Implementing OpenPLCs into a Cyber Defense Competition

Team 16

Dr. Doug Jacobson
Dr. Julie Rursch

Nick Springer - Security Engineer
Matthew McGill - Project Manager
Val Chapman - Software Testing Engineer
Josh Przybyszewski - Software Engineer
Joseph Young - Software Engineer
Liam Briggs - Hardware Engineer
Brennan Fergueson - Hardware Engineer

sdmay18-16@iastate.edu
http://sdmay18-16.sd.ece.iastate.edu

Revised: 9/22/2017

Contents

1 Introduction

1.1 Project statement

Our task is to explore the OpenPLC project and determine how it can be implemented into a Cyber Defense Competition (CDC), with the intention of simulating a real-world cyber physical environment.

1.2 purpose

With the advent of the Internet of Things (IoT), many physical systems are now relying on network connectivity to provide functionality to users. These systems are often large, and provide an invaluable service such as power or water management. In addition, they are often undersecured. By incorporating the OpenPLC project (which simulates the PLC hardware required to control and monitor these types of systems) into the CDC, we hope to provide the competition's contestants with valuable experience in securing cyber physical systems from malicious actors.

1.3 Goals

Our first task is to become familiar with the OpenPLC project; we must have a workable understanding of what a PLC is, how it is operates, and how it may be programmed. In addition, we must analyze the existing CDC environment, so we are familiar with its architecture. From there, we should develop a basic web interface which allows users to send signals to the PLC and monitor signals being received. We should first seek to produce this base integration with the CDC environment, so that it can be extended upon in future years for different scenarios. Once we have a base integration, and have brainstormed several potential scenarios that may be interesting for contestants, we will select one or two scenarios to serve as a proof of concept. We will test any new hardware required for the scenario, and develop a module which allows this scenario to serve as an extension on top of the base integration with the CDC delivery system (an ISERink). If possible, we should seek to complete the design and as much testing as possible during the first semester of the project.

2 Deliverables

Our PLC systems will control physical items to give a visual aid to the cyber defense competition. These systems will be fully implementable in the network and designed in a way to be determined so the teams are in control of the security of their own designated portion.
The project we've made the most headway with is a train track system with mobile components on a schedule. Depending on products we can find, this will include train stations, track switches, and a 'good' to be delivered by the train. Each team may be responsible for a train, or a component of the train track system. All of this will be dependant upon Raspberry PIs that will be neatly combined with system. As of now the physical system will not be very customizable, but the software will be as to be more easily used in different competitions.

3 Design

3.1 Previous work/literature

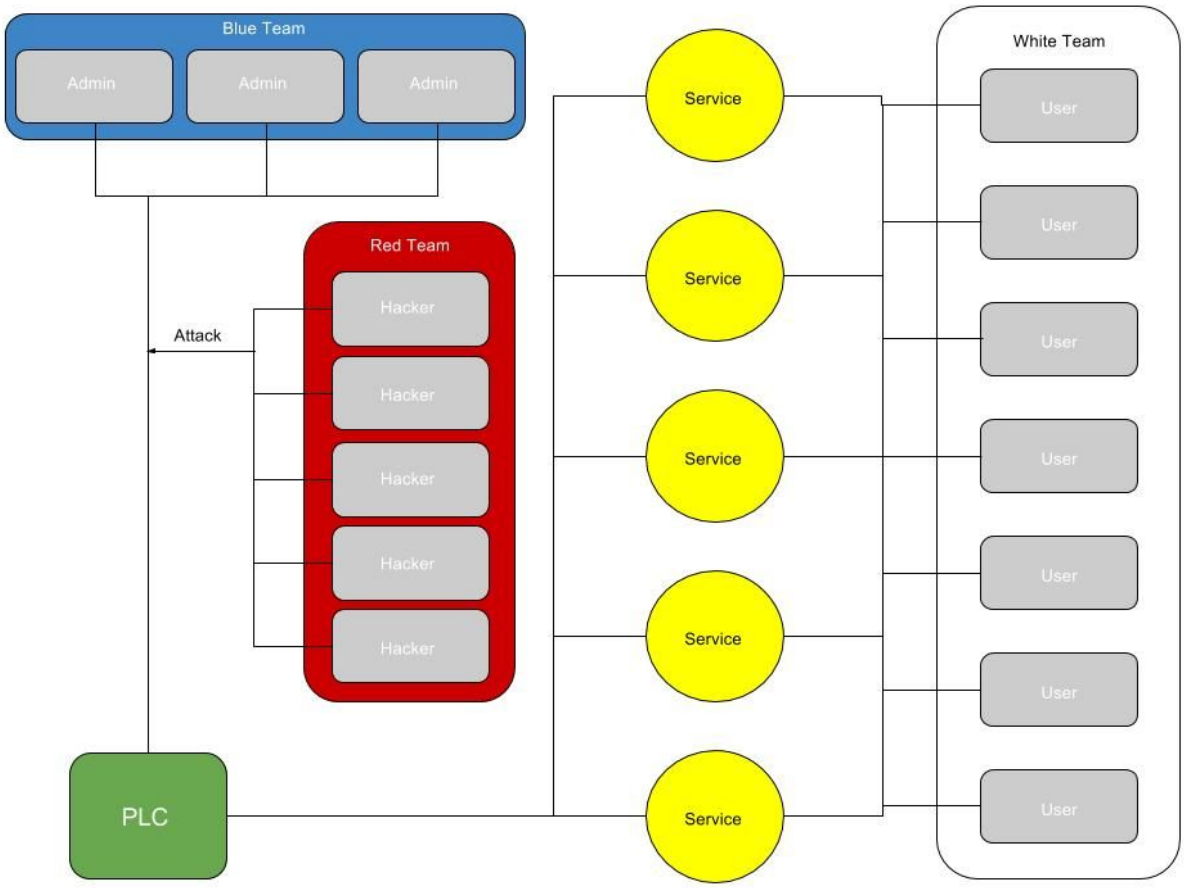
Historically, the Cyber Defense competitions have only done two cyber physical CDC's. Our project is a continuation and expansion of a previous implementation using 3D printed cities. These cities only provided output in the form of LEDs to denote whether your system has been hacked or not. In our project, we are building more hardware to simulate cyber physical systems that will be more advanced than an LED.

Our team has spent some time looking around on the internet and we haven't found many previous projects that would provide a foundation for us. As a result, we will not have a foundation to build off of other than the OpenPLC software on top of Raspberry Pis. As a result, we will be starting from scratch and have to figure out how we can interface between the CDC systems and the hardware.

3.2 Proposed System Block diagram

In our project, we will be using the PLCs to simulate cyber physical systems. These cyber physical systems will provide services to a customer base just like in the real world. To start off, our simulated environment includes the Blue Team, Red Team, and the White Team. The Blue Team simulates the IT professionals who build and have full control over the cyber physical system. Next, the Red Team simulates the hackers and criminals who try to disrupt the services. Lastly, the White Team simulates the end user of the provided services.

In the block diagram below, the PLC is the heart of the cyber physical simulation. The PLC will control the services that the White Team uses as well as take commands from the Blue Team. While the Blue Team perform their own tasks, the Red Team will attempt to hack the PLC to gain control of it. This model will represent a single team in the overall cyber defense competition.



3.3 Assessment of Proposed methods

Our design at a high level does seem to be something that will integrate well with the CDCs. The system will be able to directly connect to the participants for virtual access and will also allow the competitors to interact with the devices physically. The setup process will be virtual in order to allow remote participants the capability to work on the systems off campus.

3.4 Validation

We will verify that our solutions work by doing incremental testing. Initially, we will start with a few Raspberry Pis and put the OpenPLC software on them to see how we can interact with them. A great place to start would be trying to interact with and LED, or something else that is simple, in order to understand how the system works. This process will not only help us learn how the system works, but will provide us with an idea of what will and won't work.

4 Project Requirements/Specifications

4.1 FUNCTIONAL

Services to White Team: Most likely, these will be "virtual services" such as a model transit-train system running or security cameras watching a virtual/model bank.

Hardware Devices: Raspberry Pi, any physical connected sensors and devices (light sensors, gauges, lights, trains, pipes, etc.), potentially a camera for a live feed of the physical system.

Software Interface: NodeJS server (for uploading to Raspberry Pi), web interface for monitoring physical systems and sending signals to devices.

4.2 NON-FUNCTIONAL

Documentation: Thoroughly document vulnerabilities and design decisions. Documentation is very important for posterity, so future CDCs and CDCs at other schools can understand what we were thinking in order to duplicate and improve the scenario.

Intentional Hardware Vulnerabilities: Potentially be a physical site for red team to insert a USB drive or access a WiFi network.

Intentional Software Vulnerabilities: Multiple modular software vulnerabilities for red team to exploit. They need to be modular enough so that the CDC planners can choose a few from a larger selection so that red team doesn't see the same vulnerabilities every CDC.

NOTE (On the ethics of intentional vulnerabilities): Since the CDC is designed to give real-world experience with unethical hackers, our choice to leave intentional vulnerabilities is made in full light of the circumstance. In the real-world, hacking is illegal, immoral, and bad. However, hackers exist, and the CDC gives "the good guys" a chance to find out what hackers will do. Our intentional vulnerabilities give the blue teams the opportunity to patch these areas.

4.3 STANDARDS

Code style: Standardizing our code-base is essential to the longevity and maintainability of our software. The coding standard will be defined by language. For example, C might be standardized by K&R's C.

5 Challenges

Include any concerns or details that may slow or hinder your plan as it is now. These may include anything to do with costs, materials, equipment, knowledge of area, accuracy issues, etc.

Challenges that may slow us down in our development process are documentation of the open source projects we use, and developing a CDC project that could be used to teach students cyber security systems.

We plan on using OpenPLC in our project. This project is less used project and the documentation surrounding it is lacking. This will lead to members of our team having to work out manually many of the questions, we have that should be answered by documentation, but are not. The OpenPLC editor creator, has stated in a small document, that there is no documentation. Also, PLC's use a language called ladder logic, which a language that no members of the team have experience in, so we will all have to learn this new language to implement it into our design. When an entire team is learning a new language there is definitely going to be growing pains.

The second larger challenge we will face this project, is the designing of a OpenPLC implementation into a CDC. This will be challenging because we are in a sense building a curriculum for students to learn cyber physical devices. This project is to replicate a real world physical environment where security is a requirement, so our project will implement this as close as possible. We will face the challenge of making this project, as real as possible, without making it overly complex for the students trying to implement the security into their system.

6 Timeline

Gantt Chart will be added here in v2.

6.1 First Semester

Scenario's Picked and Designed: 11/1

Raspberry Pi's bought for experimentation: 10/21

Project Plan(v1): 9/22

Project Plan(v2): 10/27

Project Plan(Final): 12/1

End of First Semester - Our team would like to have a fully-functioning prototype by this time. We will be implementing a more basic, high level PLC that will be fully integrated in with the ISEAGE environment. We will be utilizing the OpenPLC source code, and designing a web interface to interact with our PLC.

6.2 Second Semester

Second semester schedule is *much* more tentative.

First thing in January: Purchase necessary equipment for the scenario(s) we outlined in detail first semester

Mid-February: Have our first scenario fully implemented, at least v1.

End of February: Refine our first full implementation, fix any bugs, resolve any issues

End March: Have 2-3 scenarios implemented, making refinements and solidifying presentation all throughout April.

7 Conclusions

As one can identify from the above report, my team's overall goal for this project is to take a programmable logic controller and implement it within an Iowa State cyber defense competition (CDC). Up to this point, each and every CDC has utilized virtual systems and situations to enact real-life situations. These virtual scenarios have enabled students to learn and grasp security-related concepts in incredible ways, but they do have their limitations. For starters, they don't always seem real, or practical. The stakes are never super intensive, and the situations don't always have direct application to current-events happening around the world. Learning to protect virtual environments is absolutely essential in the world of security, but security sometimes extends beyond the virtual world. The time for improvement and progress has arrived, and that's where our team's project comes into play. The need to emulate real cyber-physical systems within the context of these CDCs is really the next step in educating students about the necessity of security in almost every single industry.

To tackle this problem, my team has broken this lofty vision and long-term goal down into manageable steps. Over the course of this first semester, my team will spend a majority of our time understanding the OpenPLC project, and developing simple prototypes (for example, a simple hardware board connected to an LED panel, with the state of various inputs determining what lights turn on or off) to demonstrate our understanding of the system as a whole. We will develop a web interface to interact with our prototype PLC, with an admin role to control these inputs at will. In order to make this extremely portable for future CDCs, we want to build and design this system to work well with the ISEAGE environment. Our security engineers will work to secure our web interface, as well as fabricate some sort of design scenario where future blue teams (participants in the CDC) would have to protect the cyber-physical system against attack from the infamous red team. Moving forward into second semester, we will take the knowledge we learned from the first, and apply it towards several more complex PLCs. We have carefully crafted several different scenarios that would make for some great CDCs, bringing together the virtual aspect that has made the CDCs so successful in the past with the physical realm that will launch the CDCs into yet another generation of student success.

8 References

http://www.openplcproject.com - The OpenPLC Project Official Webpage and Documentation

http://www.plcsimulator.net/login.php - PLC Online Simulator

9 Appendices

This section is not applicable for v1, but will continue to play a larger role in later versions of this document.