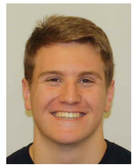
Industrial Control System Outreach Training Development

Summer 2021

FISH

Team Members



Michael Pate
- CE Senior

Taylor McCampbell
- COSC Junior

Taylor LaForce
- COSC & EE Sophomore

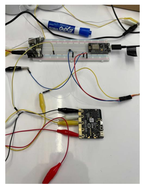
Rafer Cooley
- COSC Ph.D. Student

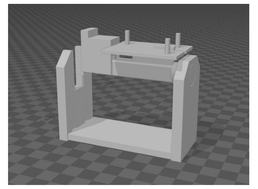
Problem Statement

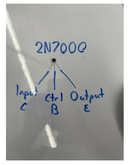
- Training and education usually focuses on regular cyber security skills.
- With these modules we are focusing on training people for critical infrastructure security specific skills.
- Including: awareness of everyday ICS and how they can be compromised, an overview of how programmable logic controllers (PLC) control and communicate in ICS, and how to mitigate ICS attacks.

Results

- 3D models generated
- Controller software produced
- Network equipment configured
- Custom HMI developed
- Paper reporting on voltage glitch attack on windmill farm model.
- Micro:bit solar panel module developed and utilized during GenCyber summer camp







Background

- Critical infrastructure part of insecure, outdated industrial control systems (ICS).
- Brands like Siemens, Allen Bradley, etc.
- Security is in question because systems are outdated and increasing number of attacks on critical infrastructure (Darkside, Meat Processing Plant, Water Treatment Facility, etc.).
- Physical world damage if infrastructure is successfully attacked.
- Lack of spare equipment, long lead time.

Methods

- Build models of critical infrastructure including a building model, an HVAC model, an oil collection model, water distribution system, and a windmill farm model.
- Build out the operating environment for these models including networking equipment, databases, and controller software.
- Experiment with side-channel and other forms of attacks in order to research attack mitigations.

Challenges & Future Work

- Print 3D models
- Connect controllers to models and wire all electronic components
- Lack of controller documentation
- Antiquated communications protocols
- Lack of free, documented, and reputable HMI software.
- Experiment with MITM attacks

University of Wyoming

Advisor: Dr. Mike Borowczak (mike.borowczak@uwyo.edu)
Group Members:
- Michael Pate (mpate2@uwyo.edu)
- Taylor McCampbell (tmccampb@uwyo.edu)
- Taylor LaForce (tlaforc1@uwyo.edu)
- Rafer Cooley (rcooley2@uwyo.edu)

CEDAR
Cybersecurity Education And Research Center