**CSI OT 3D Platform Cyber Attack Demonstration Design Document**

Date: 15/12/2020

VERSION: CORPLAB-2019-T3.1-P1

Edited by LiuYuancheng

**Introduction**

This project contains four section:

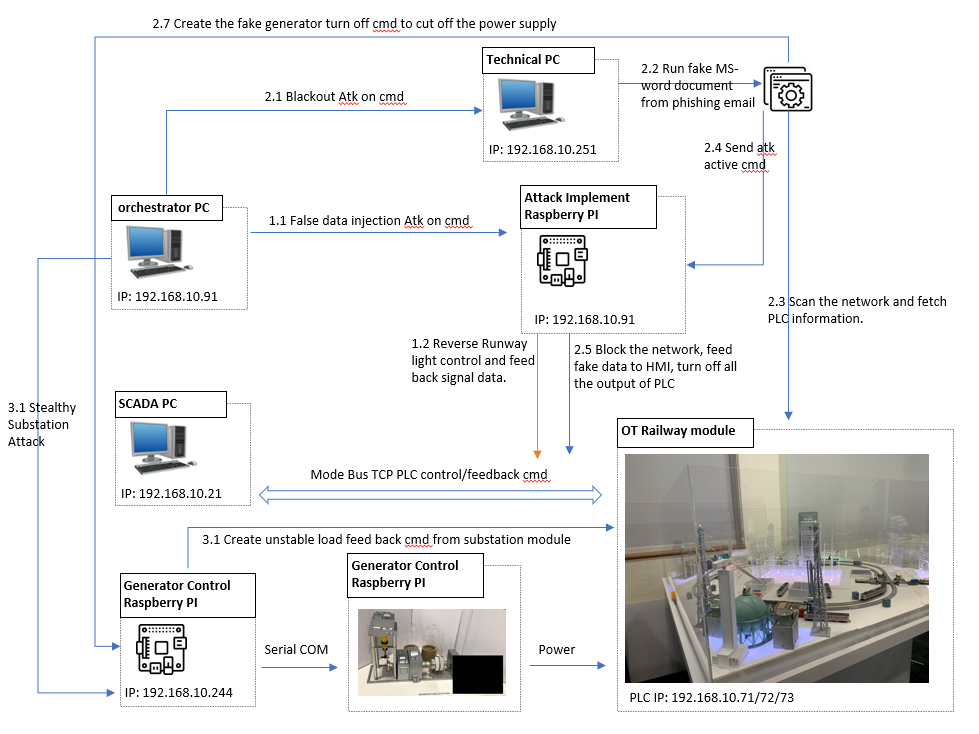
PLC-Railway HMI System: In this section we will create 2 Railway PLC SCADA HMI system with schneider wonderware(R) program and python for the user to control the PLC railway modules or simulate different railway operation for training or research purpose.

PLC-SCADA System Attack : In this section we will show 3 different kinds of cyber-attack situation on the Railway SCADA system which we have built in the previous section. Detail introduction for the attack section:

Attack Control website: In this section we will create a web site server running on the orchestrator PC to provide a web interface to let the user control different cyber attack demos on OT railway module platform and show and show feedback display during the presentation.

Power Generator Manager: We will provide A user interface to control the OT-Power Generator Module's hardware. It will send command to PLC and Arduino and receive the control request from the remove controller. The control program will do the adjust of the generator's motor and pump speed based on the loads in the system.

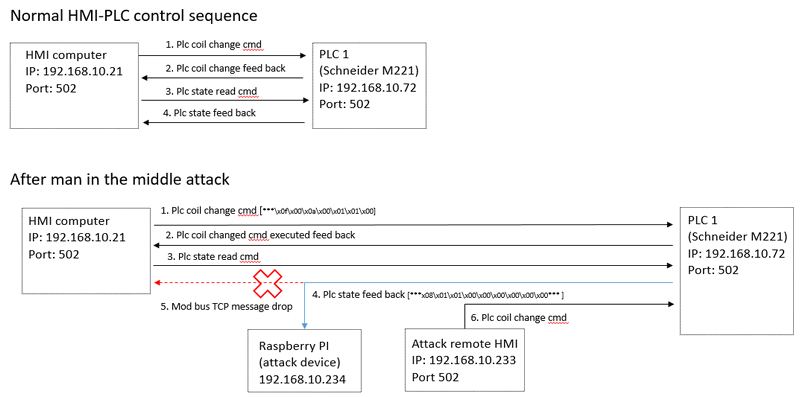
System hardware connection and IP address configuration:



Cyber attack

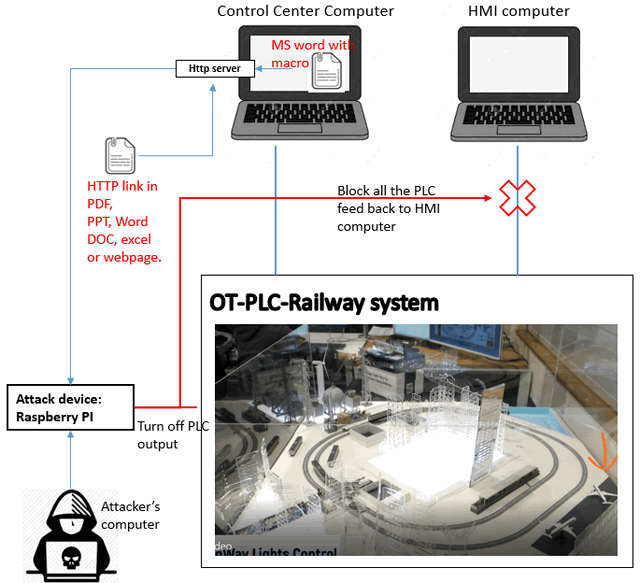
False Data Injection Attack:

In this attack, we assume an additional foreign hardware (IoT/RaspberryPi) was plug in to the OT network. This attack will manipulate the SCADA command and feedback.causes the SCADA HMI show the opposite feedback on the actual system.This demo will attack on airport light control, where the operator will see reverse PLC feedback on theactual system, e.g. When the operator try to turn on the runway lights in the airport via HMI, the actual runway lights will be turn off.



Blackout Attack:

This attack is model after 2015 Ukraine power grids cyber-attack. This attack will assume the system do not properly air-gapped, whereby the malware is enter to the system via spear phishing email. When the attack launched, all the PLC output coils (energy output) will forced to turn off.



Stealth attack:

Technically, known as False Command Injection attack.[Attack introduction will follow Shantanu ‘s paper]

Attack Control website:

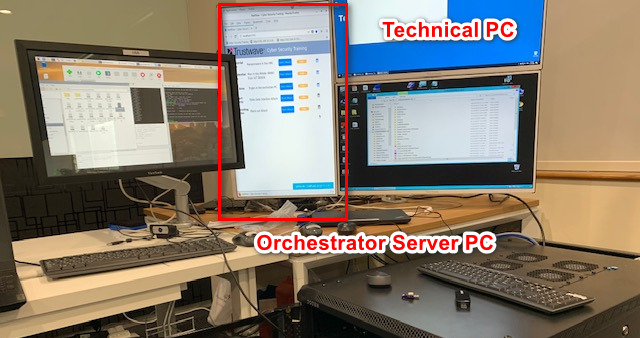
Development Environment: NodeJs(v12.18.4)/JavaScript HTML5

Additional Lib/Software Need : NodeJs(v12.18.4)

Webpage View:



Login the orchestrator PC:



open web browser and type in URL: <http://localhost:8080> or <http://127.0.0.1:8080>.

When the user press the “Start” attack button, the web host will send the attack activation command to the related agent.