WIP: Integrating Cybersecurity Education: Implementation of an Undergraduate Course on Malicious Thermal Sensor Defense

Amin Malek, SM IEEE
Department of Computer and Electrical Engineering
California State University Bakersfield, California, USA
aminmalek_m@ieee.org

Ahmad Patooghy
Department of Computer Systems Technology
North Carolina A&T State University, Greensboro, USA
apatooghy@ncat.edu

Abdel-Hameed Badawy
Department of Electrical and Computer Engineering
New Mexico State University, Las *Cruces, NM, USA*
badawy@nmsu.edu

***Abstract*—Contribution: This work-in-progress innovative practice paper presents the inception of an undergraduate course focusing on the Ensemble of Countermeasures for Malicious Thermal Sensors Attacks (ECMTA), representing a novel endeavor at this academic level. Rooted in prior research across academic and industrial domains, this ongoing initiative embodies a journey of exploration and discovery in an emerging field, awaiting feedback from students and our industrial advisory board.**

Additionally, this proposal advocates for a flipped classroom (FC) model, prioritizing pre-class materials for theoretical understanding and in-class sessions for practical application and collaboration. Simultaneously, this project is an ongoing investigation into the effectiveness of FC methodologies for Hispanic/Latino populations in cybersecurity education. Recognizing the current dearth of consensus in the literature regarding this demographic's response to FC, the project aims to address this gap through a comprehensive assessment of Hispanic/Latino students' attitudes and academic outcomes, with findings expected by the end of 2024.

Background: The surge in IoT devices revolutionized industries, offering convenience and connectivity. Yet, they pose substantial cybersecurity challenges, notably in thermal sensor vulnerabilities. Attackers' exploitation of these sensors to manipulate the temperatures of IOT devices underscores the urgent necessity for robust cybersecurity in IoT ecosystems.

***Intended outcome*: This course's intended outcome is multifaceted. Students will grasp thermal sensor vulnerabilities and learn varied countermeasures to mitigate risks. Practical skills will be honed through hands-on lab exercises and simulations. Additionally, they'll foster a mindset of continual learning, which is vital for evolving cybersecurity careers. Following this study, we aim to assess the effectiveness of flipped classroom methodologies for Hispanic/Latino populations in cybersecurity education.**

Application Design: The course offers theoretical lectures, practical workshops, research projects, and assessments focused on defending against thermal sensor attacks. It integrates cybersecurity into undergraduate curricula, fostering innovative teaching methods. Ultimately, it aims to prepare a new generation of cybersecurity professionals for security challenges.

Keywords—Active learning, Cybersecurity, Computer Engineering education, instructional design

I. Background and significance

The rapid proliferation of Internet of Things (IoT) devices has revolutionized numerous aspects of daily life, from smart homes to telecommunication and industrial automation [1]. However, this interconnected ecosystem also presents unprecedented challenges in terms of cybersecurity [2]. As IoT devices become increasingly integrated into critical infrastructure and personal environments, they become attractive targets for malicious actors seeking to exploit vulnerabilities for various nefarious purposes [3, 4]. Among the myriad IoT devices, thermal sensors play a pivotal role in diverse applications, including environmental monitoring, energy management, and healthcare. Their ability to detect and measure temperature variations makes them indispensable in numerous industries. However, thermal sensors are not immune to cybersecurity threats despite their importance. Malicious actors can exploit thermal sensor vulnerabilities to compromise data integrity and confidentiality, leading to potentially catastrophic consequences [3].

A. Significance, Goals, and the Vision

This paper advocates for tailored cybersecurity education for IoT security, particularly in countering attacks on thermal sensors, proposing an undergraduate course named Ensemble of Countermeasures for Malicious Thermal Sensors Attacks (ECMTA). The course adopts a flipped classroom model, blending theory with practical application, emphasizing research to prepare students for cybersecurity careers. It features hands-on lab exercises simulating real-world scenarios, fostering skills in network analysis, intrusion detection, secure coding, and promoting student collaboration and experimentation.

B. Course Objectives and Outline

The ECMTA course was meticulously designed to equip students with the knowledge and skills to address the evolving challenges posed by malicious actors targeting thermal sensor-enabled systems. The course objectives are outlined as follows:

- Understand the principles of thermal sensors and their importance in modern systems: This objective provides students with a comprehensive understanding of thermal sensing technologies, their applications, and their significance in various industries.
- Identify vulnerabilities and attack vectors associated with thermal sensors.

- Explore existing malicious thermal sensor attacks and their impact on various industries.
- Analyze the methodologies and techniques employed by attackers targeting thermal sensors.
- Develop strategies for detecting and mitigating malicious thermal sensor attacks.
- Design and implement an ensemble of countermeasures to enhance the security of thermal sensor-enabled systems.

The course is structured over sixteen weeks, with each week dedicated to specific topics and activities.

C. Problem Definition

Despite the escalating sophistication of cybersecurity threats, undergraduate curricula often lack specialized courses addressing emerging vulnerabilities such as malicious thermal sensor attacks. These attacks exploit vulnerabilities in sensor technology, posing significant risks to critical infrastructure, personal privacy, and national security. The absence of dedicated coursework focusing on countermeasures for such threats leaves undergraduate students ill-equipped to understand, prevent, and mitigate these evolving cybersecurity risks. Consequently, there is a pressing need to introduce a new undergraduate course titled "Ensemble of Countermeasures for Malicious Thermal Sensors Attacks (ECMTA)" to equip students with the theoretical knowledge, practical skills, and critical mindset necessary to confront and address this growing threat landscape effectively. Moreover, the project aims to shed further light on the efficacy of flipped classroom (FC) methodologies, particularly concerning Hispanic/Latino populations. The current literature presents a mixed perspective on the effectiveness of FC for this demographic group.

C. Implementation

The proposed ECMTA course initially faced approval delays, prompting the integration of its curriculum into the Microprocessor System Design course to expedite essential cybersecurity education delivery. This integration leverages the fourth-year course's structure and content alignment, offering students interdisciplinary learning experiences encompassing IoT security and thermal sensor vulnerabilities.

The Microprocessor System Design course's existing emphasis on hardware and software integration forms a robust foundation for integrating ECMTA modules and addressing emerging cybersecurity threats targeting IoT devices. This approach optimizes resource utilization and ensures timely cybersecurity education delivery, fostering students' readiness for modern technology environments where cybersecurity is paramount to system design and implementation.

D. Intended Outcome

ECMTA aims to equip students with skills to tackle threats to thermal sensor systems through a flipped classroom model that fosters interactive learning.

Comprehensive Understanding: By the end of the course, students will develop a thorough understanding of thermal sensors, their importance in modern systems, and the vulnerabilities associated with them. They will be able to analyze existing malicious thermal sensor attacks and their impact on various industries, gaining insights into the methodologies and techniques employed by attackers.

Practical Skills Development: Through hands-on lab sessions and practical exercises, students will develop practical skills in identifying vulnerabilities, detecting anomalies, and implementing mitigation strategies to enhance the security of thermal sensor-enabled systems. They will also learn to design and implement an ensemble of countermeasures, effectively integrating detection, prevention, and response mechanisms.

Critical Thinking and Problem-Solving: The flipped classroom model fosters active learning and critical thinking by encouraging students to engage deeply with theoretical concepts before coming to class. In-class sessions focus on collaborative problem-solving activities, case studies, and practical demonstrations, allowing students to apply their knowledge to real-world scenarios and develop creative solutions to cybersecurity challenges.

Research Opportunities: The course provides students with opportunities to conduct research on emerging topics in IoT security, mainly related to thermal sensor vulnerabilities and countermeasures. The course will expose undergraduate students to the research projects of an active NSF project run collaboratively by California State University, Bakersfield (CSUB), North Carolina A&T State University, and New Mexico State University. Through research projects and assignments, students can explore innovative solutions, contribute to advancing cybersecurity knowledge, and develop their analytical and research skills.

II. System Design

As previously mentioned, this paper centers on two primary objectives. Firstly, it delineates a novel course's design and implementation process that equips undergraduate students with the knowledge and skills to effectively combat emerging cybersecurity threats. Secondly, this project represents an ongoing investigation into the effectiveness of FC methodologies for Hispanic/Latino populations in cybersecurity education.

A comprehensive study conducted by Mok et al. [5] examined the integration of FC across four information systems courses, yielding favorable results. Notably, the implementations and interpretations of FC varied considerably within the study, mirroring the diversity observed in the existing literature. Broadly, FC typically involves the following components:

- Students engage with preparatory material, often in the form of videos, outside of class, sourced from instructor-provided content [5], online platforms like YouTube [6], or Massive Open Online Courses (MOOCs) [7].
- In-class sessions emphasize constructivist, dialogic learning experiences, frequently organized into groups [8] or pair activities [4].
- Assessment mechanisms, such as pre-lecture quizzes [4] or post-lecture quizzes [8], are commonly integrated before and/or after the in-class activities.
- Some implementations of FC blend traditional classroom elements, incorporating post-activity assignments like

homework [9], group tasks [4], and assigned textbook readings [4].

Based on a review of many literature sources, it is apparent that numerous studies fail to articulate their instructional approach in a manner conducive to replication by others [10]. Our contribution to the current state of research is twofold: Providing a clear and reproducible account of implementing the flipped classroom (FC) model and evaluating the attitudes of Hispanic/Latino and/or non-traditional students towards FC.

As reported in [11], The effectiveness of dialogic instructional strategies such as active learning remains uncertain across all demographic groups, including Hispanic/Latino populations [12, 13]. Within the context of undergraduate databases, Rueda [9] observed a positive reception of the FC model among Hispanic/Latino students. However, no comparative analysis was conducted between Hispanic/Latino students and the general population. In a comprehensive study by Carter et al. [14], which involved flipping 13 sections of liberal arts Mathematics courses, it was found that while Black and African American students showed significant improvement with FC, Hispanic/Latino students did not demonstrate the same level of improvement. Thus, no consensus exists regarding the efficacy of FC for Hispanic/Latino populations.

This ongoing project aims to shed further light on the efficacy of FC methodologies, particularly concerning Hispanic/Latino populations focusing on cybersecurity-related topics. While current literature presents a mixed perspective on the effectiveness of FC for this demographic group, our ongoing assessment seeks to provide more conclusive data.

At the end of this project, through rigorous data collection and analysis, we aim to generate insights that can inform future educational practices and interventions tailored to the needs of Hispanic/Latino learners. As we progress with our assessment, we anticipate obtaining clearer insights into the effectiveness of FC for Hispanic/Latino populations, thus contributing to the broader discourse on inclusive educational approaches.

A. *Design and Implementation of Class Activities, including sample assignments for the ECMTA course*

The flipped classroom model for the ECMTA course emphasizes active learning, collaborative problem-solving, and hands-on activities during in-person class sessions. These activities are designed to reinforce theoretical concepts, stimulate critical thinking, and provide students with practical experience in applying cybersecurity principles to real-world scenarios. Following are a few examples of designed class activities implemented in the ECMTA course:

1. *Group Discussions and Case Studies:*

In this activity, the instructor facilitates group discussions on recent malicious thermal sensor attacks, case studies, and research papers on IoT security. Students will analyze real-world scenarios, identify vulnerabilities, discuss attack methodologies, and brainstorm potential countermeasures in small groups.

1.1 *Sample Assignment:* Designing a Multi-Layered Defense Strategy against Malicious Thermal Sensor Attacks in Smart Home Environments

1.1.1. *Part 1: Individual Research*

Each student will conduct independent research on the following topics:

- Specific types of malicious attacks targeting thermal sensors in smart home IoT devices, such as temperature spoofing or sensor tampering.
- Existing countermeasures and defense mechanisms, including encryption protocols, anomaly detection algorithms, and hardware-based security features, are used to mitigate the risks associated with these attacks.
- Case studies or real-world examples of successful or attempted attacks on thermal sensors within smart home systems highlight vulnerabilities and lessons learned.
- Emerging trends and developments in smart home IoT security, focusing on advancements in thermal sensors protection and threat mitigation strategies.

1.1.2. *Part 2: Group Collaboration*

After completing their individual research, students will form groups to collaborate on designing a comprehensive security strategy for smart home environments. Each group will be tasked with the following:

- Combining individual research findings to identify the most significant threats posed by malicious thermal sensor attacks in smart homes, considering factors such as privacy breaches or physical safety risks.
- Developing a multi-layered defense framework that integrates diverse countermeasures and defense mechanisms, such as data encryption, anomaly detection, and physical tamper resistance.
- Creating a detailed implementation plan outlining the deployment and integration of the proposed security strategy within a hypothetical smart home environment, including user interface design and system scalability considerations.
- Presenting their security strategy to the class, showcasing innovative approaches and practical solutions employed by the group to address the unique challenges of securing thermal sensors in smart home IoT devices.

1.1.3. *Group Discussion:*

During the group discussion session, each group will present their security strategy and collaborate with the class. Topics for discussion include:

- Evaluation of the effectiveness and feasibility of different countermeasures and defense mechanisms proposed by each group, considering factors such as cost-effectiveness and user acceptance.
- Identifying potential limitations or vulnerabilities within the proposed security strategies and brainstorming additional safeguards or enhancements.
- Ethical considerations and implications associated with the implementation of security measures in smart

home environments, including issues related to data privacy and consumer trust.

- Reflection on lessons learned and insights gained from the assignment, including implications for future research in smart home IoT security and industry best practices.

Through this assignment and group discussion, students will gain practical experience in analyzing cybersecurity challenges specific to smart home environments, designing robust defense strategies, and engaging in collaborative problem-solving within a real-world context.

2. *Problem-Solving Exercises:*

In-class problem-solving exercises challenge students to apply their knowledge of detection techniques and mitigation strategies to hypothetical cybersecurity scenarios. Students work individually or in teams to analyze attack vectors, design defense mechanisms, and develop response plans.

2.1. Sample assignment:

In a simulated cyberattack scenario, an adversary seeks to manipulate thermal sensor data to disrupt the operation of a smart agriculture system. The student's task is to devise detection algorithms and mitigation strategies to thwart the attack and safeguard the system's integrity.

2.1.1. Guidelines for Answering:

2.1.1.1. Understanding the Scenario: Students will begin by carefully analyzing the scenario provided. Identify key components such as the smart agriculture system, the role of thermal sensors, and the potential impact of the cyberattack on system functionality and productivity.

2.1.1.2. Identification of Threats: List the potential threats posed by the adversary's manipulation of thermal sensor data. Consider how these threats could compromise the smart agriculture system's integrity, reliability, and security.

2.1.1.3. Detection Algorithms: Propose detection algorithms that identify anomalous or malicious activities related to thermal sensor data.

2.1.1.4. Mitigation Strategies: Devise mitigation strategies to counteract the effects of the cyberattack and protect the smart agriculture system.

2.1.1.5. Integration and Testing: Consider how detection algorithms and mitigation strategies can be integrated into the existing smart agriculture system. Outline a plan to test these measures in a simulated environment to validate their effectiveness and identify potential shortcomings.

2.1.1.6. Ethical Considerations: Reflect on the ethical implications of deploying detection algorithms and mitigation strategies in the context of smart agriculture. Consider factors such as data privacy, transparency, and the potential impact on agricultural practices and stakeholders.

2.1.1.7. Presentation: Students must present their proposed detection algorithms and mitigation strategies clearly and concisely, highlighting their rationale, technical feasibility, and potential effectiveness in safeguarding the integrity of the smart agriculture system.

By following these guidelines, students can effectively analyze the cyberattack scenario, devise proactive detection algorithms and mitigation strategies, and contribute to protecting critical infrastructure in the agricultural sector.

3.1. Sample Lab Assignment: Simulating Malicious Thermal Sensor Attacks using MATLAB

This hands-on lab uses MATLAB to simulate and analyze malicious thermal sensor attacks in an IoT environment. MATLAB is a versatile software platform for simulating various experiments across fields such as electronics, telecommunications [15], and cybersecurity, enabling complex modeling, analysis, and data visualization. Through this lab, students will gain practical experience in understanding the behavior of thermal sensors, identifying potential vulnerabilities, and developing countermeasures to mitigate the impact of attacks.

3.1.2. Lab Activities:

Below are the tasks students need to complete to import and visualize the data

3.1.2.1. Data Visualization and Analysis:

- Import the sample dataset into MATLAB.
- Visualize the temporal and spatial distribution of thermal sensor readings using MATLAB's plotting functions.
- Calculate descriptive statistics such as mean, median, and standard deviation to characterize the behavior of the thermal sensors under normal operating conditions.

3.1.2.2. *Injection of Malicious Data*:

- Simulate a malicious attack by injecting anomalous data into the sample dataset to mimic the behavior of compromised thermal sensors.
- Modify the temperature readings of selected sensors to simulate various attack scenarios, such as temperature spoofing or sensor tampering.
- Introduce different levels of attack severity by varying the magnitude and duration of the injected anomalies.

3.1.2.3. Detection Algorithms Development:

- Develop MATLAB detection algorithms to identify anomalous patterns in thermal sensor data.
- Implement statistical analysis, machine learning, or signal processing techniques to distinguish between normal and malicious sensor readings and evaluate their performances

3.1.2.4. Mitigation Strategies Implementation:

- Design mitigation strategies using MATLAB to mitigate the impact of malicious thermal sensor attacks.
- Implement countermeasures, such as data encryption, anomaly detection, or sensor redundancy, to enhance the IoT system's resilience against attacks.
- Assess the effectiveness of the mitigation strategies by comparing the system's performance before and after their implementation under simulated attack scenarios.

3.1.2.5. Performance Evaluation and Reporting:

- Evaluate the performance of the detection algorithms and mitigation strategies using metrics such as detection accuracy, false positive rate, and system recovery time.

- Generate visualizations and reports summarizing the findings of the lab experiments.

Through this hands-on lab, students will gain valuable experience in simulating, analyzing, and mitigating malicious thermal sensor attacks using MATLAB or Python. They will enhance their understanding of cybersecurity challenges in IoT environments and develop practical skills in cyber defense.

III. Evaluation and Future Work

As this paper represents a work in progress, a comprehensive evaluation of the ECMTA course using the outlined criteria has not yet been conducted. However, the methodology presented provides a framework for future evaluation efforts to assess the course's effectiveness in achieving its learning objectives and enhancing student outcomes.

In our future work, we plan to conduct thorough evaluations of the ECMTA course using a combination of formative and summative assessment methods. These evaluations will include:

Formative Assessment: Throughout the course, formative assessments like quizzes, exercises, and discussions will track progress and offer feedback. Summative assessments at the course end will evaluate mastery through exams, presentations, and papers. Additionally, student feedback via surveys and discussions will inform course design and delivery improvements.

Continuous Improvement: Based on evaluation findings, we will implement revisions and refinements to the course curriculum, instructional materials, and assessment methods to address identified needs and improve student learning outcomes. Continuous improvement efforts will be guided by data-driven decision-making and informed by best practices in cybersecurity education.

External Review: In addition to internal evaluation processes, external review mechanisms may be employed to validate the quality and rigor of the course. Subject matter experts, industry professionals, and academic peers will be invited to provide feedback on course materials, instructional activities, and assessment practices.

By conducting comprehensive evaluations of the ECMTA course, we aim to assess its effectiveness, identify areas for improvement, and make informed decisions to enhance student learning and success in the field of cybersecurity. We will report the results of these evaluations in future publications, providing valuable insights and contributions to cybersecurity education's growing body of knowledge.

Moreover, by assessing the attitudes and academic achievements of Hispanic/Latino students towards FC, we expect to attain a more profound comprehension of its effects on this particular demographic. By conducting thorough data collection and analysis, our goal is to produce valuable insights that can guide forthcoming educational strategies and interventions specifically designed to address the requirements of Hispanic/Latino learners.

Acknowledgment

This work is supported by the National Science Foundation under Grant No. 2219678, a collaborative grant between California State University, Bakersfield (CSUB), North Carolina A&T State University, and New Mexico State University. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the National Science Foundation.

References

[1] T. Kouvara, A. Fanariotis, V. Fotopoulos, C. Karachristos and T. Orphanoudakis, "Why Re-Focus on IoT in Education? Evidence of the PARADIGM Project," in 2023 IEEE Frontiers in Education Conference (FIE), College Station, TX, USA, 2023, pp. 1-9.

[2] D. Tayouri; S. Hassidim; A. Smirnov; A. Shabtai, "Cybersecurity in Agile Cloud Computing--Cybersecurity Guidelines for Cloud Access," in Cybersecurity in Agile Cloud Computing--Cybersecurity Guidelines for Cloud Access, 28 Sept. 2022, pp.1-36.

[3] M. Abdelrehim, A. Patooghy, A. Malekmohammadi, and A. -H. A. Badawy, "BIC: Blind Identification Countermeasure for Malicious Thermal Sensor Attacks in Mobile SoCs", in 23rd International Symposium on Quality Electronic Design (ISQED), Santa Clara, CA, USA, 2022, pp. 1-6.

[4] A. Cruz, A. Malek, A. Medina, and M. Danforth. "Addressing the Needs of Hispanic/Latino(a) Students with the Flipped Classroom Model". In 2023 ASEE Annual Conference & Exposition,

[5] H. Ngee Mok, 'Teaching tip: The flipped classroom', Journal of Information Systems Education, vol. 25, no. 1, 2014, pp. 7–11.

[6] R. A. Salas Rueda, 'Use of the flipped classroom to design creative and active activities in the field of computer science', Creativity Studies, vol. 13, no. 1, 2020, pp. 136–151.

[7] S. Bhat, R. Raju, S. Bhat, and R. D'Souza, 'Redefining quality in engineering education through the flipped classroom model', Procedia Comput Sci, vol. 172, 2020, pp. 906–914.

[8] B. H. Shraddha et al., 'Enhanced learning experience by comparative investigation of pedagogical approach: Flipped classroom', Procedia Comput Sci, vol. 172, 2020, pp. 22–27.

[9] G. Akçayır, M. Akçayır, "The flipped classroom: A review of its advantages and challenges", Computers & Education, Volume 126,2018, Pages 334-345.

[10] A. Cruz, D. Derickson, and A. Malek. "Board 393: Supporting Student Internships with the Nsf Hsi Program at a Medium-Sized Hispanic-Serving Institution." In 2023 ASEE Annual Conference & Exposition. 2023.

[11] A. M. Mohammadi, A. Hajrasouliha, J. P. Cleary, and J. H. Woo. "The smart campus as a testing ground for smart cities." In 2021 ASEE Virtual Annual Conference Content Access. 2021.

[12] P. den Brok, J. Levy, T. Wubbels, and M. Rodriguez, 'Cultural influences on students' perceptions of videotaped lessons', International Journal of Intercultural Relations, vol. 27, no. 3, 203, pp. 355–374.

[13] J. R. Lotto, 'Engagement of Hispanic/Latinx ESL Students in Higher Education Flipped Classrooms: A Qualitative Descriptive Study Submitted by', Grand Canyon University, 2022

[14] C. L. Carter, R. L. Carter, and A. H. Foss, "The Flipped Classroom in a Terminal College Mathematics Course for Liberal Arts Students", AERA Open, vol. 4, no. 1, 2018

[15] S.R. Imam, N. Dong-Nhat, and A. Malekmohammadi. "High dispersion four-mode fiber for mode-division multiplexing systems." Optik 181, 2019, pp. 1-12.