Pwning an Internet Connected Traffic Light: An Educational Experience

Jim Solderitsch
Electrical and Computer Engineering Department
Villanova University
james.j.solderitsch@villanova.edu
610-519-4975
Experiencing Control System Security

- Power Systems are examples of Industrial Control Systems
- Students need equipment to practice with even if they are remotely connected like many of my students are
  - We need to bring the ICS lab to them so that they can participate
  - We want them to experience ICS security hands-on
- We can’t put a power system in their hands but want them to:
  - work with a control system with real kinetic effects
  - have the experience of creating an HMI and programming a PLC
  - have experience with real attack and defense scenarios and exercises
- Equipment must be inexpensive and easy to set up
  - The CYBATI platform provides an affordable and immersive educational experience as we show in the rest of this talk
HMI and Engineering Workstation Interfaces
Traffic Light PLC Model
Ettercap MITM Attack: Light ’em Up

HMI Disabled

Traffic Light Operates Normally
Modbus Injection Attack: Dangerous Condition!
Attack via UbiDots API: Attack from Anywhere

Modbus Attack Triggered from iPad
Traffic Light All Green
HMI Inconsistent
Defense is Possible Using Security Onion NSM

Security Onion

Arpwatch/OSSEC

Digitalbond Snort Rules