

# EE/CprE/SE 492 WEEKLY REPORT

1/27/18 – 2/09/18

## Implementing OpenPLC's into a Cyber Defense Competition

**Group number: 16**

**Faculty Advisors: Drs. Jacobson and Rursch**

### Team Members/Role:

Matthew McGill — *Meeting Facilitator, Project Manager*

Brennen Ferguson — *Hardware Engineer*

Joseph Young — *Security Engineer*

Liam Briggs — *Hardware Engineer*

Joshua Przybyszewski — *Software Engineer*

Nicholas Springer — *Security Engineer*

Val Chapman — *Testing Engineer*

### ○ Weekly Summary

This week we were able to meet up with the White team and receive feedback about what is needed for a real CDC. Using this feedback we are guiding the steps we are taking now and for the rest of the semester to ensure that our product is in as complete of a state as possible to be able to hand off to future users for more diverse implementations.

### ○ Past week accomplishments

**Matthew McGill:** Me and few other team members met with the IASG (Information Assurance Student Group) CDC White Team to discuss the logistical elements needed to take an idea and spin it into a fully fleshed out scenario. We learned so much during this meeting. One of the first things they mentioned was “documentation” across the board. Scenario docs, vulnerabilities fully explained, etc. All of the documentation needs to be completed, so we have quite a bit of upcoming work on our hands. Josh Przybyszewski and I will also continue work on the application, and connection the .NET SDK to an instance of Factory I/O.

**Brennen Ferguson:** Finished a more complex Palletizer scenario in Factory I/O. Met with CDC White Team to figure out CDC integration. Began looking into documentation, and Factory I/O performance issues.

**Joseph Young:** Researched potential methods for exploiting intentionally vulnerable systems in the VCenter environment. Continued to mirror research and testing between personal machines and ISELAB VMs.

**Liam Briggs:** Communicated with RealGames about their SDK and received testimonials from well known corporations using their software and organized the requests and tips from the CDC white team meeting into goals.

**Joshua Przybyszewski:** Worked on .NET application in Windows machine, investigated diminishing the number of required cores for FactoryIO to run.

**Nicholas Springer:** Met with White Team to discuss what needs to be done before handing off the application. Created a list of what needs to be documented/what needs to be considered in the project.

**Val Chapman:** From the meeting this week, I am working with the White team to acquire templates for user documentation for all the different teams for the CDC. I am then starting to fill these out according to our scenario.

○ **Pending issues (if applicable)**

**Team:** From the meeting this week we learned about the resources available for a CDC. Currently our implementation uses a large portion of the available resources to a CDC so we will be looking into reducing the number of cores we use if possible.

**Matthew McGill:** Prior to the work accomplished these past two weeks, my team was planning on creating an Angular Dart application that would interface with Factory I/O. However, it turns out that the SDK the developers have provided (on GitHub) only works with .NET applications, so we have to completely rewrite everything we've done so far. Hopefully we will have some updated progress to report in two weeks after rewriting and working with the Factory I/O provided SDK.

**Joseph Young:** Lack of direction without input from the White Team. It would be useful to have a more targeted goal for the environment's vulnerabilities.

**Liam Briggs:** Creating a large interconnected factory scenario

**Nicholas Springer:** Continue documenting any changes to vulnerabilities added to the servers. Experiment with core usage to see if we can use less resources.

○ **Individual contributions**

Team Member	Contribution	Biweekly Hours	Total Hours
Matthew McGill	Met with the Information Assurance Security Group on campus, and learned a lot of information about turning an idea into a CDC scenario. I also continued development on the implementation of the Factory I/O SDK.	14	72
Brennen Ferguson	Finished a more complex Palletizer scenario in Factory I/O. Met with CDC White Team to figure out CDC	12	74

	integration. Began looking into documentation, and Factory I/O performance issues.		
Joseph Young	Continued security research and testing in the VCenter environment	8	62
Liam Briggs	Began work on specific white team requests and organizing presentation of Factory I/O for others	8	70
Joshua Przybyszewski	Continued progress for the web application	12	71
Nicholas Springer	Maintained and updated virtual machines and the teams credentials for testing	8	90
Val Chapman	Looked into testing of web application and documentation requirements for the different CDC teams.	10	64

**Plan for coming week**

Our plan is to take the information from the White team meeting and update our documentation and ensure our documentation is up to date. We will also be researching into our resource usage of factory I/O and seeing if we can reduce this to require less hardware.