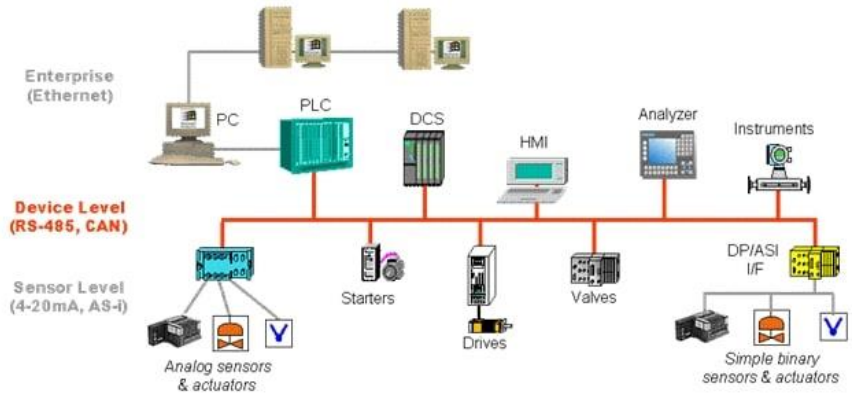
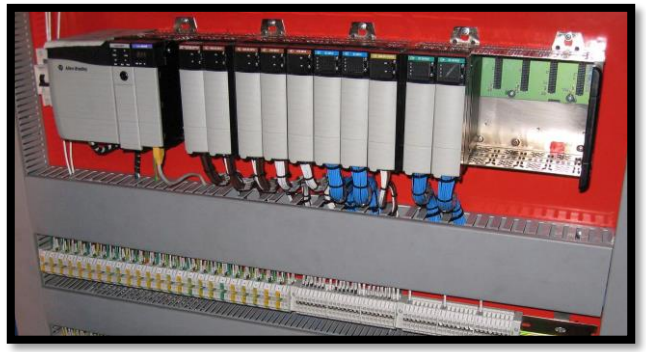
Northwest State Community College

Cyber Security Education for Advanced Manufacturing Organizations (CAMO)

Overview

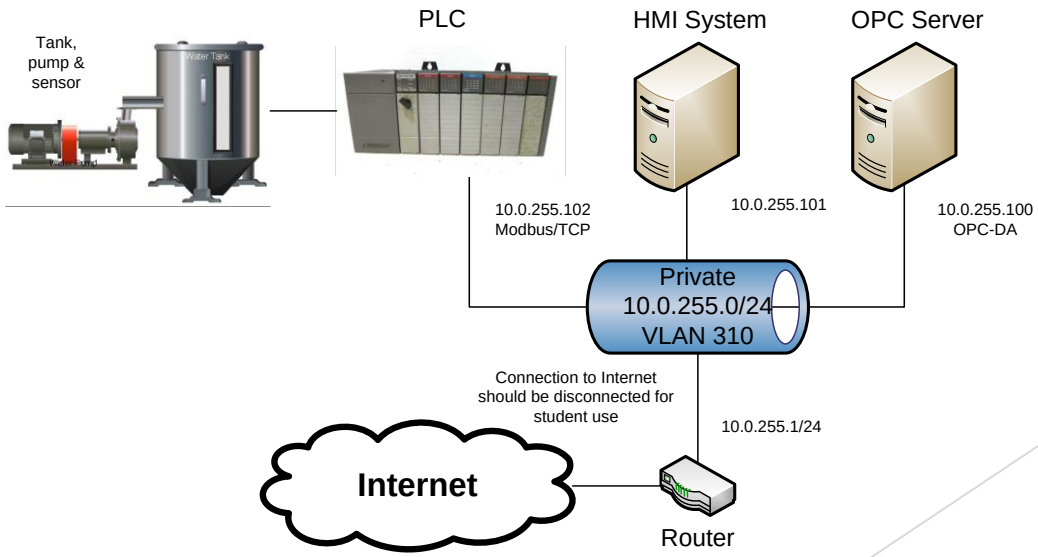
- Project Goal - To educate and train advanced manufacturing technicians in industrial cybersecurity theories, standards, best practices, and control for Northwest Ohio.
  - Create virtual training scenarios with a focus on issues and equipment encountered in manufacturing environments.





Virtual Industrial Control Network (ICS)

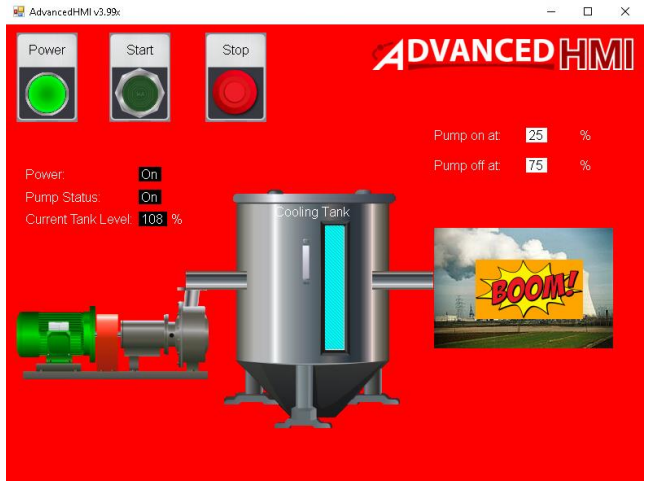
- One major component of the project is the creation of a virtual ICS
  - Because the environment is virtual no investment in physical industrial hardware is necessary
  - The system is designed to allow scenario designers to easily add additional components or to use different software and technology
  - A virtual environment provides students with a safe learning environment



Virtual Industrial Control Network (ICS)

- The virtual ICS allows students to safely demonstrate how hackers can compromise a system, then implement and observe the effectiveness of different security measures

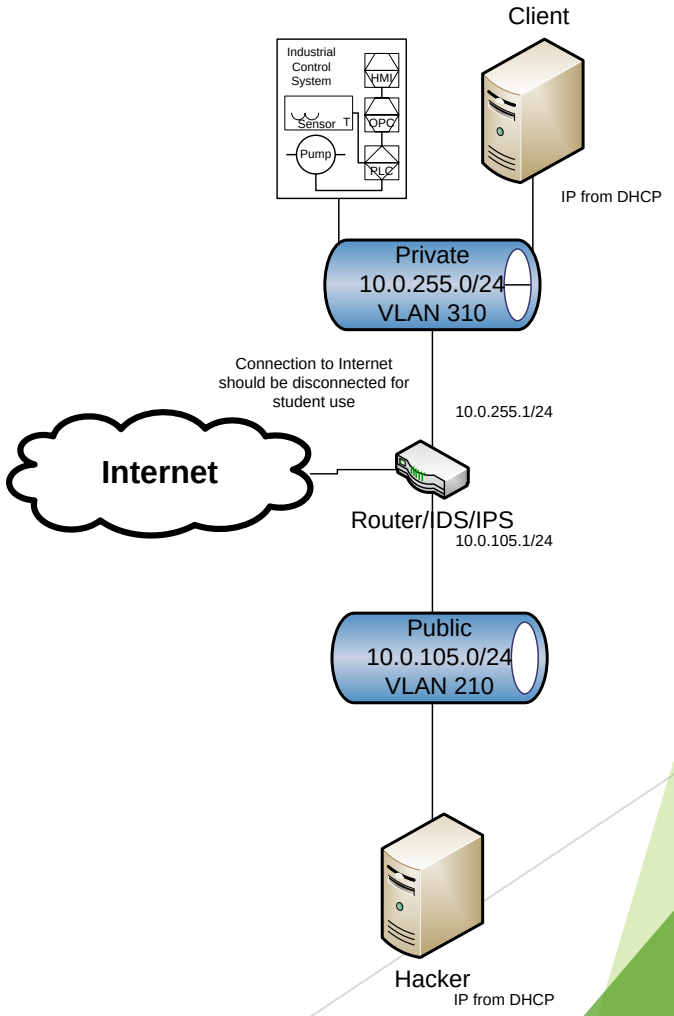
Normal operation



*** Hacked ***

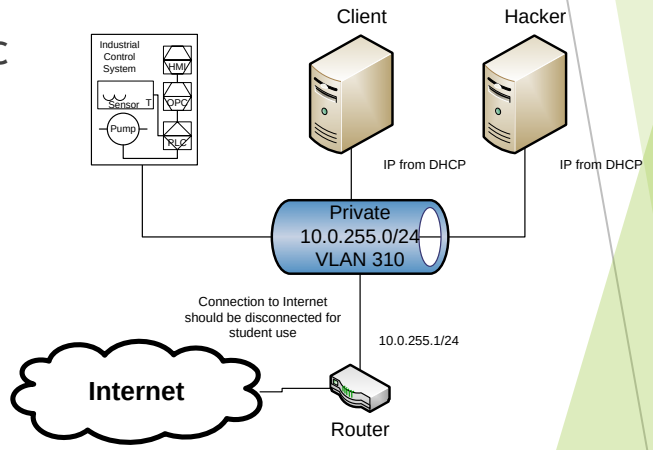
Proposed Training Scenario Topic

- Using IDS/IPS to Identify or Prevent Industrial Network Attacks
  - Monitoring network traffic flowing to and from industrial devices is one method of detecting and preventing hacking attempts on industrial devices. This monitoring can be automated using Intrusion Detection/Prevention Systems (IDS/IPS). In this training scenario students will learn the difference between different types of monitoring software and when each type should be implemented. Students will configure an IDS/IPS and see firsthand how these can be used in an industrial environment.



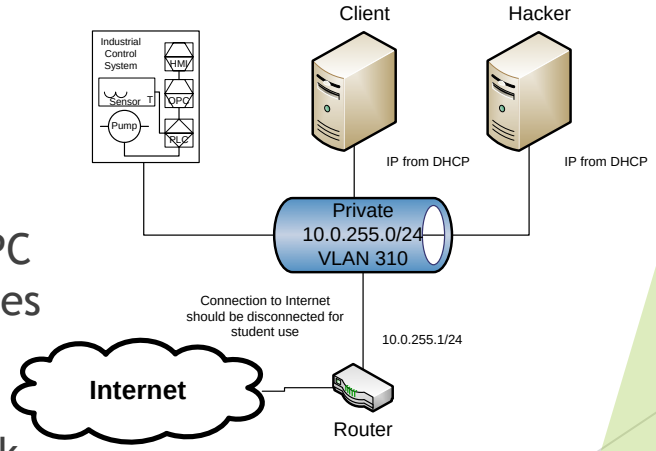
Proposed Training Scenario Topics

- Industrial Networking Basics
  - Industrial network protocols are designed to allow communication between sensors, motors, programmable logic controllers and other devices found in a manufacturing/industrial environment. These protocols were historically developed to reduce the amount and complexity of physically wired connections needed to implement a typical industrial system's control loop. Industrial networking has since evolved allowing industrial devices to communicate over TCP/IP and the Internet. Since these protocols are designed to be simple and reliable security is often minimal or nonexistent. This scenario teaches students the basics of three industrial networking protocols and some security vulnerabilities found in each. The scenario includes lab work in which the student will use common security tools to observe how industrial networking protocols function.



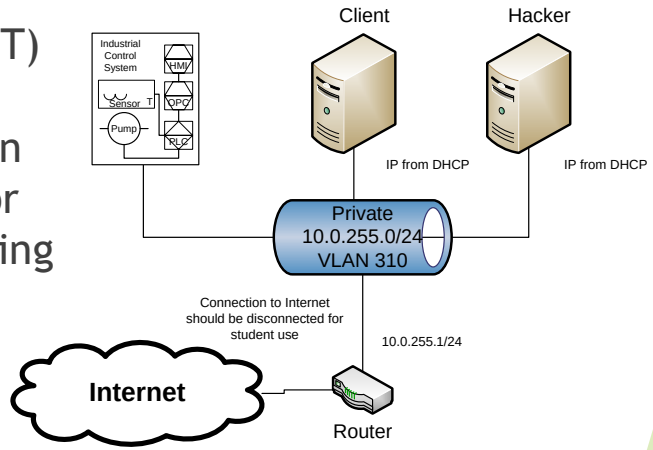
Proposed Training Scenario Topics

- OPC Server Security
  - Open Platform Communication (OPC) servers are commonly used to consolidate access to multiple industrial devices from different manufacturers. This makes it easy for engineers and programmers to directly access data registers and modify device configuration from a central location. One major problem with this is that it is often done without much thought as to authentication, confidentiality or data integrity. To make things worse OPC servers usually have, and make available, access to devices on multiple networks. Because of this OPC servers, and their hosts, are commonly targeted by hackers. This scenario will examine general OPC concepts and then look at multiple attack strategies which have been used to compromise OPC servers.



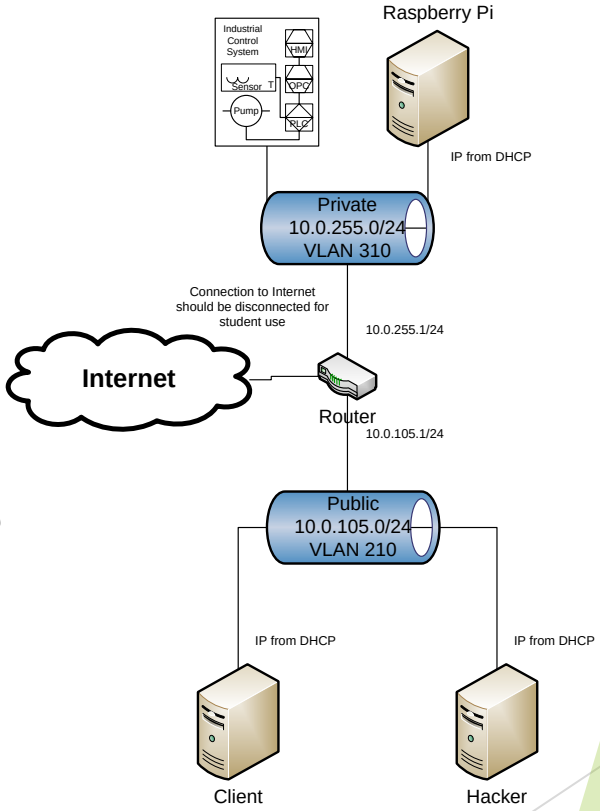
Proposed Training Scenario Topics

- Public Key Infrastructure and Industrial Cybersecurity
  - Some industrial technology such as Open Platform Communications (OPC) servers and Internet of Things (IoT) devices offer the ability to increase security by using certificates. Once a certificate has been issued, it is then used to prove a user or device's identity, provide keys for encryption or to sign network communication. This training will educate the student in the basics of encryption and how it is used with certificates and other Public Key Infrastructure (PKI) concepts. Students will have the opportunity to complete a lab in which they observe possible consequences arising from not using PKI security then they will configure PKI security and view the resulting increase in security.



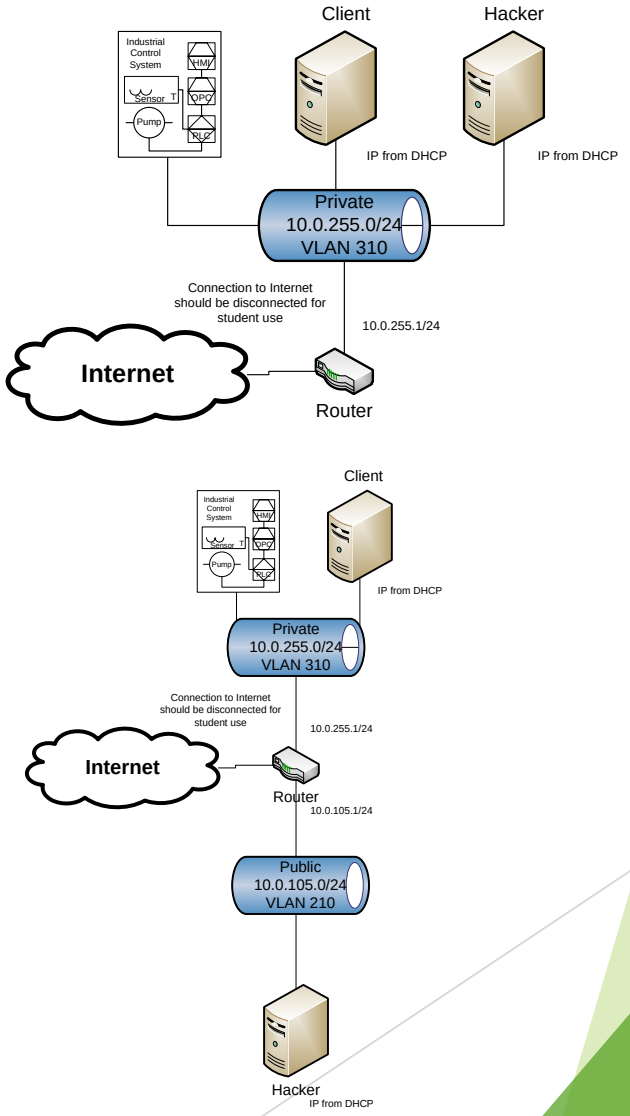
Proposed Training Scenario Topics

- Secure Remote ICS Access Using a VPN
  - Most devices connected to an Industrial Control System (ICS) should not be connected to the Internet. Even so, technicians and others often need to be able to access these devices remotely via the Internet or using other shared networks. If proper precautions are not taken this will create a risk that can be exploited by hackers and cause expensive and/or dangerous security breaches. One way of reducing this risk is to encrypt all traffic to and from the ICS network by using a Virtual Private Network (VPN).



Proposed Training Scenario Topics

- Using Zoning for ICS Security
  - Industrial control systems (ICS) and Internet of Things (IoT) devices often lack effective security controls. Because of this, workarounds need to be implemented to prevent these vulnerabilities from causing costly and or even dangerous security breaches. One effective way of preventing insecure devices from being exploited is to implement zoning as defined by the Purdue model. Part of zoning involves placing insecure or mission critical devices on to their own networks. This provides these devices the access they need to function properly while at the same time preventing them from being accessed or exploited by hackers in other zones.



For More Information

- If you wish to know more about this project please contact any of the following:
  - Tony Hills – thills@northweststate.edu – (419) 267-1354
  - Mike Kwiatkowski – mkwiatkowski@northweststate.edu – (419) 267-1231
  - Bill Chaplin – wchaplin@northweststate.edu
  - Sarah Stubblefield - sestubblefield@northweststate.edu - (419) 267-1512

Northwest State Community College