ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION

Paper ID #35701

A Capstone Project: Designing an IoT Threat Modeling to Prevent Cyber-attacks

Ms. Otily Toutsop, Morgan State University

Otily Toutsop is a Ph.D. student with a concentration on secure embedded systems in the Electrical and Computer Engineering department at Morgan State University. She is also affiliated with the Cybersecurity Assurance and Policy (CAP) center. She received her bachelor's degree in Computer Science. Her research interests focus on IoT Security, machine learning, artificial intelligence, cyber-physical system, software security, home automation systems, and networking security. Her work has been published in several conferences, including the IEEE Computer Science, IEEE Applied Imagery Pattern Recognition Workshop (AIPR), IEEE International Conference on Internet of Things: Systems, Management and Security (IoTSMS), IEEE Future Internet of Things and Cloud (FiCloud), IEEE International Conference on Smart Innovations (SCI).

Mrs. Rachida Satio Constance Kone, Morgan State University

Rachida is a PhD candidate in embedded systems at Morgan State University. After earning a Master's degree in electrical and energy engineering, Rachida worked as a Software Engineer before joining the PhD program at Morgan State University. As a project supervisor at the Cybersecurity Assurance and Policy (CAP) center, her research focuses on artificial intelligence, Internet of Things (IoT) and autonomous navigation.

Dr. ketchiozo wandji

With over 15 years of academic research and teaching, private industry, and government experience, Dr. Ketchiozo Thierry Wandji is an expert in cybersecurity risk management and software security. Dr. Wandji used to be the Software Security Technical Lead in the Systems Security Division of the US Navy's Naval Air Warfare Center Aircraft Division (NAVAIR) and the Cybersecurity Technical Expert in the Cyber Warfare Detachment, Dr. Wandji's duties at NAVAIR included assessing software security throughout the software development lifecycle; planning, developing, and coordinating high-impact research projects on cyber defensive technologies; overseeing the development of innovative cyber technologies; providing policy guidance and standards as well as workforce development for software security; and integrating these standards into the acquisition process to ensure that systems are both reliable and highly-resilient to cyberattacks. Currently, Dr. Wandji advances education in the field as an Associate Director for the Cybersecurity Assurance and Policy (CAP) Center and an Associate Professor at Morgan State University where he currently teaches cybersecurity, oversees cybersecurity research studies, and designs cybersecurity curriculum. He has played an integral role in the design and implementation of cybersecurity virtual labs (cyber range) for students to have a hands-on cybersecurity experience. Likewise, Dr. Wandji helped put together a comprehensive program of cybersecurity workforce development for the Department of the Navy which helped many engineers to become cybersecurity experts.

Prof. kevin kornegay, Morgan State University

Kevin T. Kornegay received the B.S. degree in electrical engineering from Pratt Institute, Brooklyn, NY, in 1985 and the M.S. and Ph.D. degrees in electrical engineering from the University of California at Berkeley in 1990 and 1992, respectively. He is currently the IoT Security Professor and Director of the Cybersecurity Assurance and Policy (CAP) Center for Academic Excellence in the Electrical and Computer Engineering Department at Morgan State University in Baltimore, MD. His research interests include hardware assurance, reverse engineering, secure embedded systems, and smart home/building security. Dr. Kornegay serves or has served on the technical program committees of several international conferences, including the IEEE Symposium on Hardware Oriented Security and Trust (HOST), IEEE Secure Development Conference (SECDEV), USENIX Security 2020, the IEEE Physical Assurance and Inspection of Electronics (PAINE), and the ACM Great Lakes Symposium on VLSI (GLSVLSI). He serves on the State of Maryland Cybersecurity Council and the National Academy of Sciences Intelligence

Community Science Board Cybersecurity Committee. He is the recipient of numerous awards, including He is the recipient of multiple awards, including the NSF CAREER Award, IBM Faculty Partnership Award, National Semiconductor Faculty Development Award, and the General Motors Faculty Fellowship Award. He is currently a senior member of the IEEE and a member of Eta Kappa Nu and Tau Beta Pi engineering honor societies.

Miss Caroline Kinyanjui, Morgan State University

Caroline Kinyanjui is a Ph.D. student with a concentration in secure embedded systems in the Electrical and Computer Engineering Department at Morgan State University. She holds a B.S. in electrical engineering in the same department. She is affiliated with the Cybersecurity Assurance and Policy (CAP) Center in the same institute. Her research interest includes security and privacy in Internet of Things (IoTs), Machine Learning, Cyber Security and Data Privacy.

Mr. Vinton Amsley Morris

Vinton received his bachelor's and master's degree in Information Systems from the University of Maryland Baltimore County. He is currently pursuing a Ph.D. in Secure Embedded Systems in the Department of Electrical and Computer Engineering (ECE) at Morgan State University. He is currently conducting research in the Cybersecurity Assurance and Policy (CAP) Center and the Center for Reverse Engineering and Assured Microelectronics (CREAM) Lab with a research focus on network and IoT device security. Additional research interest includes machine learning applications, artificial intelligence, and privacy.

Mr. Jay Jemal
Javaun Rose, Morgan State University

Electrical Engineering undergraduate student with a concentration in cybersecurity at Morgan State University.

A Capstone Project: Designing an IoT Threat Model to Prevent Cyber-attacks

Abstract

An NTT (Nippon Telegraph and Telephone) Data Corporation report found that 80% of U.S. consumers are concerned about their smart home data security. The Internet of Things (IoT) technology brings many benefits to people's homes, and more people across the world are heavily dependent on the technology and its devices. However, many IoT devices are deployed without considering security, increasing the number of attack vectors available to attackers. Numerous Internet of Things devices lacking security features has been compromised by attackers, resulting in many security incidents. Attackers can infiltrate these smart home devices and control the home via turning off the lights, controlling the alarm systems, and unlocking the smart locks, to name a few. Attackers have also been able to access the intelligent home network, leading to data exfiltration. There are many threats that smart homes face, such as the Man-in-the-Middle (MIM) attacks, data and identity theft, and Denial of Service (DoS) attacks. The hardware vulnerabilities often targeted by attackers are SPI, UART, JTAG, USB, etc. Therefore, to enhance the security of the smart devices that permeate every aspect of our daily lives, threat modeling should be considered early in the development cycle of any system.

This past Spring semester, the Cybersecurity Assurance and Policy (CAP) Center launched a senior capstone project for electrical engineering students to study IoT device security. The primary purpose of the capstone project was to help students further develop both hardware and software skills while researching. For the project, students focused on the Arduino Mega Board. Some of the expected outcomes for the project include: 1) understand the physical board components; 2) learn how to attack the board using the STRIDE technique; 3) create a Data Flow Diagram (DFD) of the system using the Microsoft threat modeling tool; 4) understand the attack patterns; and 5) generate a threat model based on the user's input.

The goal of threat modeling is to prevent future threats and attacks from taking advantage of systems vulnerabilities. This method allows the analysis of potential attackers, including their goals and techniques, while also providing solutions and mitigation strategies. Although threat modeling can be performed throughout the development of a system, implementing it during developmental stages will enhance device security. Identifying threats and providing countermeasures will save both time and money while also keeping the consumers safe. As a result, students learn the significance of detecting and preventing attacks is to protecting consumer information systems and networks. At the end of this capstone project, students should take away hands-on skills in cyber defense.

Keywords: Internet of Things (IoT), Team Collaboration, Data Flow Diagram, Arduino Mega, Engineering education, Capstone Project, Cybersecurity Concepts.

Introduction and Motivation

Technology education is attracting big tech corporations and researchers. Unfortunately, with various Internet of Things devices available in the market, it has become challenging to rely on the security built into the actual device. Therefore, creating a large team of people with diverse skills and potential will help leverage some of the critical issues faced during the IoT device operation. Even though many universities provide engineering courses to students, some do not necessarily point out problems faced by big tech corporations. Students exposed to engineering education early will most likely have a higher chance of getting a job upon graduation. Thus, the vision of this project is to facilitate the integration of minorities into the work environment. Working on the real-life, hands-on project will increase the student's ability to be leaders at their workplace. This capstone project is centered around designing an IoT threat modeling to mitigate cyberattacks (e.g., Man in the Middle attack (MIM), Denial of Service (DoS)) during the development process of the system.

The Internet of Things (IoT) represents the physical items and machines that can connect to the Internet without requiring any humans to intervene. Internet of Things has various applications, including smart agriculture and intelligent healthcare, intelligent transportation, smart home, and smart city. Globally, over 8.74 billion IoT devices will be used in 2020 [1,2], surpassing the total number of humans on the planet. The installation of IoT devices by 2030 has a wide range of predictions. According to Statista, a German research firm, 25.4 billion IoT devices will be used by 2030 [1].

The increased number of cybercriminals exploiting IoT devices to conduct cyberattacks demonstrates the IoT's negative impact on security. According to a survey by Deep Instinct, malware usage climbed by 35.8% from 2019 to 2020, and ransomware usage increased by 43.5% [3]. There are many different types of ransomware. An example of a ransomware attack was the colonial pipeline affected by the supply of gas [4]. There was also a ransomware attack on the computer manufacturer ACER [5]. In 2016, a cyberattack also disabled access to popular websites like Twitter and Netflix [6]. Various IoT architectures and a lack of security features are the primary causes of compromised security in the IoT. To develop low-cost gadgets, manufacturers may reduce security features, resulting in insecure devices prone to hackers.

In addition, any connected device, including automobiles and appliances, is vulnerable [6]. It is easier for an attacker to manage and access multiple devices linked to the same network if a single device is compromised. Vulnerabilities are also part of the hardware; therefore, if the design is not good enough, malicious, or unauthorized parties will have access to the hardware at any production process. In this case, threat modeling can identify and mitigate security vulnerabilities protecting the target system from potential attacks. Threat modeling is a method for assessing an application's security. This capstone project outlines the process of implementing threat modeling for an IoT device at the beginning stage. The project focused on the Arduino Mega board to facilitate the learning process for the students who are just learning hardware design.

Students identify entry points that attackers could exploit to attack the Arduino Mega board. The entry points consisted of the Serial Peripheral Interface (SPI), the Universal Synchronous Receiver and Transmitter (UART), the Universal Serial Bus (USB), the Pulse-With Modulation (PWM), and the In-Circuit Serial Programming (ICSP). They then use the STRIDE threat modeling method to identify Spoofing (Authentication), Tampering (Integrity), Repudiation (Non-repudiation), Information Disclosure (Confidentiality), Denial of Service (Availability), and Elevation of Privilege (Authorization) to evaluate different threats on the Arduino Mega board.

Capstone Project Objectives

The primary purpose of this project is to get students involved in research at an early stage in their academic journey. Students engaged in research at the early phase could potentially pick up valuable hands-on expertise. Those skills can help to complete their senior design project and open many job market opportunities. Moreover, the Internet of Things innovation has been used in several domains such as transportation for smart cities, the medical sector, agriculture, and many other industries. Students working on this project will learn various skills, including communication skills, presentation mastering, writing report, critical thinking skills, teamwork collaboration, cybersecurity concepts, Internet of Things education, exposure to Microsoft threat modeling tool, self-development, self-confidence, and programming skills (e.g.., C/C++).

Related work/Literature Review

Security issues in IoT devices stem from an overall lack of standards when processing, sensing and actuating capabilities when connecting to the Internet. IoT devices typically have more features, such as pushing functionality to social networks, which produces more information [7,8,15]. Devices are a breeding ground for existing cyber threats and consist of three main layers: perception, transportation, and application. Each layer brings a security issue of its own.

Authors in [14] discovered that significant holes in the security of IoT devices leave them vulnerable to malicious attacks such as botnet attacks. Threat modeling is implemented early in the design phase to mitigate the possible threats that could occur. The threat modeling approaches used in this paper were the STRIDE and VAST methods. STRIDE involves spoofing, tampering, repudiation, information disclosure, and elevation of privilege. VAST involves visual, agile, and simple threats. A process flow diagram is created to identify the process level threats. IoT devices are divided into five zones: the IoT device zone, IoT field gateway zone, Azure zone, Cloud gateway zone, and Consumer zone. The botnet life cycle consists of (CRIME) conception, recruitment, interaction, marketing, and execution. These threats can be mitigated by limiting unused services, implementing implicit jailbreak or root detection, embedding firewalls for auditing, and encrypting traffic.

Authors in [16,17] explored the security issues in smart home devices and medical Internet of Things devices. The papers depicted some of the vulnerabilities often found in IoT devices, such as weak passwords, lack of firmware updates, and technical support. The paper carried out the Man in the middle attack to address such critical security issues and proved that IoT devices are still becoming the target for hackers despite the enhancement of the technology.

Frustaci et al. [9] discussed trust in IoT devices and how devices react to unknown entities the same way we do with human behavior. The authors covered traditional security and IoT security, which involve highly secure devices, inaccessible to everyone, containing complex algorithms. IoT devices are typically locked, so customers cannot add additional security functionality.

Dalvi et al. [10] examined the primary attack vectors in a Smart Light bulb using the threat modeling technique based on the attack tree. The tool used for this threat model is the AD (Attack Defensive) tool that represents attacks in a tree. The root indicates processes that may lead to an attack. In the attack tree described in this paper, the sub-goals are the branches, and the leaves are the threats coming from the attacker. Circles and ovals represent attack nodes, and rectangles represent defense nodes. The threat model exposed the holes in security protocols, and the attack tree showed the purpose and goal of each part of the attack vector.

Methodology

Throughout the project, student tasks were partitioned into achievable milestones to leverage the level of understanding. During the pandemic, students completed the work remotely. The Arduino Mega board was shipped to the students with their laptops to implement the capstone project. We had three different teams in total working on other milestones sessions. The teams and milestones broke down were as follow:

A -Milestone II: Threat Modeling TEAM (I, II, III)

- Explore the IoT hardware device, which is the Arduino Mega board, for this project.
- Identify different parts of Arduino Mega board ports/interfaces such as the Serial Peripheral Interface (SPI), the Universal Synchronous Receiver and Transmitter (UART), the Universal Serial Bus (USB), the Pulse-With Modulation (PWM), and the In-Circuit Serial Programming (ICSP), Wifi.
- Describe each port/interface to understand the essential function.
- Investigate the type of attacks that can be performed on each port, e.g., Man in the Middle attack, spoofing attack, and others.

B- Milestone II: Threat Modeling TEAM II

- Select at least four entry points and attacks using the STRIDE method. The entry point identified for this project is UART, SPI, ICSP, PWM, USB, and Wifi.
- Propose countermeasures to prevent the attacks discovered from the previous milestone.
- Create a Data Flow Diagram using the open-source Microsoft threat modeling Tool.
- Checkpoints to make sure the students acquired a better understanding of each task.

C- Milestone I: Common Attack Pattern Enumeration and Classification (CAPEC) - TEAM I

- Present the list of possible attack patterns related to the Arduino Board.
- Explore the attacks patterns.

D- Milestone III: Learning how to use the Pythonic Threat Modeling Framework (PyTM) to generate the Data Flow Diagram (DFD) - TEAM III

- Explore the PyTM to understand how the tool work.
- Identify the inputs to use for the PyTM tool.
- Install all the dependencies or software required for the PyTM on the student's local computer.
- Generate the Data Flow Diagram (DFD) using the PyTM tool.
- Analyze the findings threats.

Figure 1 shows the flow of the work assigned to each team member.

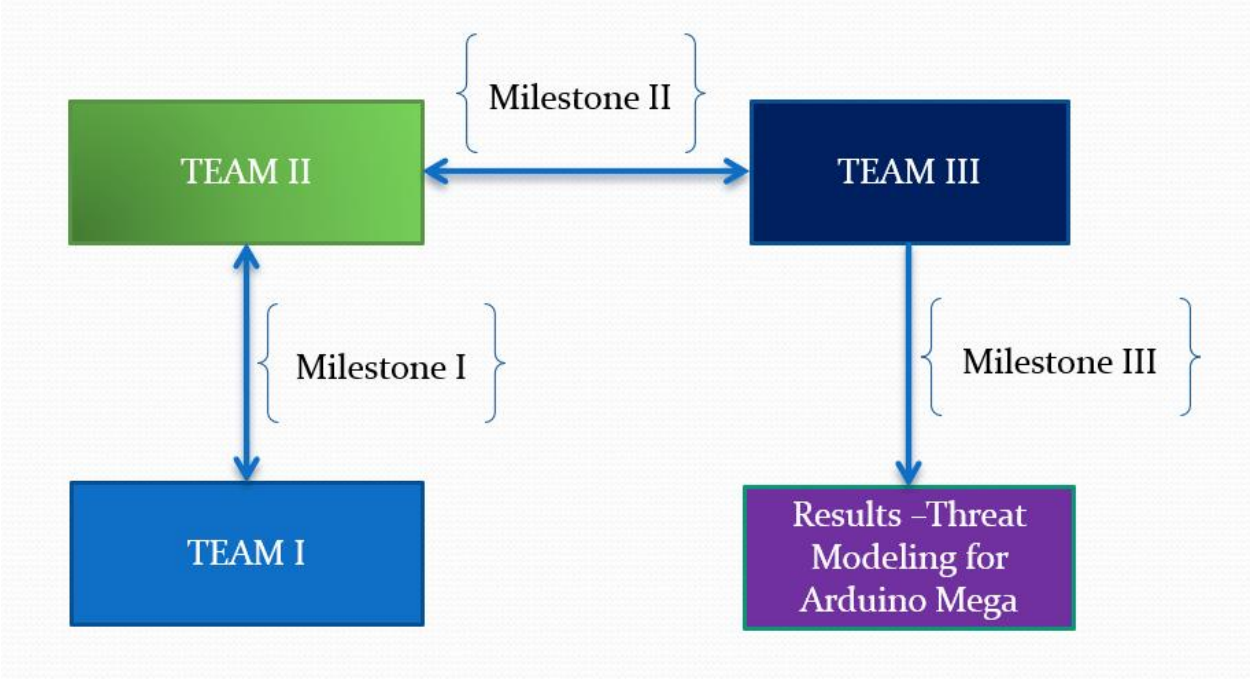

Figure 1: Flow of the work

Students Explore and Describe the hardware and software Components - TEAM (I, II, III)

The understanding of different hardware and software components were necessary for students to implement the project in-depth and included the following:

1- Arduino Mega Board

Arduino Mega model 2560 is an open-source development board with a microcontroller that is easy to program and facilitates implementing multiple basics hands-on projects.

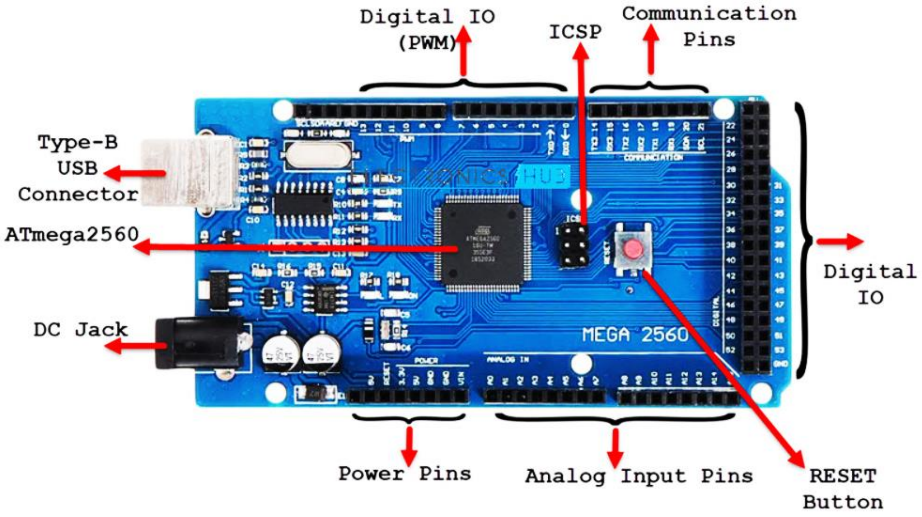

Figure 2: Arduino Mega Board Model 2560

The Arduino Mega board has multiple analog and digital inputs and outputs pins, a Universal Asynchronous Receiver and Transmitter (UART) interface, an oscillator with 16 MHz frequency, a Universal Serial Bus (USB), an In-Circuit Serial Programming (ICSP) interface, a Pulse Width Modulation (PWM) chip, a reset button, different power sources and the integrated Wifi and Bluetooth modules.

Some basics functions of the Arduino Mega components:

- Input/outputs modules are used to access and program the board to perform a specific task and output using the serial interface.
- Universal Asynchronous Receiver and Transmitter (UART) interface sends and receives data from the board. The UART module is present in any given hardware device.
- Universal Serial Bus (USB) interface allows the board to communicate with external devices.
- In-Circuit Serial Programming (ICSP) interface used to write code and program the board.
- Joint Test Action Group (JTAG) standard allows the users to access the embedded chips on the board.

- The reset button allows the users to restart the board.
- The power source (DC Jack) supplied the board with enough power during the active mode.
- Wifi and Bluetooth provide Internet connectivity.
- Pulse With Modulation (PWM) generates an analog signal from a digital source.

2- Microsoft Threat Modeling Tool - TEAM II

The Microsoft Threat Modeling tool provides a user-friendly platform for creating data flow diagrams. For threat generation, the tool employs the STRIDE approach based on the threat vector model. The Threat Modeling framework provides a list of risks that show which threat the Arduino is exposed to and explores the available mitigation options. The tool creates a threat report from the threat list as an organized document that displays all threats/mitigations in the environment. The STRIDE technique allows users to select from a variety of processes and data flows. Table 1 below indicates the STRIDE technique type, definition, and proposed mitigation approach.

Table 1: Arduino Mega Board Threat Break Down with Potential Mitigation

STRIDE	Arduino Threat	Arduino Threat Break Down	Potential Mitigation
S	Spoofing	Authentication - Attackers, assume the identity of something or someone other than themselves	Create a solid and long password that is not easily guessable
T	Tampering	Integrity - Attackers delete, change, and modify the Arduino firmware	Use digital signature to enhance the security of the board
R	Repudiation	Attackers pretend not to be responsible for the illegal action perform on the Arduino Board	The usage of the digital signature could also prevent the repudiation
I	Information disclosure	Confidentiality - Attackers have access to the data flowing through the Arduino board (Chip)	Encrypted password / encryption
D	Denial of Service	The attackers prevent the user of the Arduino board from accessing the components or services	The usage of Firewalls to block unknown data traffic
E	Elevation of Privilege	Unauthorized user accessing the board	Secure the inputs data, encryption

3- Common Attack Pattern Enumeration and Classification (CAPEC) - TEAM I

The Common Attack Pattern Enumeration and Classification (CAPEC) [13] is an online platform or database containing a list of possible attacks and patterns for any given embedded system.

List of possible attacks and the patterns:

- Access to sensitive information (CAPEC-37)

Often, attackers gain access to sensitive information by analyzing the system to find sensitive data embedded within the device. Access to such information gives attackers the power to obtain sensitive information such as private credentials or account numbers. With such information, attackers can perform a more powerful attack (Li, 2016). Hackers actualize an attack by identifying the target, applying data mining techniques, and carrying out the attack to access the information.

- Man in the Middle (CAPEC-94)

Man in the Middle attack targets communication between two components, such as the client and the server. In this case, the attackers work to gain access to the communication channel between two entities. Attackers can access information sent from the server even before it reaches the intended client. When this happens, the attacker alters the information and then sends it to the client, unaware of the potential leakage or corruption of the received information.

- Evil Twin (CAPEC-615)

Evil Twin is a type of attack related to CAPEC where the attackers install Wifi equipment that gives them access to Wifi network points. The Evil Twin attack is complex to identify because it appears as a real network access point. For instance, attackers can intercept the data traffic and analyze it from a device connected to a compromised access point.

- Eavesdropping (CAPEC-651)

Regarding Common Attack Pattern Enumeration and classification, eavesdropping is where hackers intercept communication such as texts, videos, or audio. This type of attack's main objective is to unauthorizedly gain access to sensitive data and information either for financial, political, or personal gain [11].

- Denial of Service (CAPEC-469)

Denial of service or DoS is when hackers perform flooding at the HTTP level to bring down a specific website application. DoS attack, unlike other types of attack patterns related to CAPEC, is challenging to detect. The idea behind this type of attack pattern is to keep the HTTP session alive for a very long time and then repeating it hundreds of times. When this happens, the user is unable to access the specific website application that is under attack.

- Spoofing (CAPEC-151)

Concerning Common Attack Pattern Enumeration and classification, spoofing is when hackers assume the third party's identity to accomplish their objective. For instance, the attacker may craft messages to make them seem like they come from a different principle. Also, attackers may execute this type of attack by intercepting messages from the sender, then changes the message to appear as if they come from them, but without altering the content [11,13].
Often, hackers use this technique to hijack credentials from their targets without their knowledge.

- Access to Data Logs (CAPEC-81)

Access to data logs is related to Common Attack Pattern Enumeration and Classification (CAPEC) because attackers inject, manipulate, delete, or forges suspicious log entries into the log files in the system. This type of attack intends to mislead an audit of the data logs or cover tracks of a possible attack. Attackers can execute such actions either because of the logging mechanism or insufficient access controls to the data log files.

4- Exploring the Pythonic Framework known as PyTM for Threat Modeling
The pythonic framework, also known as PyTM, is a code-based tool that gives developers the ability to automate the process of generating a threat model for any system. Students started by learning the basic requirements to install the necessary libraries or dependencies for the code to work on their computer.
Dependencies requirements for the pythonic framework:

- Linux or Mac operating system.
- An advanced version of python 3. x version and above.
- The Graphviz library is available online for free.
- Java 10 or 11 version to run the application.
- Plantuml.jar is another library for visualization.

After installing all the dependencies, students used the example code available on GitHub [12] to practice how to generate the diagram. Once they understood how the code worked, they wrote their code from scratch to create threats from the Arduino board. The results session presents the expected outcomes from the pythonic framework.

Findings/Results

Students were able to generate the Data Flow Diagram and the list of possible threats for the Arduino Mega board as shown in the diagram below:

1- Data Flow Diagram implemented with the Microsoft Threat Modeling Tool

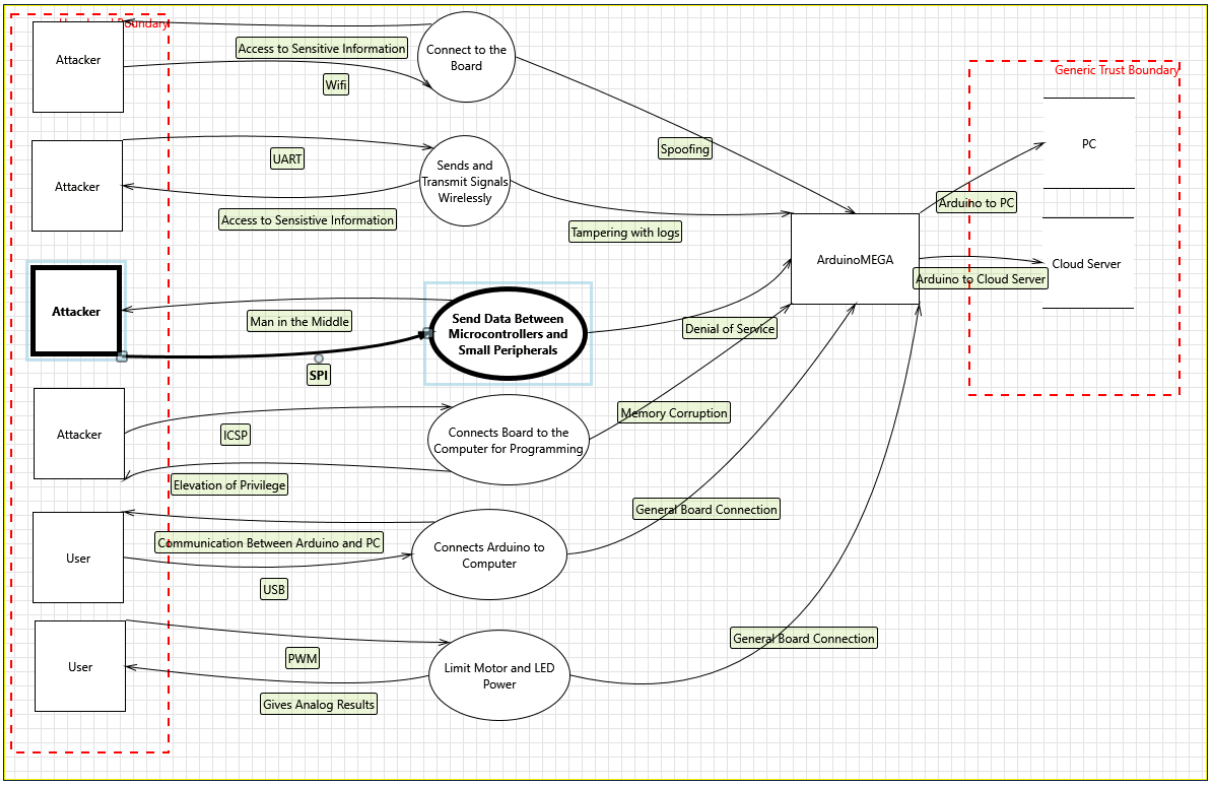

Figure 3: Data Flow Diagram of the Arduino Mega Board showing different inputs components and the corresponding threats

Validation Messages from the threat report:

- Data flow between external interactor "Arduino Mega" and data store "Cloud Server" should be avoided.
- Data flow between external interactor "Arduino Mega" and data store "PC" should be avoided.

a- External Entity Attacker Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: Medium]

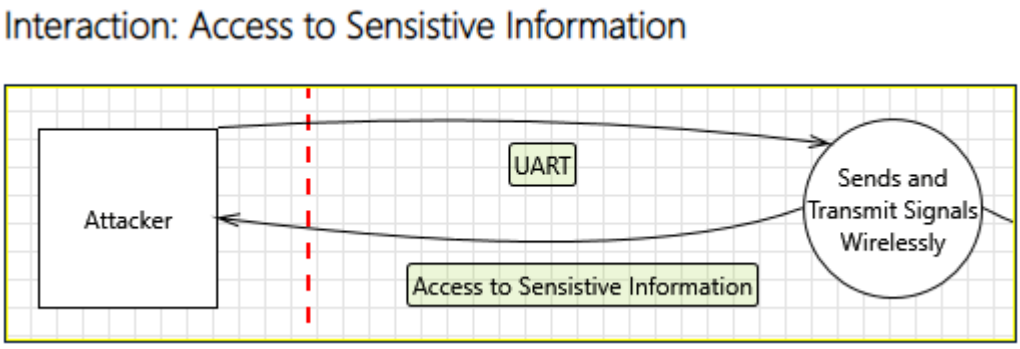

Figure 4: Access to sensitive data via UART

Table 2: Interpretation of Figure 4

Category:	Repudiation threats involve an adversary denying that something happened.
Description:	The attacker claims it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification:	Consider using logging or auditing to record the source, time, and summary of the received data.

b- Spoofing of the Attacker External Destination Entity [State: Mitigation Implemented] [Priority: High]

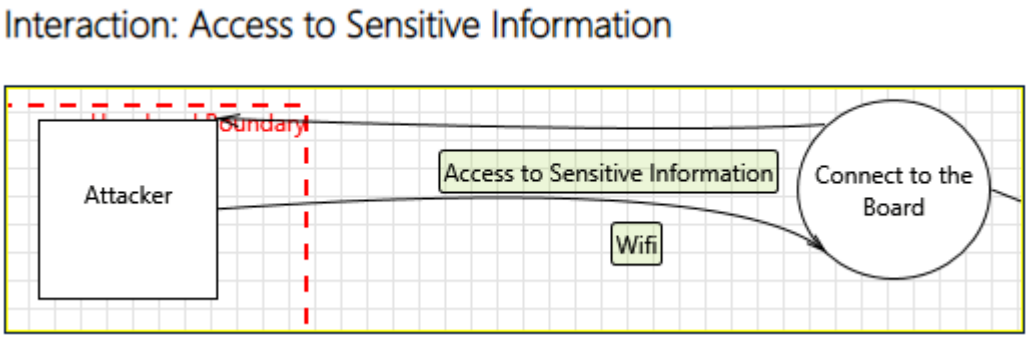

Figure 5: Access to sensitive data via Wifi

Table 3: Interpretation of Figure 5

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, a website, or a network address.
Description:	An attacker may spoof the user, sending data to the attacker's target instead of the user. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Have strong WEP/WAP encryption on access points, stronger router login credentials, or use VPN. Consider using a standard authentication mechanism to identify the external entity.

c- External Entity Attacker Potentially Denies Receiving Data [State: Mitigation Implemented] [Priority: High]

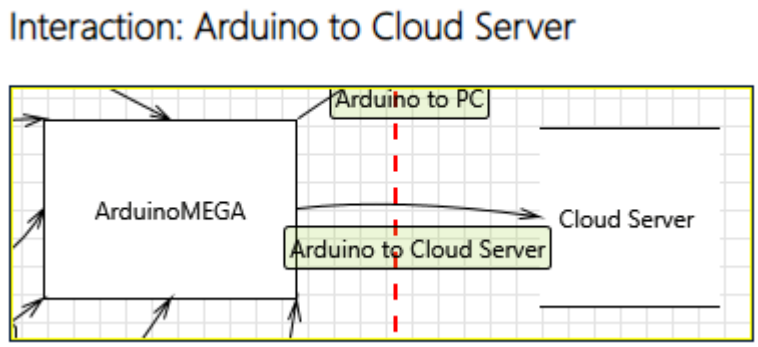

Figure 6: Data flow between Arduino to Cloud Server

Table 4: Interpretation of Figure 6

Category:	Repudiation threats involve an adversary denying that something happened.
Description:	The attacker claims it did not receive data from a process on the other side of the trust boundary. Consider using logging or auditing to record the source, time, and summary of the received data.
Justification:	Encourage secure logging so we can record if the user received the data.

d- Spoofing of Destination Data Store Cloud Server [State: Mitigation Implemented] [Priority: High]

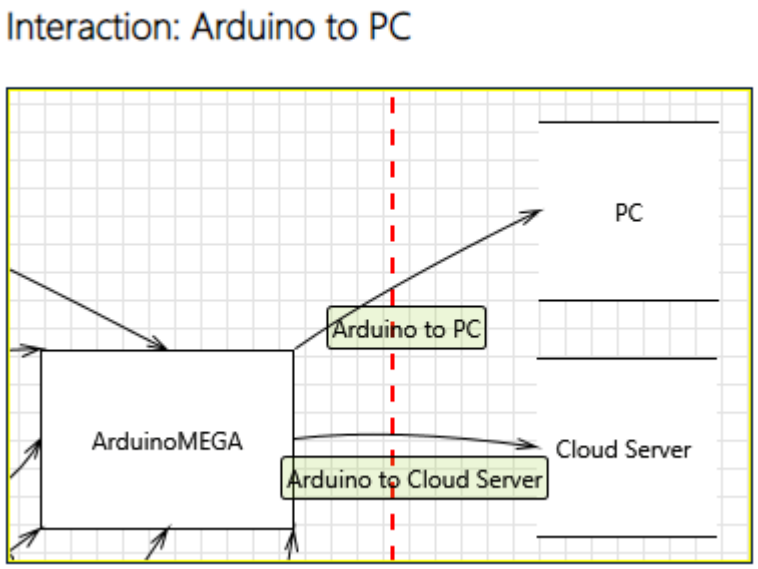

Figure 7: Interaction between Arduino and the PC

Table 5: Interpretation of Figure 7

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, a website, or a network address.
Description:	An attacker may spoof the cloud Server, directing data to the attacker's target instead of the Cloud Server. Consider using a standard authentication mechanism to identify the destination datastore.
Justification:	Use authentication to make the user identify themselves before the data store.

e- Spoofing of Destination Data Store PC [State: Mitigation Implemented] [Priority: High]

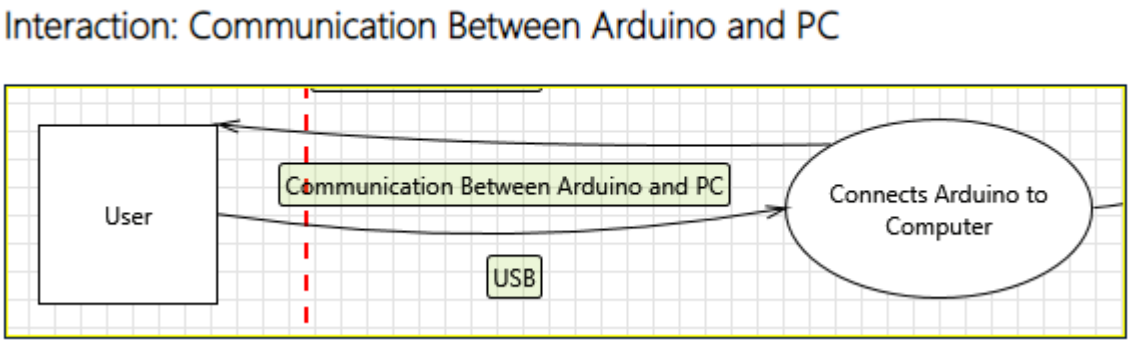

Figure 8: Communication between Arduino and PC

Table 6: Interpretation of Figure 8

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, a website, or a network address.
Description:	An attacker may spoof the PC sending data to the attacker's target instead of the PC. Consider using a standard authentication mechanism to identify the destination datastore.
Justification:	Establish user authentication when connecting to the PC datastore.

f- Data Flow Generic Data Flow Is Potentially Interrupted [State: Not Applicable] [Priority: Low]

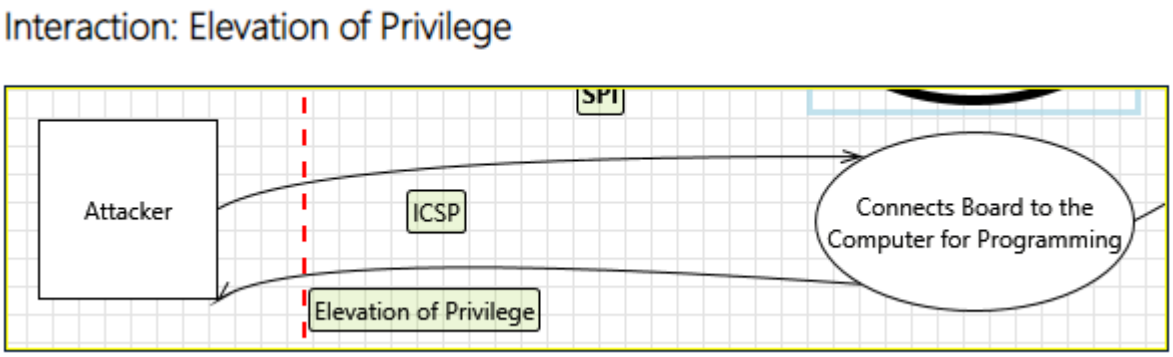

Figure 9: Elevation of Privilege on the ICSP port

Table 7: Interpretation of Figure 9

Category:	Denial of Service happens when the process or a datastore cannot service incoming requests or perform up to spec.
Description:	An external agent interrupts data flowing across a trust boundary in either direction.
Justification:	The Denial of Service is an example authenticated user with no intentions of attacking the board.

g- Spoofing of the User External Destination Entity [State: Mitigation Implemented] [Priority: Medium]

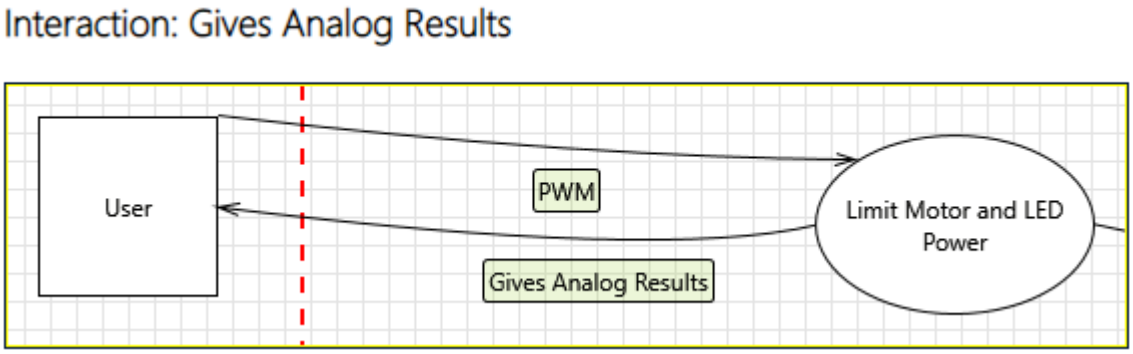

Figure 10: Spoofing via the Pulse Width Modulation Interface

Table 8: Interpretation of Figure 10

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, a website, or a network address.
Description:	The attackers may use spoofing, directing data to the attacker's target instead of the user. Consider using a standard authentication mechanism to identify the external entity.
Justification:	Establish user authentication

h- Spoofing the Connects Board to the Computer for Programming Process [State: Mitigation Implemented] [Priority: High]

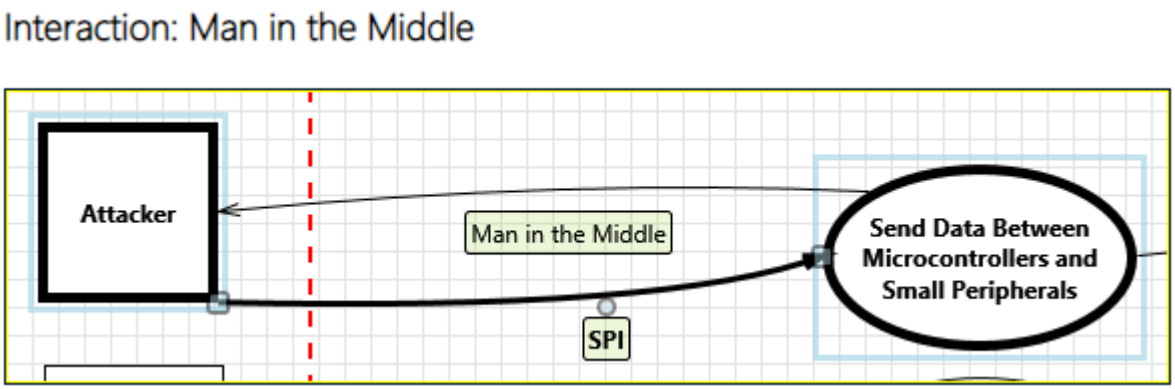

Figure 11: Man in the Middle Attack

Table 9: Interpretation of Figure 11

Category:	Spoofing is when a process or entity is something other than its claimed identity. Examples include substituting a process, a file, a website, or a network address.
Description:	Connects board to the Computer for Programming may be spoofed by an attacker, leading to information disclosure by a user. Consider using a standard authentication mechanism to identify the destination process.
Justification:	Establish user authentication.

2- Generating Threats for Arduino Mega Board using a Sequential Diagram

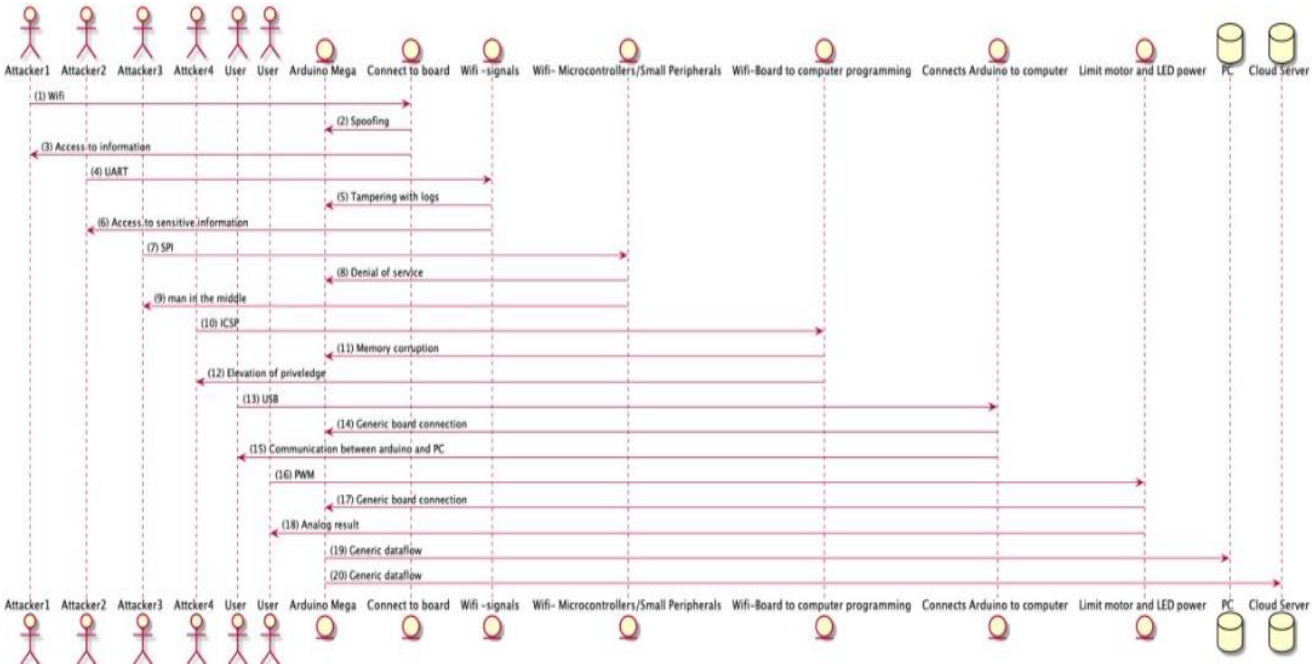

Figure 12: Generating Threat for Arduino board

Figure 12 shows a step-by-step process of how the attackers will enter the Arduino board and gain control or perform an attack. The diagram starts with the board's entry points and then provides the attack according to the board components and priority.

Takeaways and Program Learning Experiences

The capstone project has exposed students to the threat modeling technique and a new insight into the security used in hardware devices. The project examined the Arduino Mega board (IoT device) and found possible hardware threats through threat modeling. To do that, students had to understand the device on a deep level. The methodology encourages to familiarize with the device and learn different functions, both software and hardware. Students learned how an attacker could gain access to entry points and secure systems using the attacker's perspective, making it easier to know what preventative measures to implement.

To understand how an attacker can manipulate the hardware/devices, students had to get familiar with essential Arduino Mega entry points such as UART, SPI, PWM, and USB. Ironically, students noticed that an innovative device with many capabilities makes it more susceptible to attacks than a more specific device. Throughout the research, students learned about threat modeling implementation, cybersecurity threats and concepts, Microsoft Threat Tool, research techniques, presentation skills, experience with python code, teamwork experience.

Discussions and Challenges faced throughout the project

Once students were aware of all the possible entry points in the Arduino board, they focused on three significant aspects of the project that helped generate the findings into a model: CAPEC, Data Flow Diagram, and the threat model for the Arduino board through the sequential diagram. CAPEC acts as a threat library with common attack patterns that expose the complexity and likelihood of the attack occurring on the board. The Data Flow Diagram and Sequence Diagram show a step-by-step process of how the attacker can enter any system and gain control or perform an attack. The diagrams are very user-friendly and help to show the findings to an audience that lacks security awareness.

Students had to do some basic research to understand how the Arduino board function using the schematics provided. The schematics detailed all the features available on the board and how to program. Students found that every element matters in the device because attackers could easily exploit the one that got ignored. They realized that programming follows the principle of trial, error, and debugging.

Capstone Project Timeline

Tasks	February 2021	March 2021	April 2021	May 2021
Research on Threat Modeling				
Research on CAPEC				
Research on Microsoft Tool				
Order the Arduino Mega board				
Explore the entry points of the board				
Describe each port/interface to understand the essential function				
Investigate the type of attacks that can be performed on each port				
Choose relevant interfaces for Arduino Mega board four minimum				
Propose countermeasures to prevent the attacks				
Understand how to generate the DFD				
Generate the Data Flow diagram				
Generate the found threats				
Check the progress				
Provide a list of possible attack patterns related to the Arduino Board				
Explore the attacks patterns				
Explore the PyTM to understand how the tool work.				
Identify the inputs to use for the PyTM tool				
Generate threats for the board based on user input				
Install all the dependencies or software				
Analyze the findings threats				
Draft Proposal				
Draft Project Report				
Draft Presentation				
Final Revisions				

Color Code

Color Code
Yellow = Task completed by TEAM I
Pink = Task achieved by TEAM II
Blue = Task completed by TEAM III
Orange = Task completed by TEAM I, II, III

Hardware Components Budget

Budget	
Materials	Cost $
Arduino Mega board(hardware)	$30
EVO select SD card 256gb	$40
USB power cable	$15

Capstone Project Formal Assessment and Criteria

This capstone project involved undergraduate students from the Department of Electrical and Computer Engineering (ECE) working together to complete the work. This project aims to provide students the opportunity to learn how to solve real-world problems and collaborate with their peers as a team. Many students exposed to project at the early stage would eventually succeed at the industrial level as well. Table 10 describes the criteria used to evaluate the work at the end of the project.

Table 10: Capstone Project Evaluation Criteria

Position in the ECE	Tasks	Contributions	Assessment Criteria
ECE Faculties (2)	- Project advisors -IoT Security Professor - Associate professor -Point of Contact for the project	-Provide thoughts on designing the capstone project. -Provide feedback to enhance the activities. -Graduate mentors faculty advisor. -Provide the equipment to experiment.	Not Applicable (N/A)
Graduate Mentors Ph.D. students	Project Mentors	-Engage students to get started with the work. -Schedule a daily meeting to assist students. -Provide a research paper to facilitate the understanding of the project. -Monitor the progress of each student in the team. -Provide feedback to each student in the team. -Facilitate collaboration with students.	-Friday's meeting presentation with the current progress of the work and the next phase. -Check to see if the students comprehend the project. -Check the final report submitted by the team.
Undergraduate students in the Electrical and	Project Mentees	- Read at least one research paper per day and present it to the group.	-Weekly presentation.

Computer Engineering (ECE) Department		- Provide daily updates to the team. - Explore the Arduino board components to understand the functionality. - Contribute to designing the threat modeling to identify and mitigate the threat in the IoT Hardware design.	-Problem-solving skills. -Presentation mastering. -Final project report and accomplishments

Conclusion and Future Work

At the end of this capstone project, students were able to show that threat modeling can be used to mitigate vulnerabilities in an IoT device. But how could this be applied in a situation with multiple IoT devices? Threat modeling has the potential to go even further to secure multiple devices in an intelligent home setting. Realistically, the average person will own various IoT devices inside their home without realizing the basic functionalities. IoT devices are highly susceptible to cyber-attacks making a homeowner set in an unsafe environment. Students used threat modeling to analyze the Arduino board, but it can expand to map out the security posture of an entire system of devices using the same methodology. In the case of devices in an intelligent home, students would start focusing on the cloud capabilities, the software, and hardware. Having our threat model target different capabilities will give us a more detailed outlook on the system's complexity while bringing forth new threats that may have gone overlooked. With this capstone project, students are able to learn some in-demand hands-on skills while gaining experience working as a team. The project also motivates students to become critical thinkers, leading to job market opportunities.

Acknowledgement

The authors of this work would like to thank the anonymous reviewers for their valuable time and comments. We also would like to appreciate the Center for Reverse Engineering and Assured Microelectronics (CREAM) Research Laboratory, and the Cybersecurity Assurance and Policy (CAP) Center for their support.

References

[1] A. Holst, "IoT connected devices WORLDWIDE 2019-2030," Statista, 25-Aug-2021. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices worldwide/#:~:text=The%20number%20of%20Internet%20of,China%20with%203.17%20billion%20devices. (Statista Research Department, "IoT: number of connected devices worldwide 2019-2030," Statista. [Accessed: 20-Sep-2021].

[2] "NTT data study finds 2 out of 3 consumers would switch insurers to get discount for using smart home devices," *NTT*. [Online]. Available: https://us.nttdata.com/en/news/press-release/2017/january/ntt-data-study-finds-2-out-of-3-consumers-would-switch-insurers. [Accessed: 20-Sep-2021].

[3] Help Net Security February 17, Help Net Security, and F. 17, "Malware increased by 358% in 2020," *Help Net Security*, 15-Feb-2021. [Online]. Available: https://www.helpnetsecurity.com/2021/02/17/malware-2020/. [Accessed: 21-Sep-2021].

[4] S. M. Kerner, "Colonial pipeline Hack EXPLAINED: Everything you need to know," *WhatIs.com*, 07-Jul-2021. [Online]. Available: https://whatis.techtarget.com/feature/Colonial-Pipeline-hack-explained-Everything-you-need-to-know. [Accessed: 21-Sep-2021].

[5] L. Abrams, "Computer giant Acer hit by $50 million ransomware attack," *BleepingComputer*, 20-Mar-2021. [Online]. Available: https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/. [Accessed: 20-Sep-2021].

[6] K. Moskvitch, "Securing IoT: In your smart home and your connected enterprise," in Engineering & Technology, vol. 12, no. 3, pp. 40-42, April 2017, doi: 10.1049/et.2017.0303.

[7] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "STRIDE-based threat modeling for cyber-physical systems," 2017 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2017, pp. 1-6, doi: 10.1109/ISGTEurope.2017.8260283.

[8] B. Bokan and J. Santos, "Managing Cybersecurity Risk Using Threat Based Methodology for Evaluation of Cybersecurity Architectures," 2021 Systems and Information Engineering Design Symposium (SIEDS), 2021, pp. 1-6, doi: 10.1109/SIEDS52267.2021.9483736.

[9] M. Frustaci, P. Pace, G. Aloi, and G. Fortino, "Evaluating Critical Security Issues of the IoT World: Present and Future Challenges," in *IEEE Internet of Things Journal*, vol. 5, no. 4, pp. 2483-2495, Aug. 2018, doi: 10.1109/JIOT.2017.2767291.

[10] A. Dalvi, S. Maddala and D. Suvarna, "Threat Modelling of Smart Light Bulb," 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), 2018, pp. 1-4, doi: 10.1109/ICCUBEA.2018.8697723.

[11] Li, T., Paja, E., Mylopoulos, J., Horkoff, J., & Beckers, K. (2016, June). Security attack analysis using attack patterns. In *2016 IEEE Tenth International Conference on Research Challenges in Information Science (RCIS)* (pp. 1-13). IEEE.

[12] Izar, "Izar/Pytm: A pythonic framework for threat modeling," *GitHub*. [Online]. Available: https://github.com/izar/pytm. [Accessed: 25-Sep-2021].

[13] "Common attack pattern enumeration and classification," *CAPEC*. [Online]. Available: https://capec.mitre.org/. [Accessed: 25-Sep-2021].

[14] S. G. Abbas, S. Zahid, F. Hussain, G. A. Shah and M. Husnain, "A Threat Modelling Approach to Analyze and Mitigate Botnet Attacks in Smart Home Use Case," 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE), 2020, pp. 122-129, doi: 10.1109/BigDataSE50710.2020.00024.

[15] O. Toutsop, P. Harvey and K. Kornegay, "Monitoring and Detection Time Optimization of Man in the Middle Attacks using Machine Learning," 2020 IEEE Applied Imagery Pattern Recognition Workshop (AIPR), 2020, pp. 1-7, doi: 10.1109/AIPR50011.2020.9425304.

[16] Toutsop, Otily and Das, Sanchari and Kornegay, Kevin, Exploring the Security Issues in Home-Based IoT Devices Through Denial of Service Attacks (October 18, 2021). IEEE International Conference on Smart City Innovations.

[17] P. Harvey, O. Toutsop, K. Kornegay, E. Alale and D. Reaves, "Security and Privacy of Medical Internet of Things Devices for Smart Homes," *2020 7th International Conference on Internet of Things: Systems, Management and Security (IOTSMS)*, 2020, pp. 1-6, doi: 10.1109/IOTSMS52051.2020.9340231.