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 #48393

Introducing an Interactive Hands-On Educational Module for an Embedded Systems Course focused on embedded security

Dr. Ashish Kharel, The University of Toledo

Ashish Kharel received a Ph.D. in Engineering, with concentration in Computer Science from the University of Toledo, OH, USA. Currently, he is a Visiting Assistant Professor at the University of Toledo. His research interests include machine learning and optimization of deep networks. Most of his published papers implement very deep neural networks to help solve problems involving cellular biology.

Dr. Ahmad Y Javaid, The University of Toledo
Quamar Niyaz, Purdue University Northwest
Sidike Paheding, Fairfield University

Assistant Professor in the Department of Computer Science and Engineering.

Devinder Kaur, The University of Toledo

Introducing an Interactive Hands-On Educational Module for an Embedded Systems Course focused on Embedded Security

Ashish Kharel[1], Ahmad Y Javaid[1], Quamar Niyaz[2], Sidike Paheding[3], Xiaoli Yang[4], and Devinder Kaur[1]
[1]The University of Toledo, Toledo, OH 43607, USA
{ashish.kharel, ahmad.javaid, devinder.kaur}@utoledo.edu
[2]Purdue University Northwest, Hammond IN 46323, USA
qniyaz@pnw.edu
[3]CS Department, Fairfield University, Fairfield, CT 06824, USA
spaheding@fairfield.edu
[4]Talwar College of Engineering and Computer Sciences, Fort Wayne, IN 46803, USA
xxyang@indianatech.edu

Introduction

In today's digital age, cybersecurity has become a critical concern for individuals, organizations, and governments worldwide. The increasing reliance on digital technologies and the internet has exposed systems to a wide array of cyber threats, ranging from data breaches and ransomware attacks to sophisticated state-sponsored cyber espionage. The consequences of these cyber threats can be devastating, leading to financial losses, reputational damage, and even national security risks. As such, the importance of cybersecurity cannot be overstated; it is essential for protecting sensitive information, ensuring the integrity of systems, and maintaining the trust of users [1, 2].

Embedded systems, which are specialized computing systems designed to perform dedicated functions within larger systems, are ubiquitous in modern technology. They are found in a wide range of applications, from household appliances and medical devices to industrial control systems and critical infrastructure. As these systems become more interconnected and integrated into the Internet of Things (IoT), the need for robust cybersecurity measures to protect them has grown exponentially. Embedded systems often operate in environments where security vulnerabilities can have severe consequences, such as in automotive systems, where a security breach could compromise the safety of passengers [3, 4].

The unique characteristics of embedded systems present distinct challenges for cybersecurity. Unlike general-purpose computing systems, embedded systems often have limited processing power, memory, and energy resources, which can constrain the implementation of traditional security measures. Additionally, embedded systems frequently operate in real-time environments, where delays caused by security processes can be unacceptable. These constraints necessitate the development of specialized security solutions tailored to the specific needs and limitations of embedded systems [5].

Moreover, the proliferation of embedded systems in critical infrastructure, such as power grids, transportation networks, and healthcare systems, underscores the importance of securing these systems against cyber threats. A successful cyber-attack on embedded systems in these sectors could lead to widespread disruptions, endangering public safety and causing significant economic damage. Therefore, ensuring the security of embedded systems is not only a technical challenge but also a matter of public interest and national security. Addressing these challenges requires a tailored approach to embedded system security, including system hardening, encryption for communication, and secure coding practices [6].

.

In conclusion, cybersecurity is a fundamental aspect of modern technology that protects against a wide range of cyber threats. The importance of cybersecurity is magnified in the context of embedded systems, which are integral to many critical applications and face unique security challenges. Addressing these challenges requires a comprehensive understanding of both cybersecurity principles and the specific requirements of embedded systems, making it a vital area of focus for researchers, practitioners, and policymakers alike [7].

Goals and Objectives

The primary goal of this module is to provide students with a comprehensive understanding of cybersecurity principles as they apply to embedded systems. The specific objectives include:

1. **Understanding Cybersecurity Fundamentals**: Students will learn the basic concepts of cybersecurity, including the importance of protecting systems, networks, and programs from digital attacks. They will become familiar with key terms such as attack vectors, attack surfaces, threat actors, and vulnerabilities. Understanding these fundamentals is crucial for recognizing the various ways in which embedded systems can be compromised and the potential impact of such compromises.
2. **Identifying Cybersecurity Threats**: The module will cover various types of cybersecurity threats specific to embedded systems, such as unauthorized access, data breaches, denial-of-service attacks, malware, physical attacks, and supply chain attacks. Students will also learn about common embedded software vulnerabilities like buffer overflows and improper input validation. By identifying these threats, students can better understand the specific risks associated with embedded systems and how to mitigate them.
3. **Addressing Unique Challenges**: Students will explore the unique challenges of securing embedded systems, including limited resources, power consumption considerations, real-time operation requirements, limited connectivity options, legacy systems, heterogeneous ecosystems, and lack of security expertise. These challenges require specialized security solutions that are tailored to the constraints and requirements of embedded systems.
4. **Implementing Security Measures**: The module will teach techniques for hardening embedded systems, implementing encryption for communication, and following secure coding practices. Practical exercises will involve identifying and mitigating vulnerabilities in a traffic light controller program. Implementing these security measures

is essential for protecting embedded systems from cyber threats and ensuring their reliable operation.

5. **Conducting Cybersecurity Assessments**: Students will learn how to conduct vulnerability scans, identify potential security weaknesses, and implement mitigation strategies. They will also engage in code review and debugging exercises to reinforce their understanding of secure coding practices. Conducting regular cybersecurity assessments is crucial for maintaining the security of embedded systems and addressing emerging threats.

By achieving these objectives, the module aims to equip students with the knowledge and skills necessary to protect embedded systems from various cybersecurity threats. This comprehensive approach ensures that students are well-prepared to address the unique security challenges associated with embedded systems and contribute to the development of secure and reliable embedded technologies.

Research Methodology and Activities:

The research methodology for this study involves a combination of pre-and post-learning surveys, practical exercises, and a comprehensive test to assess student's knowledge and confidence levels before and after completing the module. The methodology is designed to provide a thorough evaluation of the module's effectiveness in teaching cybersecurity principles for embedded systems. The course module was attended by 58 students, primarily first-year students, who are being introduced to the fundamentals of cybersecurity in embedded systems

1. **Pre- and Post-Learning Surveys**:
    - **Purpose**: The surveys are designed to measure students' general cybersecurity knowledge, understanding of embedded system security, and specific cybersecurity concerns for embedded systems.
    - **Structure**: The surveys consist of multiple-choice questions covering topics such as the definition of cybersecurity, the CIA triad, common cybersecurity threats, and best practices for securing embedded systems. The post-lab survey also includes questions to assess students' confidence in identifying and fixing vulnerabilities, as well as their comfort level with various aspects of cybersecurity for embedded systems. Table 1 lists the questions and their categories for the pre/post surveys.

Table 1. Pre-/Post-Lab Survey Questions

Section	**Question**
General Cybersecurity	What do you understand by the term "cybersecurity"?
	What are the three main components of the CIA triad?
	What are some common types of cybersecurity threats?
Embedded System Security	What is embedded systems cybersecurity?
	What are some common vulnerabilities in embedded systems?
	What are some ways to mitigate these vulnerabilities?
	What is the relationship between embedded systems cybersecurity and traffic light controllers?
	What are some specific cybersecurity concerns for traffic light controllers?

Section	Question
	What are some best practices for implementing secure embedded systems?
	Can you identify any potential vulnerabilities in the following code snippet?
	If you identify any vulnerabilities in the code snippet above, how would you mitigate them?
	What are some challenges of implementing secure embedded systems?
Knowledge Improvement	How confident are you in your ability to identify and fix vulnerabilities in embedded system s/w?
	How confident are you in your ability to secure embedded systems from cyberattacks?
	What aspects of cybersecurity for embedded systems do you feel most comfortable with?
	What aspects of cybersecurity for embedded systems do you feel least comfortable with?
	How can this lab be improved to help students learn more about cybersecurity for embedded systems? (Only Post-Lab Survey)

2. **Reading Material**:
   - **Purpose**: The reading material titled "Cybersecurity Fundamentals for Embedded Systems" is provided to students after the pre-survey and before engaging in the module/experiment. It aims to equip students with foundational knowledge of cybersecurity concepts and the specific challenges associated with securing embedded systems.
   - **Content**: The document covers various topics, including:
     - **Definition and Importance of Cybersecurity**: Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. It is crucial for preventing unauthorized access, tampering, or exploitation of vulnerabilities in embedded systems.
     - **Types of Cybersecurity Threats**: Common threats include unauthorized access, data breaches, denial-of-service attacks, malware, physical attacks, and supply chain attacks.
     - **Unique Challenges of Securing Embedded Systems**: These challenges include limited resources, power consumption considerations, real-time operation requirements, limited connectivity options, legacy systems, heterogeneous ecosystems, and lack of security expertise.
     - **Cybersecurity Measures**: Techniques for system hardening, implementing encryption for communication, and following secure coding practices.
     - **Vulnerability Scanning and Mitigation**: Conducting vulnerability scans, identifying potential security weaknesses, and implementing mitigation strategies.
   - **Assessment**: The effectiveness of the reading material is assessed through its impact on students' performance in the post-survey and practical exercises.
3. **Practical Exercises**:
   - **Purpose**: The practical exercises are designed to provide hands-on experience in identifying and mitigating vulnerabilities in embedded systems. These exercises reinforce theoretical knowledge and help students develop practical skills.
   - **Activities**: Students will engage in activities such as system hardening, implementing encryption for communication, and following secure coding practices. For example, students may work on identifying and mitigating vulnerabilities in a traffic light controller program.

- **Assessment**: The effectiveness of the practical exercises is assessed through observations, student feedback, and performance in the exercises.

4. **Comprehensive Test**:
   - **Purpose**: The comprehensive test is administered at the end of the module to evaluate students' practical understanding and application of the concepts taught.
   - **Structure**: The test includes sections on understanding code, debugging and testing, code auditing and analysis, principles applied, problem-solving techniques, and application of programming concepts. Table 2 lists the complete set of questions that were used for this test.

Table 2. Test Questions

Section	**Question**
Understanding the Code	Explain in your own words the purpose of a finite state machine in the provided traffic light code.
	What vulnerability was intentionally introduced in the code, and how does it impact the behavior of the traffic lights?
Debugging and Testing	Outline the steps you would take to verify the vulnerability and its impact on the traffic light operation.
	Describe a debugging technique you used to identify potential issues in the code, particularly related to the vulnerability.
Code Auditing and Analysis	What specific parts of the code did you analyze thoroughly to identify potential vulnerabilities? Describe your approach to auditing the code.
	Besides the introduced vulnerability, did you uncover any other potential weaknesses or issues in the code? If yes, elaborate.
Principles Applied	If you were to fix the introduced vulnerability, how would you approach modifying the code? Explain your strategy.
	What testing methods would you implement to ensure the code's robustness against similar vulnerabilities in the future?
Problem-Solving Techniques	Did you use a systematic approach or a brute-force method to find the vulnerability? Explain your methodology.
	What key lesson did you take away from this exercise about code security, debugging, and the importance of comprehensive testing?
Application of Programming Concepts	Which register is utilized for controlling the direction of GPIO pins in the code?
	What is the purpose of the Next array in the STyp struct?
	Which port and pin is used to detect north-facing car presence in the code?
	What does the PLL_Init(Bus80MHz) function call signify in the code?
	If an external interrupt was added to trigger a state change in the FSM, which register would likely be involved in configuring the interrupt?

Data Analysis and Conclusion Drawing

The data was collected from a class of 58 students in the Fall of 2024. The data collection process involved administering pre- and post-learning surveys to measure students' general cybersecurity knowledge, understanding of embedded system security, and specific cybersecurity concerns for embedded systems. The surveys consisted of multiple-choice questions covering various topics. It should be noted that the total number of responses varied between 54-58 while it remained the same for a few questions. The data collected from the surveys is summarized in Table 3.

Table 3. Comparative Summary of the Collected Pre/Post-Survey Data

Question	**Option**	**Pre**	**Post**
What do you understand by the term 'cybersecurity'?	All of the above	49	50
	I am not sure	1	0
	The practice of protecting systems, networks, and data from unauthorized access, use, disclosure, disruption, modification, or destruction	7	4
	The study of computer security and cryptography	1	1
	The process of developing and implementing security controls to protect against cyber threats	0	0
What are the three main components of the CIA triad?	Authentication, authorization, and auditing	1	0
	Confidentiality, integrity, and availability	38	51
	I am not sure	7	0
	Prevention, detection, and response	12	3
	None of the Above	0	1
What are some common types of cybersecurity threats?	All of the above	41	47
	I am not sure	1	4
	Malware, phishing, and social engineering attacks	15	1
	Denial-of-service attacks, man-in-the-middle attacks, and zero-day attacks	0	2
	None of the Above	0	0
What is embedded systems cybersecurity?	All of the above	34	43
	I am not sure	1	1
	The practice of protecting embedded systems from cyberattacks	3	0
	The process of developing and implementing security controls to protect embedded systems from unauthorized access, use, disclosure, disruption, modification, or destruction	20	11
	None of the Above	0	0
What are some common vulnerabilities in embedded systems?	All of the above	32	42
	Buffer overflows, cross-site scripting, and SQL injection	4	5
	I am not sure	9	0
	Lack of input validation and output encoding	7	3
	Weak passwords, insecure coding practices, and outdated software	5	4
How are some ways to mitigate these vulnerabilities?	All of the above	35	49
	I am not sure	5	0
	Input validation and output encoding	10	3
	Use of strong passwords and encryption	6	1
	Least privilege access	0	2
What is the relationship between embedded systems cybersecurity and traffic light controllers?	All of the above	36	50
	Cyberattacks on traffic light controllers can have serious consequences, such as causing traffic accidents or allowing unauthorized access to critical infrastructure	6	2
	I am not sure	2	0
	There are a number of specific cybersecurity concerns for traffic light controllers, such as the need to protect them from denial-of-service attacks and tampering	5	2
	Traffic light controllers are an example of embedded systems that need to be protected from cyberattacks	5	1
	All of the above	37	50

What are some specific cybersecurity concerns for traffic light controllers?	I am not sure	2	0
	Tampering	8	3
	Unauthorized access to configuration settings	8	1
	Denial-of-service attacks	0	1
What are some best practices for implementing secure embedded systems?	All of the above	38	51
	I am not sure	6	0
	Keep software and firmware up to date	8	4
	Use strong passwords and encryption	2	0
	Implement least privilege access	0	0
Can you identify any potential vulnerabilities in the following code snippet?	All of the above	14	19
	I am not sure	18	14
	Yes, the code is vulnerable to buffer overflows	11	15
	Yes, the code is vulnerable to cross-site scripting	8	3
	Yes, the code is vulnerable to SQL injection	4	3
If you identify any vulnerabilities in the code snippet above, how would you mitigate them?	All of the above	12	27
	I am not sure	17	6
	Use a parameterized query to prevent SQL injection attacks	3	3
	Use input validation to ensure that the input to the button_pressed() function is within the bounds of the buffer	17	14
	Use output encoding to ensure that the output from the button_pressed() function is not malicious	6	4
What are some challenges of implementing secure embedded systems?	All of the above	33	44
	Embedded systems are often deployed in remote and inaccessible locations, making it difficult to install and maintain security updates	5	1
	Embedded systems often have complex and interconnected software and hardware components	5	4
	Embedded systems often have limited resources, such as memory and processing power	7	3
	I am not sure	5	2
How confident are you in your ability to identify and fix vulnerabilities in embedded system software?	Extremely confident	0	1
	Moderately confident	11	26
	Not at all confident	16	3
	Somewhat confident	25	18
	Very confident	3	6
How confident are you in your ability to secure embedded systems from cyberattacks?	Extremely confident	0	1
	Moderately confident	8	23
	Not at all confident	23	6
	Somewhat confident	20	18
	Very confident	4	6
What aspects of cybersecurity for embedded systems do you feel most comfortable with?	All of the above	5	7
	Fixing vulnerabilities in embedded system software	7	13
	I am not sure	17	3
	Identifying vulnerabilities in embedded system software	20	27
	Implementing security measures to protect embedded systems from cyberattacks	6	4

What aspects of cybersecurity for embedded systems do you feel least comfortable with?	All of the above	15	6
	Fixing vulnerabilities in embedded system software	10	9
	I am not sure	8	3
	Identifying vulnerabilities in embedded system software	7	11
	Implementing security measures to protect embedded systems from cyberattacks	15	25

Figures 1-4 provide a more detailed look at how the students performed on some specific questions. We hand-picked the charts that visually show the huge difference this module made in enhancing the students' understanding of cybersecurity for embedded systems and increasing the student's confidence in their ability to handle and mitigate vulnerabilities within embedded software. Overall, more than 76% of students scored 70% or more on the 10-question test that was given to the students, as shown in Figure 4.

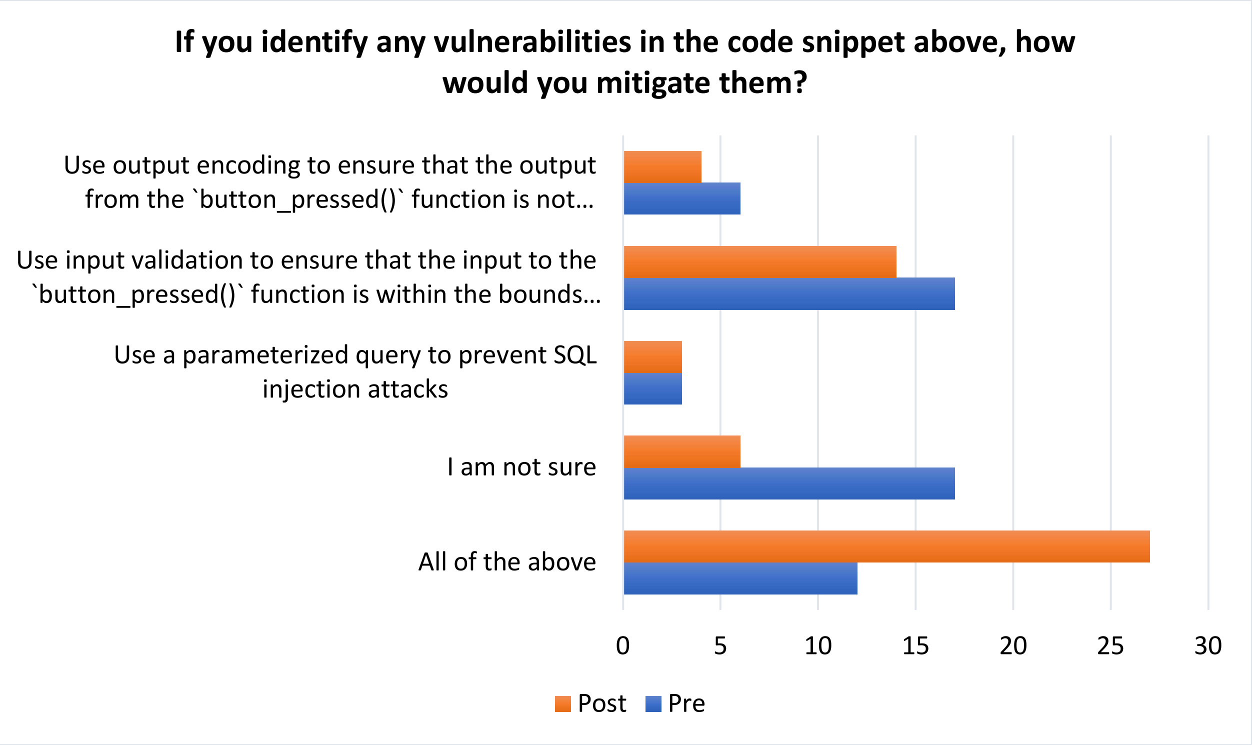

Figure1. Overall improvement in students' understanding of vulnerability mitigation

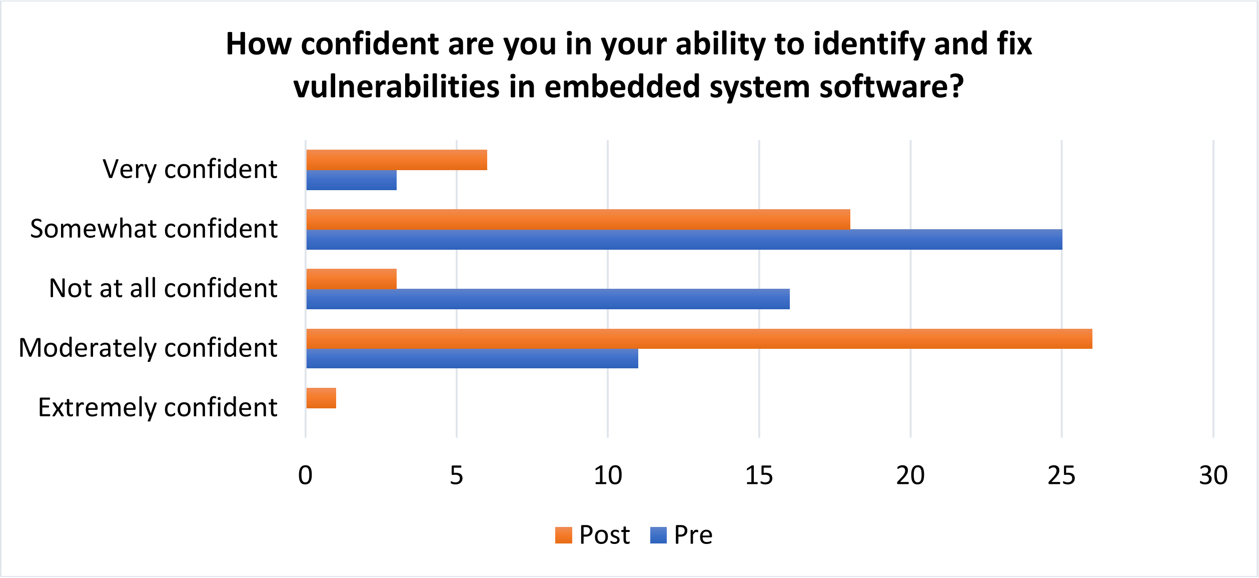

Figure 2. Overall improvement in students' confidence in their ability to identify and fix vulnerabilities in embedded system software

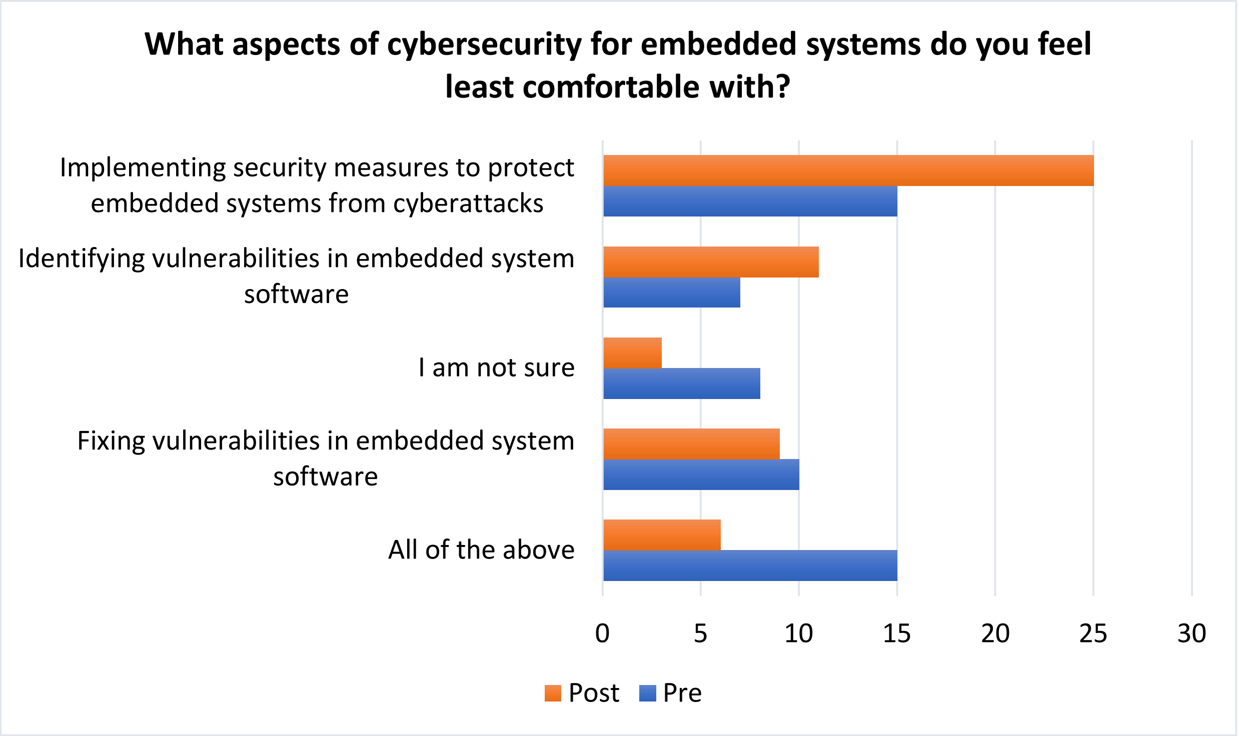

Figure 3. Overall improvement in student's comfort with dealing with cybersecurity-related aspects of an embedded system software

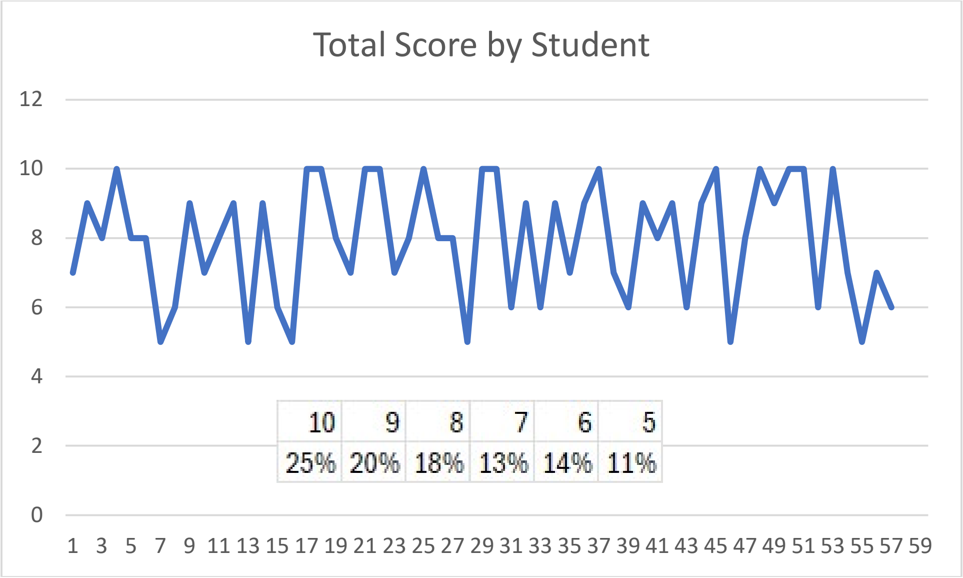

Figure 4. Total test score for the total of 56 attempts (range: 5-10)

The analysis of the survey data reveals the following insights:

1. **General Cybersecurity Knowledge**:
    - There was an increase in the number of correct responses for questions related to the CIA triad and common cybersecurity threats. This suggests an improvement in students' understanding of these fundamental concepts.
2. **Embedded System Security**:
    - The responses for questions related to embedded systems cybersecurity, common vulnerabilities, and mitigation strategies showed improvements. This indicates that students gained a better understanding of these specific areas.
3. **Confidence Levels**:
    - The confidence levels in identifying and fixing vulnerabilities in embedded system software showed significant improvement. This highlights the effectiveness of the practical exercises and hands-on experience in building students' confidence in these skills.
4. **Specific Concerns and Best Practices**:
    - The responses to questions related to specific cybersecurity concerns for traffic light controllers and best practices for implementing secure embedded systems showed improvements. This suggests that the module was effective in addressing these specific topics.
5. **Test Performance:**

- The test scores indicate that a majority of students performed well, with 14 students scoring a perfect 10 and 11 students scoring 9. This demonstrates a strong understanding of the concepts taught in the module.

Conclusion and Future Work

The data collected from the pre-and post-learning surveys, along with the comprehensive test scores, provide valuable insights into the effectiveness of the module in teaching cybersecurity principles for embedded systems. The analysis reveals areas where students showed improvement, as well as areas where additional support is needed.

1. **Knowledge Improvement**:
    - There were significant improvements in the number of correct responses to questions related to the CIA triad, common cybersecurity threats, embedded systems cybersecurity, common vulnerabilities, and mitigation strategies. This indicates that the module was effective in addressing these topics and enhancing students' understanding.
2. **Confidence Levels**:
    - The significant improvement in confidence levels for identifying and fixing vulnerabilities highlights the effectiveness of the practical exercises and hands-on experience. Providing students with additional opportunities to practice these skills can further enhance their confidence and proficiency.
3. **Test Performance**:
    - The test scores indicate that a majority of students performed well, with 14 students scoring a perfect 10 and 11 students scoring 9. This demonstrates a strong understanding of the concepts taught in the module and suggests that the instructional methods were effective.

To enhance the effectiveness of the module in the future, it is important to include more practical exercises and hands-on activities that focus on identifying and mitigating vulnerabilities in embedded systems. Additionally, reinforcing fundamental cybersecurity concepts through supplementary materials and interactive sessions can help improve students' overall understanding and retention of the material. By addressing these recommendations, the module can be further refined to better meet the needs of students and enhance their learning outcomes in the field of embedded system security, especially if the intention is to provide more detailed cybersecurity exposure in this course. This comprehensive approach ensures that students are well-prepared to tackle the unique challenges associated with securing embedded systems and contribute to the development of secure and reliable embedded technologies.

However, it should be noted that this was one of 10 modules developed by our team for various CSE/CS courses. The primary goal of developing these modules was to distribute training in cybersecurity across the entire CSE/CS curriculum, providing students with a holistic view and comprehensive cybersecurity training. Future work may focus on integrating advanced on-device security measures with real-time detection capabilities to protect production-network building controllers from cyber threats. This will provide students with hands-on experience in dealing with sophisticated cybersecurity challenges.

Acknowledgments

This material is based upon the work supported by the United States National Science Foundation under Grant No. by National Science Foundation Awards No. 1903419 and 1903423 through the Improving Undergraduate STEM Education (IUSE) program. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation. This study was approved by the Institutional Review Board (IRB) at Purdue University Northwest and the University of Toledo under protocol numbers IRB-2020-1119 and IRB-301407-UT, respectively. The authors may be contacted to get access to any material that has been developed as part of this module.

References

[1]. T. Tunggal, "Why is Cybersecurity Important?" UpGuard, Jan. 2025. [Online]. Available: https://www.upguard.com/blog/cybersecurity-important

[2]. "Why Is Cybersecurity Important," CompTIA, Oct. 2023. [Online]. Available: https://www.comptia.org/content/articles/why-is-cybersecurity-important

[3]. "What Is Embedded Systems Security?" Wind River. [Online]. Available: https://www.windriver.com/solutions/learning/embedded-systems-security

[4]. R. August, "The Importance of Embedded System Security in Modern Technology," Matt Brogi, Aug. 2024. [Online]. Available: https://mattbrogi.com/the-importance-of-embedded-system-security-in-modern-technology/

[5]. "Embedded System Security: Important Steps And Main Issues," Sirin Software. [Online]. Available: https://sirinsoftware.com/blog/embedded-system-security-important-steps-and-main-issues

[6]. "Why end-to-end security is important for embedded systems," Secure Code Warrior. [Online]. Available: https://www.securecodewarrior.com/article/embedded-systems-security

[7]. "Importance of Cyber Security: Need and Benefits," Knowledge Hut. [Online]. Available: https://www.knowledgehut.com/blog/security/importance-of-cyber-security