**STEM Outreach - SCADA Home Security**

**(Formerly SCADA Home Automation)**

**Progress Report 2**

**2023-02-21**

**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:**

As of this report, all parts have been ordered/received and tested to ensure they work correctly. The exterior case is currently 90% complete. Since the last progress report, locking latches have been added to the case to keep it close during transportation, and stabilizer feet have been added to the bottom to allow the case to be adjusted if needed. In addition, the case has been sanded and prepped for paint, and a test sample has been painted to test for proper adhesion before painting the exterior case. The progress on the home model has been going well, and it now looks more like a building than a box. This was aided by the front windows and trim that were added to the building during the current sprint. The component layout has been decided, and the process of integrating the sensors into the model can begin. Over the duration of the current sprint a number of system components have been connected to OpenPLC and are working correctly. These components include the following: IR sensor, motion sensor, the RF transmitter and receiver, and the DC motor. Radzio Modbus Master is also being used to check the input/output signals being transferred via Modbus. Despite the progress that was made during the current sprint, the team did not meet their goals of completing the exterior case or integrating the right interior panel. This is mainly due to the time that needed to be dedicated to fixing the teams’ presentations and the handles and access panel for the case stopping the progress on the right interior panel. These issues encountered will be discussed further in the next section. The team was still able to progress the project forward in other areas.

**Problems/Solutions**

1. Magnetic Sensor – The magnetic sensor does not work with OpenPLC consistently. Majority of the time the magnetic sensor does not work with OpenPLC. When it does work the input signal does not provide the expected behavior. Instead of receiving a constant signal when the two halves are separated the signal is more attuned to a pulse. The magnetic sensor was also tested using an Arduino sketch and the expected behavior was achieved. The results of the magnetic sensor not working correctly in OpenPLC has meant we had to reevaluate the component layout for the right panel and has contributed to the right panel's integration being delayed.

**Solution**: Spoke to Dr. Coe on Monday 2/20/2023 about the issues we are encountering with the sensor, and he said we could eliminate it since we have enough additional functionality to provide a robust experience. So as of now the Magnetic Sensor is no longer being used in the model but depending on time could be circled back to.

2. Case Handles – Determining the best carrying handle for the exterior case that will be durable and comfortable has taken longer than expected.

**Solution:** We determined that a heavy duty duffle bag handle would allow the handles to be moved out of the way easily and allow the handle to fit comfortably in the hand.

3. No access to the right rear panel – During the process of designing the layout of the right interior panel we determined the current design did not allow for easy access to the components in the back of the right panel.

**Solution:** We determined that an access panel should be added to the back of the exterior case to allow for easy access to components and to allow for easy setup.

**Goals for the next Sprint**

The primary goals for the upcoming sprint are to complete the exterior case by adding handles, access panel, corner guards and paint the exterior case. For the home model the goals include integration of white/green LED lights, IR Sensor, Motion Sensor, and building the garage door and front door. For cyber the goals are to reinstall OpenPLC and ScadaBR on the Raspberry Pi 3B+ that have been donated to the project by the ECE department and set up the LAN so vulnerability testing can start. In addition, the cyber team will set up the “Attack VM” by downloading the tools needed such as Wireshark, Python 3, and the Modbus library “PyModbus” that will be used to develop attacks. Dr. Coe mentioned that an ARP Poisoning attack would be easier to perform than an DOS attack and suggested how we could mitigate it, so the cyber team will need to do further research during the next sprint. Dr. Coe also mentioned speaking with Dr. Wells about obtaining a copy of the “Diamond Vault” project so the cyber team can see what attack and mitigation strategies were used for the previous project.

**Team Assignment**

Jon Beason – topical seminar, build model garage door/ front door, cut access panel, and install handles, integrate motion sensor.

Chad Bryan – topical seminar, create garage door circuit using micro switched, DC motor and RF receiver, integrate LED lights.

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

Ben Curths – topical seminar, integrate small locking solenoid with Smart deadbolt to create front door circuit, integrate LED lights.

Simone Gbouomou – topical seminar, Setup attack VM by installing the tools needed, research ARP poisoning attack,

Ben McAnulty – topical seminar, research ARP poisoning mitigation, setup LAN.

**Individual Responsibility Record:**

* Jon Beason - 44 hours – mainly working IDR, writing progress report, added windows and trim to home model, added locking latch and stabilizer feet to case, got RF remote/receiver working with OpenPLC & Radizo Modbus and troubleshooting magnetic sensor.
* Chad G Bryan - 10 hours - IDR, worked on DC motor, magnetic sensor, IR Sensor, and motion sensor utilizing Open PLC logic
* Ben Calvert - 15 hours - IDR, helped with troubleshooting magnetic sensor, prototyping OpenPLC installations and functionality
* Ben Curths - 6 hours - IDR, testing and troubleshooting of magnetic switch, IR beam, and PIR sensors, integration of slave PLC board with host PLC board.
* Simone Gbouomou -7 hours- IDR, OpenPLC installation and functionality, prototyping.
* Ben McAnulty - 10 hours - IDR, prototyping OpenPLC installations and functionality