**STEM Outreach - SCADA Home Security**

**(Formerly SCADA Home Automation)**

**Progress Report 3**

**2023-03-07**

**TeamMembers:**

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 progress on the building model and the exterior case was not as productive as the two previous sprints, but this is mainly due to the sprint falling on the same week as midterms. In addition, the team’s topical seminar presentation was scheduled during the last sprint, so the majority of the free time allotted to work on the project was used to finish/practice the presentation. Despite having limited time to work on the actual project, some progress was made. The slots for the carrying handles were cut in the side of the case and the handles have been attached. External force was applied to the handles that exceeded normal conditions to test that the handles had been securely attached and could support the load. The access panel was eliminated during the sprint in favor of using a pass through for the power and ethernet. The location for the components has been laid out for the right-side panel and the hole for the HMI screen has been cut. The housing for the alarm has been constructed and the alarm has been attached to the panel. Layers of foam board have been laminated together to equal the thickness of a door for the electric deadbolt to be attached to.

Testing and prototyping of both the ladder logic and OpenPLC and ScadaBR configurations has been largely completed. The master-slave device pairing has been successfully demonstrated with the program running on the Pi able to control the Arduino I/O. Additionally, Modbus I/O addressing has been mapped for our intended Pi-Arduino configuration, and ScadaBR has been installed and is successfully communicating with OpenPLC via Modbus. With this experience in place, we are ready to begin the integration of the final components into the case.

There were a few problems that were encountered during the sprint that are discussed below in the problems section.

**Problems/Solutions**

1. **HMI** ­– The monitor used for the HMI can not be attached directly to the right panel because foam board was used to construct the right panel. The foam board helped to keep weight down but doesn’t allow screws to be used to attach components.

**Solution**: A strip of wood or possibly something else will need to be glued to the foamboard that will allow screws to be used.

2. **Case Handles** – The slots that were cut for installing the carrying handles ended up being slightly larger than the handles.

**Solution:** The access space was filled and sanded to create a smooth surface for painting.

3. **Apache Tomcat Server Errors** – The Tomcat server that provides the backend of ScadaBR entered an error state in which previously functioning communications with OpenPLC repeatedly failed. The root cause of the problem could not be identified.

**Solution:** A restart of the Tomcat server and ScadaBR corrected the error state, but it is not currently known whether this will be a recurring issue or a one-time incident due to external software conflicts. Further testing is needed to determine the severity of this issue and whether it is something that will need to be accounted for in the design.

**Goals for the next Sprint**

The primary goals for the upcoming sprint have largely been carried over from the last sprint. They are to complete the exterior case by adding the passthrough for the power and ethernet, complete the right side panel by attaching the rest of the components, and create the ladder logic program to control the devices. 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 a 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 mentioned that we should obtain 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 – build model garage door/ front door, integrate lights and IR Sensor.

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

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

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

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

Ben McAnulty– research ARP poisoning mitigation, setup LAN.

**Individual Responsibility Record:**

Jon Beason - 15 hours – mainly working on the topical seminar, cut slots for carrying handles and attached handles, progress report.

Chad G Bryan - 8 hours - Worked primarily on the topical seminar

Ben Calvert - 10 hours - Installed and configured Pi OS’s, made slides for topical seminar presentation

Ben Curths – 10 hours - Topical seminar, system testing, experimentation, and prototyping

Simone Gbouomou -7 hours working on installing the VM. Also made Slide for the topical seminar presentation.

Ben McAnulty - 8 hours - Topical seminar;