**STEM Outreach - SCADA Home Security**

**(Formerly SCADA Home Automation)**

**Progress Report 4**

**2023-03-21**

**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. Some issues arose during the sprint that caused some of the sprint goals to not be met. As of this progress report, the construction of the exterior case has been completed. During the last sprint, pass-throughs have been added to the back of the case to supply power to the components and to allow connection points for the LAN via ethernet and a USB port to connect the home model. The case also had some minor repairs that had to be made from the exterior sheathing releasing from the structural frame. This was due to an insufficient amount of adhesive that was applied in a few sections. The sections have been repaired and tested to ensure proper adhesion. A second coat of paint was also applied to the exterior case and the inside of the exterior case was also painted to give an uniformed look.

The right interior panel is currently about 70% complete. Since the last sprint the IR sensors box has been constructed to house the sensor and has been attached to the right panel. The IR sensors have also been tested to ensure the component is still functioning as desired. The Motion sensor has also been attached to the ride side panel but a problem has arisen due to the motion sensor being highly sensitive. The issue that will be discussed further in the “Problem/Solution” section. Wood strips have been attached to the back of the foamboard to allow the HMI monitor to be securely attached to the right panel. Progress is being made on integrating the consumer smart lock into the system. We have been able to observe the signals for the deadbolt motor and drive it using external signals from the microcontroller, but the locking device relies on lever position sensors that act as limit switches for the motor. These are currently inaccessible, but the next step will involve a further teardown of the device to examine the structure and usability of the sensors.

The progress on the home model has improved over the last sprint. Windows have been added to the back panel of the model to give a uniformed appearance. Lighting has been added to the model including the back window panel and is currently 90% completed. Once lights are added to the first floor the lighting will be 100% completed. Additional light diffusers were added to the windows to improve the distribution of light emitted from the LEDs. The white and green lighting has been integrated to the second floor of the model and the magnetic sensor and the motion sensor has been added as well bringing the second floor to 95% completed. The third floor has also had white and green lighting added and the IR sensors have been integrated bringing the third floor to 80%. There was an issue with the IR sensors that delayed the progress of the home model. The construction of the garage door is currently 80% completed but an issue was encountered that has paused progress. The circuit for the garage door has been created and is working using ladder logic. The construction of the front door has started and is expected to be completed over the next sprint.

The attacking VM has been downloaded and has been set up. This includes downloading all the necessary tools needed to read network traffic and to develop attacks. OpenPLC and ScadaBR have been reinstalled on the Raspberry Pis and are communicating to each other via Modbus. During the last sprint we encountered some problems with setting up the LAN that has delayed us getting the local network set up.

**Problems/Solutions**

1. **Motion Sensor** ­– The sensitivity of the motion sensor is too high even when it has been turned all the way down to use pointing out on the right panel.

**Solution**: A momentary push button will be added to restrict the motion sensor from working until it is activated by the user.

2. **IR Sensor** – Two of the Four sets of IR sensors appeared to be broken because they did not function when connected in the manner as the working sets. Two additional sets were ordered and seemed to arrive broken as well.

**Solution:** After about 10 hours of researching and tinkering some of the IR sensor sets require a pull up resistor to work and other sets do not. A pull up resistor will be integrated with the IR sensors to ensure proper functionality.

3. **Green LEDs:** – The original green diffused LEDs that came with the pack of assorted LEDs was too weak to give the desired appearance.

**Solution:** Super bright green LEDs were ordered and integrated to provide the desired appearance.

4. **Small solenoid:** The Arduino has insufficient voltage to power the DC TT motor used for the garage door and the solenoid used to emulate the door lock.

**Solution A:**  Possible solution would be to add an external 9V power supply to provide additional power to drive the small locking solenoid.

**Solution B:**  Redesign the lock for the front door to allow for the less power hungry tt motor to be used.

5. **LAN Switch:** The switch does not broadcast packets like we were expecting and may cause an issue with being able to capture and read the MODBUS packets.

**Solution:** May need to order a different hub/switch but we are going to test to see if we can capture packets transferred through the switch using Wireshark, or consider swapping our MiTM attack for another.

6. **Smart Lock:** Control signals from the logic board of the device, including the lever position sensor signals, are not currently accessible without further, potentially destructive, dismantling of the device.

**Solution:** A spare lock assembly has been ordered to provide insurance against destruction. With this as security, we have begun modifying the wire assembly within the lock to better access the control signals for monitoring, interception, and possibly replication.

**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, magnetic sensor, 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 finish setting up the LAN and start developing the ARP Poisoning attack and the Modbus flood attack. This will include developing the mitigations to prevent the attacks. 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, Work on Ladder Logic program for the Model.

Chad Bryan – create garage door circuit using micro switch, DC motor and RF receiver, integrate first floor LED lights.

Ben Calvert – reinstall OpenPLC and ScadaBR on the Pi 3 B+, Paint exterior case, LAN setup.

Ben Curths – integrate small locking solenoid with Smart deadbolt to create front door circuit,

Simone Gbouomou – Research ARP poisoning attack, Work on Ladder Logic program for the right panel.

Ben McAnulty – Research Modbus flooding attack, Finish LAN setup and test to see if Modbus traffic can be intercepted.

**Individual Responsibility Record:**

* Jon Beason - 60 hours - soldered and installed LED lights, constructed and installed IR sensor housing in the home Model and Right panel, added wood strips to the right panel to securely attach the monitor. Built and installed motion sensor in the model and right panel. Started building the garage door model. Install passthroughs for power, USB and ethernet.
* Chad G Bryan - 10 hours - Got DC motor for garage door to flip polarity in openPLC
* Ben Calvert - 6 hours - Re-installed and configured Raspbian for Pi’s
* Ben Curths – 5 hours - Teardown and analysis of smart lock device
* Simone Gbouomou - 5 hours - Installed Kali VM, Downloaded additional tools for attacks
* Ben McAnulty - 6 hours - LAN setup