**STEM Outreach - SCADA Home Security**

**(Formerly SCADA Home Automation)**

**Progress Report 5**

**2023-03-28**

**Team Members:**

* Jon Beason - Team Lead/Cybersecurity Engineer
* Chad G Bryan - Computer Engineer
* Ben Calvert - Cybersecurity Engineer
* Ben Curths - Computer Engineer
* Simone Gbouomou - Cybersecurity Engineer
* Ben McAnulty - Cybersecurity Engineer

**Project Summary:**

The SCADA Home Security project will design and develop an interactive physical model that simulates some common components in today’s smart home systems and demonstrates how those systems may be vulnerable to malicious actors via targeted cyberattacks. This model aims to educate and generate interest in cybersecurity amongst prospective students and young professionals entering the field by clearly demonstrating the physical effects of real-world vulnerabilities created by digital cyberattacks.

To accomplish this demonstration, the project will incorporate microcontrollers, including two Raspberry Pis and an Arduino running the open-source ScadaBR and OpenPLC software packages. The ScadaBR device will connect to an LCD panel to serve as a human-machine interface. The OpenPLC devices will be connected to and manage the external sensors and actuators that simulate the common home automation components. These simulated components will include an IR sensor for alarm and intrusion detection, an electronic lock for access control, a DC-motor-controlled door for remote opening/closing, and LED lighting for model illumination and status indication. The final objective is to have the demonstration participant launch preloaded cyber-attacks and exploits from an attached device to change the model state without using the embedded HMI.

**Current Project Status:**

The goals over the last sprint were mostly completed. Progress on the model has continued to improve. The construction of the interactive buttons has been completed, and the led buttons have been soldered. All that remains is integrating the button housing into the model and connecting it to the microcontroller. The diffusers that were added have been removed due to them restricting too much light flow and causing the lights to look washed out. The construction of the Garage Door is currently around 75% completed. The addition of the coupling to connect the motor to the door will allow us to dial in the operation of the door. The front door is currently 70% completed with the construction of the door frame remaining. Over the last sprint we were able to get the DC motor and the locking solenoid to operate on a single H-Bridge by changing the power source.

The progress on the right panel has somewhat remained the same. The motion sensor has been reworked to allow the component to be displayed and at the same time restrict the motion sensor from accidentally being triggered. The magnetic sensor housing was also constructed and integrated into the right panel. All that remains on the right panel is integrating the deadbolt and attaching the Garage Door transmitter and receiver. We are also currently discussing the removal of the uno controller from the right panel and running it using the Raspberry Pi 3B but testing will need to be conducted to determine the best route.

On the cybersecurity side of the project over the last sprint we were able to solve the issues we were experiencing with the network switch. We were also able to successfully perform the ARP Poisoning attack on the LAN. During the last sprint we were also able to develop a mitigation script that will update the OpenPLC and ScadaBR Pis and mitigate the ARP Poisoning attack. By performing the ARP Poisoning attack we are now able to intercept network traffic between the PLC and the HMI. This will allow us to start developing our second cybersecurity attack and mitigation.

**Problems/Solutions**

1. **Pull Up Resistor** ­– A pull up resistor is required for the magnetic sensor and the IR sensor on the model and the magnetic sensor on the right panel.

**Solution A**: Develop a small circuit board for the pull up resistor that will allow us to easily connect the components to a pull up resistor.

**Solution B**: Not ideal but we could hardwire a jumper between the power and the signal using a resistor to create.

**Goals for the next Sprint**

The goals for the next sprint are to finish the Right panel by integrating the remaining components such as the commercial electronic deadbolt, various buttons and then attach the garage door remote. For the home model the goals are to finish the third floor by constructing the anti-theft sensor and adding various push buttons in the home model. Finish constructing the garage door and attach it to the model and finish the front door construction and install it on the model. In addition, over the next sprint we need to develop the second attack and a mitigation. We will also begin the development of the HMI graphical which will include custom images to provide a custom interface for the users to interact and monitor the system.

**Team Assignment**

Jon Beason – Finish building garage door and front door. Start creating graphics for HMI

Chad Bryan –

Ben Calvert – work on integrating the (LL) Ladder Logic unit into the master LL program. Start creating the second attack and mitigation.

Ben Curths – Finish analysis of the deadbolt signals and integrate the deadbolt into the LL program.

Simone Gbouomou – work on integrating the (LL) Ladder Logic unit into the master LL program. Start creating the second attack and mitigation.

Ben McAnulty – work on integrating the (LL) Ladder Logic unit into the master LL program. Start creating the second attack and mitigation.

**Individual Responsibility Record:**

* Jon Beason – 25 hours – Research LAN issues and how to implement ARP Poisoning attack, rework the right panel motion sensor, made magnetic sensor housing for right panel, made push buttons for home model, Created progress report.
* Chad G Bryan -
* Ben Calvert - 20 hours – Helped develop LAN functionality, cyberattacks, and mitigations.
* Ben Curths – 5 hours – Finished breakout and resoldering of deadbolt wiring.
* Simone Gbouomou –3 hours Researched on how to implement ARP Poisoning.
* Ben McAnulty - 10 hours - Researched and helped develop LAN functionality, cyberattacks, and mitigations.