successes while finding ways to increase participation in optional labs and maintain high levels of student motivation and engagement.

5 Conclusion

This paper presented the design and implementation of a hands-on IoT security course which was designed and taught at Florida International University, Miami, Florida, USA. The course was tailored for STEM students with the goal of addressing the critical need for educational programs in the face of growing cybersecurity challenges. Our study demonstrated the efficacy of a bonus-based teaching approach in enhancing IoT security education. This method significantly boosted student engagement and comprehension, effectively bridging the gap between theoretical knowledge and practical application. Our approach combined theoretical knowledge with practical application through extensive hands-on laboratory exercises and projects. Feedback from student surveys highlighted the increased motivation and improved performance resulting from this approach, affirming its value in preparing students to understand real-world security challenges in an ever-evolving technological landscape. Additionally, the course's success underscored the importance of adaptive educational models that respond to technological advancements and security demands. Future teachings/iterations of the course will continue to refine this model, ensuring it remains responsive to new developments in IoT security and educational methodologies.

6 Acknowledgements

We thank the anonymous reviewers for their helpful feedback and time. This work has been partially supported by the US National Science Foundation's (NSF) Intergovernmental Personnel Act Independent Research & Development Program, NSF grant CNS-2219920, Florida International University Graduate School, Microsoft, and US Dept. of Education's STEM Strategies for Maximizing Achievement, Retention and Transfer Grant program. The views expressed are those of the authors only, not of the funding agencies.

References

[1] Amit Kumar Sikder, Hidayet Aksu, and A. Selcuk Uluagac. 6thsense: A context-aware sensor-based attack detector for smart devices. In *USENIX Security 17*.

[2] Z. Berkay Celik, Leonardo Babun, Amit Kumar Sikder, Hidayet Aksu, Gang Tan, Patrick McDaniel, and A. Selcuk Uluagac. Sensitive information tracking in commodity iot. In *USENIX Security 18)*, August 2018.

[3] Nurul Amirah Abdul Rahman, Izzah Hanis Sairi, Nurul Akma M Zizi, and Fariza Khalid. The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, 10(5): 378–382, 2020.

[4] Leonardo Babun, Kyle Denney, Z Berkay Celik, Patrick McDaniel, and A Selcuk Uluagac. A survey on iot platforms: Communication, security, and privacy perspectives. *Computer Networks*, 192:108040, 2021.

[5] Amit Kumar Sikder, Giuseppe Petracca, Hidayet Aksu, Trent Jaeger, and A Selcuk Uluagac. A survey on sensor-based threats and attacks to smart devices and applications. *IEEE Communications Surveys & Tutorials*, 23(2):1125–1159, 2021.

[6] Suat Mercan, Lisa Cain, Kemal Akkaya, Mumin Cebe, Selcuk Uluagac, Miguel Alonso, and Cihan Cobanoglu. Improving the service industry with hyper-connectivity: Iot in hospitality. *International Journal of Contemporary Hospitality Management*, 33(1):243–262, 2021.

[7] Ege Tekiner, Abbas Acar, and A Selcuk Uluagac. A lightweight iot cryptojacking detection mechanism in heterogeneous smart home networks. In *NDSS*, 2022.

[8] Leonardo Babun, Amit Kumar Sikder, Abbas Acar, and A Selcuk Uluagac. The truth shall set thee free: Enabling practical forensic capabilities in smart environments. In *NDSS*, 2022.

[9] Derin Cayir, Reham Mohamed, Riccardo Lazzeretti, Marco Angelini, Abbas Acar, Mauro Conti, Z Berkay Celik, and Selcuk Uluagac. Speak up, i'm listening: Extracting speech from zero-permission vr sensors. In *NDSS*, 2025.

[10] H. Maenpaa, S. Varjonen, A. Hellas, S. Tarkoma, and T. Mannisto. Assessing iot projects in university education - a framework for problem-based learning. In *2017 IEEE/ACM 39th International Conference on Software Engineering: Software Engineering Education and Training Track (ICSE-SEET)*, pages 37–46, May 2017. doi: 10.1109/ICSE-SEET.2017.6.

[11] Derin Cayir, Abbas Acar, Riccardo Lazzeretti, Marco Angelini, Mauro Conti, and Selcuk Uluagac. Augmenting security and privacy in the virtual realm: An analysis of extended reality devices. *IEEE Security & Privacy*, 2023.

[12] Cobalt. Cybersecurity statistics 2024. Cobalt Blog, 2024. URL https://www.cobalt.io/blog/cybersecurity-statistics-2024.

[13] Harun Oz, Güliz Seray Tuncay, Ahmet Aris, Amin Kharraz, and Selcuk Uluagac. Beyond the upload button: A 10-year retrospective on security issues within file upload. *IEEE Communications Magazine*, 63(2):104–110, 2025.

[14] Florent Bruguier, Pascal Benoit, Lionel Torres, and Lilian Bossuet. Hardware security: From concept to application. In *Microelectronics Education (EWME), 2016 11th European Workshop on*, pages 1–6. IEEE, 2016.

[15] Razvan Beuran, Jidong Wang, Min Zhao, and Yasuo Tan. Iot security training for system developers: Methodology and tools. *Internet of Things*, 24:100931, 2023.

[16] Fernando Brito, Yassine Mekdad, Monique Ross, Mark A Finlayson, and Selcuk Uluagac. Enhancing cybersecurity education with artificial intelligence content. In *Proceedings of the 56th ACM Technical Symposium on Computer Science Education V. 1*, pages 158–164, 2025.

[17] Feng Xia, Laurence T Yang, Lizhe Wang, and Alexey Vinel. Internet of things. *International Journal of Communication Systems*, 25(9):1101, 2012.

[18] K. Akiyama, M. Ishihara, N. Ohe, and M. Inoue. An education curriculum of iot prototype construction system. In *2017 IEEE 6th Global Conference on Consumer Electronics (GCCE)*, pages 1–5, Oct 2017. doi: 10.1109/GCCE.2017.8229221.

[19] Tushar M Jois, Tina Pavlovich, Brigid M McCarron, David Kotz, and Timothy J Pierson. Smart use of smart devices in your home: A smart home security and privacy workshop for the general public. In *Proceedings of the 55th ACM Technical Symposium on Computer Science Education V. 1*, pages 611–617, 2024.

[20] Zouheir Trabelsi. Iot based smart home security education using a hands-on approach. In *2021 IEEE Global Engineering Education Conference (EDUCON)*, pages 294–301. IEEE, 2021.

[21] Mounib Khanafer and Tushar M. Jois. Towards application-driven iot education. In *2023 IEEE Global Engineering Education Conference (EDUCON)*, pages 1–7, 2023. doi: 10.1109/EDUCON54358.2023.10125155.

[22] Alexandre Oliveira Junior, Gustavo Funchal, Jonas Queiroz, Jorge Loureiro, Tiago Pedrosa, Javier Parra, and Paulo Leitao. Learning cybersecurity in iot-based applications through a capture the flag competition. In *2022 IEEE 20th International Conference on Industrial Informatics (INDIN)*, pages 560–565. IEEE, 2022.

[23] Pallavi P Deshmukh, Cameron D Patterson, and William T Baumann. A hands-on modular laboratory environment to foster learning in control system security. In *Frontiers in Education Conference (FIE), 2016 IEEE*, pages 1–9. IEEE, 2016.

[24] Leonardo Babun, Z Berkay Celik, Patrick McDaniel, and A Selcuk Uluagac. Real-time analysis of privacy-(un) aware iot applications. *arXiv preprint arXiv:1911.10461*, 2019.

[25] Abbas Acar, Hossein Fereidooni, Tigist Abera, Amit Kumar Sikder, Markus Miettinen, Hidayet Aksu, Mauro Conti, Ahmad-Reza Sadeghi, and Selcuk Uluagac. Peek-a-boo: I see your smart home activities, even encrypted! In *Proceedings of the 13th ACM Conference on Security and Privacy in Wireless and Mobile Networks*, pages 207–218, 2020.

[26] Z Berkay Celik, Leonardo Babun, Amit Kumar Sikder, Hidayet Aksu, Gang Tan, Patrick McDaniel, and A Selcuk Uluagac. Sensitive information tracking in commodity {IoT}. In *27th USENIX Security Symposium (USENIX Security 18)*, pages 1687–1704, 2018.

[27] Amit Kumar Sikder, Hidayet Aksu, and A Selcuk Uluagac. {6thSense}: A context-aware sensor-based attack detector for smart devices. In *26th USENIX Security Symposium (USENIX Security 17)*, pages 397–414, 2017.

[28] J. He, Dan Chia-Tien Lo, Y. Xie, and J. Lartigue. Integrating internet of things (iot) into stem undergraduate education: Case study of a modern technology infused courseware for embedded system course. In *2016 IEEE Frontiers in Education Conference (FIE)*, pages 1–9, Oct 2016. doi: 10.1109/FIE.2016.7757458.

[29] Mark JW Lee, Sasha Nikolic, Peter J Vial, Christian H Ritz, Wanqing Li, and Tom Goldfinch. Enhancing project-based learning through student and industry engagement in a video-augmented 3-d virtual trade fair.

[30] José P Queiroz-Neto, Diego C Sales, Hayanne S Pinheiro, and Benjamin O Neto. Using modern pedagogical tools to improve learning in technological contents. In *Frontiers in Education Conference (FIE), 2015. 32614 2015. IEEE*, pages 1–8. IEEE, 2015.

[31] Tanja Zseby, Félix Iglesias Vázquez, Alistair King, and KC Claffy. Teaching network security with ip darkspace data. *IEEE Transactions on Education*, 59(1):1–7, 2016.

[32] Jeannie Oakes. Opportunities, achievement, and choice: Women and minority students in science and mathematics. *Review of research in education*, 16:153–222, 1990.

[33] Zhang Kai. Specialized course" salary+ bonus" assessment. In *Computer Science & Education (ICCSE), 2015 10th International Conference on*, pages 870–873. IEEE, 2015.