SCADA Home Automation

Interim Report

Project Summary:

The SCADA Home Automation 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. The purpose of this model is to educate and generate interest in the cybersecurity discipline amongst prospective students and young professionals entering the field by clearly demonstrating the physical effects of and real-world vulnerabilities created by digital cyberattacks.

To accomplish this demonstration, the project will incorporate a set of microcontrollers that includes two Raspberry Pi's and an Arduino running the open-source ScadaBR and OpenPLC software packages, respectively. The ScadaBR devices will connect to an LCD panel to serve as a human-machine-interface, and the OpenPLC device 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, and a DC-motor controlled door for remote opening/closing.

Team Description:

The team is loosely segmented into two groups based upon the specialization and skills possessed by the members of each group. These consist of a four-member cybersecurity engineering group as well as a two-member computer engineering group. Team members and their relevant skills are as follows:

Project Manager:

- **Jon Beason (Cybersecurity)**
  - Secure Software Development
  - Network Security
  - Fabrication

Cybersecurity Engineering:

- **Ben Calvert**
  - C++/Python
  - Network Security
  - Linux
- **Simone Gbouomou**
  - Network Security
  - C/C++
  - Cybersecurity Management

- **Ben McAnulty**
    - Network Security
    - C/C++
    - Secure Software Development

Computer Engineering:

- **Chad G Bryan**
    - Embedded Programming
    - C++/ARM Assembly
    - Digital Logic Design
- **Ben Curths**
    - Digital Circuit Design
    - Embedded Systems Design
    - Software Engineering and Design
        - C/C++
        - ARM

Contingency Plan:

In the event that a team member becomes unavailable or is unable to fulfill his/her obligations, other team members will be required to step in and complete the required work, and assistance from additional members may be supplied as needed. Task assignments in following work periods may be rearranged to compensate and balance team workloads if the required coverage is especially demanding. Each specialization group, either cybersecurity or computer engineering, contains more than one team member with the necessary skills to complete the tasks required of that group, and this skill redundancy will provide a buffer to help reduce any impact resulting from the loss of a single member.

In the event that multiple team members become unavailable, the remaining team will request a meeting with the project sponsors/mentors to discuss and decide upon an appropriate course of action up to and including project scope redefinition.

Introduction:

SCADA Home Automation is a faculty-sponsored project put forth by Dr. David Coe of the UAH Engineering Department. The project is an adaptation of the SCADA Elevator demonstration conducted in previous terms and originally put forth for this term as well. The initial project proposal called for the creation of an interactive display model that simulates a home automation system utilizing a SCADA framework in which users could deploy developed cyberattacks to disrupt the proper functionality of the system in real time. From further discussion with project sponsor, the following marketing requirements were defined:

- The system must be portable.
- The system must be easy to set up and interact with.
- The system must be based upon SCADA and PLC elements.

- The system should be flashy and/or interesting to interact with.

The exact nature of the elements and interactivity of the project are left to the team to decide upon as part of the design. However, the following constraints are in place:

- The project has an overall maximum budget of $400.00.
- The system must operate on an independent physical LAN.
- The PLC elements must use the OpenPLC software package and be programmed via ladder logic.

Complex Design Problem Declaration:

We believe that the proposed SCADA Home Automation project qualifies as a complex design problem due to the following properties:

- **The project is a non-trivial problem with no obvious solution.**
  - Developing a malicious attack against an interconnected home automation system requires unconventional approaches and often involves one or more non-obvious attack vectors. Similarly, developing countermeasures for these attacks requires identifying the vulnerabilities exploited and creating mitigation tools to prevent further exploitation.
- **The problem is decomposable into several subcomponents.**
  - The proposed demonstration for this project requires the development of several functional components: the hardware of the simulated interconnected home automation system, the software to control and monitor the system, the cyber attack methods used to compromise the demonstration system, and the mitigation tools for defending against the developed attacks. Each of these components can be further decomposed into subcomponents that will require research, design, implementation, and testing.
- **The problem involves the synergistic integration of multiple technical disciplines.**
  - The proposed project requires the technical expertise to implement the integration of physical hardware in the form of the interconnected home automation simulation and the controlling software for managing the physical system. Additionally, the project requires cybersecurity expertise in analyzing the developed system for potential vulnerabilities, exploiting said vulnerabilities, and developing countermeasures to secure the system against further attack.

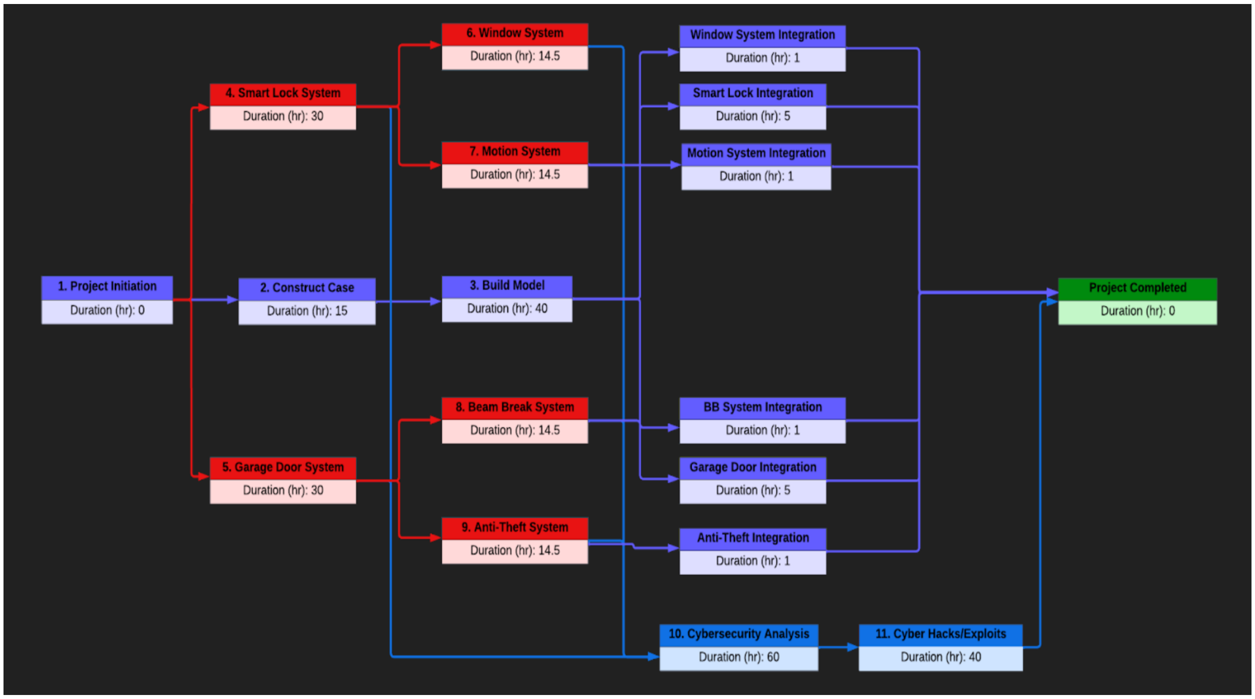
Each team member has relevant expertise earned through the UAH Computer Engineering and Cybersecurity Engineering programs, including but not limited to digital circuit design, embedded systems design, computer organization and architecture, and software engineering practices and principles, cybersecurity threat assessment, and cybersecurity threat mitigation. These skills will likely prove invaluable in both the hardware selection and design process and the software design and implementation for this project.

Project Management Plan:

Project development will follow a modified scrum-based Agile framework. Work will take place in a series of sprints with durations of two weeks each. Each sprint will begin with a kickoff meeting during which project tasks will be assigned to team members from the project backlog, and there will be a sprint retrospective meeting at the end of each sprint during which the progress of the last two weeks is reviewed. Project sponsors/mentors are invited to attend these meetings and offer their feedback or guidance at their discretion. A regularly scheduled mid-sprint meeting will be held to formally allow for updates and issues to be communicated to the team, and irregular unscheduled meetings may occur as needed throughout the project.

At the end of every two sprints, on a roughly monthly basis, anonymous peer review surveys will be conducted to measure individual team member performance. Contribution to project artifacts as well as sponsor/mentor feedback may also be factored into these evaluations.

Project Timeline:



Test Plan:

Unit Testing: The functionality of the individual system components will be tested during the development of the Ladder Logic.

Integration Testing: As each component is integrated into the model, that component will be tested to ensure it works within the overall system and provides the correct functionality.

Regression Testing: As the system is altered by modification or the integration of new components, the system will be retested to verify continued proper functionality of existing components.

Acceptance Testing: Upon completion of the project, thorough testing of the system as a whole will be performed to ensure it functions per the stated requirements and meets stakeholder expectations.

Project Cost Evaluation:

Components / Hardware		
Qty	**Component Name**	**Price**
1	Arduino Mega	$50
1	Monitor	$80
2	3mm IR Sensors	$6
2	PIR Motion Sensors	$20
3	Magnetic Sensor	$8
1	Force-Sensitive Sensor	$6
1	Small Solenoid	$8
2	Micro Limit Switch 10 pack	$7
1	DC Motor	$13
1	10 count 1000mm Alum. Extrusion	$80
1	Smart Deadbolt	$40
1	5 Port Ethernet Hub	$10
1	Led Strobe Beacon (flashing light)	$20

Labor Cost	
Job / Task	Price in Hours
Building Model	40 hr
Building Case	15 hr
Ladder Logic Programming	60 hr
Circuit Prototyping	20 hr
Integration	14 hr
Testing	38 hr
Cybersecurity Analysis	60 hr
Cybersecurity Exploits/Hacks	30 hr

Software / Services	
Software	**Price**
OpenPLC	Free
scadaBr/Home Assistant	Free
Linux 0S	Free
Kali Linux	Free

Background:

As the world grows ever more interconnected, the threat presented by weaknesses in device security and those who would exploit those vulnerabilities also grows ever larger. Internet connected devices are migrating further into the consumer space, and always-online household devices provide a vector through which the threat of cyberattack can directly affect the lives of everyday people. Because of this, the need for cybersecurity engineers and trained specialists has never been higher.

The SCADA Home Automation System is a physical and interactive education model designed to emulate today's smart home systems. The focus of the project is to introduce and generate interest in cybersecurity amongst students and young professionals through the use of a demonstration model. By interacting with the model, students and young professionals will be able to see the effects of cyber-attacks manifest in a physical manner.

Smart Home Automation devices were intentionally chosen for the demonstration components of the project to create a direct connection between cybersecurity and the technology they interact with on a daily basis. The SCADA Home Automation System project helps fulfill the essential need to generate interest in cybersecurity amongst students and young professionals. With the shortage of cybersecurity professionals and the limited existence of educational models that highlight and demonstrate the importance of cybersecurity, the need for this project is paramount.

Environmental and Societal Impact:

The SCADA Home Automation project will not have a global and societal impact on the environment, and this is mainly due to the project type. The SCADA Home Automation project is a custom interactive educational model built to demonstrate Computer/Cybersecurity Engineering principles in an indoor controlled environment. Therefore the project will not have any negative impact on wildlife, forest, wet-lands, air quality, and water quality. Nor will it emit any type of harmful gasses, pollute the environment, increase the level of audible noise, or affect the aesthetic beauty of the surrounding area.

The expected life cycle of the project is ten years with the hope that at the end of its life the product components can be repurposed. The materials and components for the product will be off-the-shelf products procured from online retail stores or salvaged from previous projects. Since the SCADA Home Automation project is designed from the ground up to be a closed looped system, there are no outside security issues or vulnerabilities associated with the project other than those intentionally placed in the project for educational purposes, which are themselves contained within the closed system and have no impact on any system or device outside the model.

The project is designed to only need a wired LAN connection via ethernet and power from an electrical receptacle. Therefore, backwards compatibility or the ability to work with emerging systems is not an issue. In addition, the product does not contain nor is it designed to store any personal or proprietary information. The only possible health and safety issues associated with the project is the product's use of a flashing light. Since flashing lights have been known to cause seizures with people who have photosensitive epilepsy, extra care will be taken to place any flashing lights out of direct visual contact with people. Issues that may arise during construction of the home model include soldering iron burns, toxic fumes from the soldering iron, electrical shocks from prototyping, and sharp edges. These safety issues can be mitigated by utilizing tools with proper knowledge and being equipped with proper safety equipment.

The SCADA Home Automation system is not designed with the intention of mass production, it is not intended to be commercially sold, and contains no hazardous or restricted materials. Therefore, there are no legal or regulatory issues that would affect the product. Also, there are no major trade-offs to the product that pertain to the project design such as environmental versus economic, health and safety versus economic, and software versus hardware. As stated earlier, the product is an educational demonstration that is contained within a closed-loop system and the presence of risk and threats are placed within a controlled environment with the purposes of teaching about cybersecurity vulnerabilities.