Using Zoning for ICS Security

Summary

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 network segments. 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.

Learning Outcomes

- Discuss the concept of network zoning using the Purdue Model.
- Learn how to create network zones using segmentation.
- Demonstrate how hackers can take advantage of improperly segmented networks and intercept communications.
- Demonstrate how network segmentation restricts a hacker's ability to intercept communications.

Systems

The industrial control system (ICS) used in this scenario simulates an environment that might be used to cool a nuclear power station. The ICS is made up of five systems. The first system contains a tank, tank level sensor and a water pump. The second system is a programmable logic controller (PLC) which controls the water pump based on the level of water found in the attached tank. The third system is an OLE for Process Control (OPC) server which accesses and modifies data found on the PLC. The fourth system is running Human Machine Interface (HMI) software which communicates with the OPC server to provide a human system operator with system statistics and control. The final system in the ICS is a security appliance that provides routing and firewall services for all systems.

- Kali Linux – Hacker
- Virtual Industrial Control System
  - Windows XP – OPC Server
  - Windows XP – HMI
  - PLC/Pump/Sensors
- pfSense – Router/Firewall

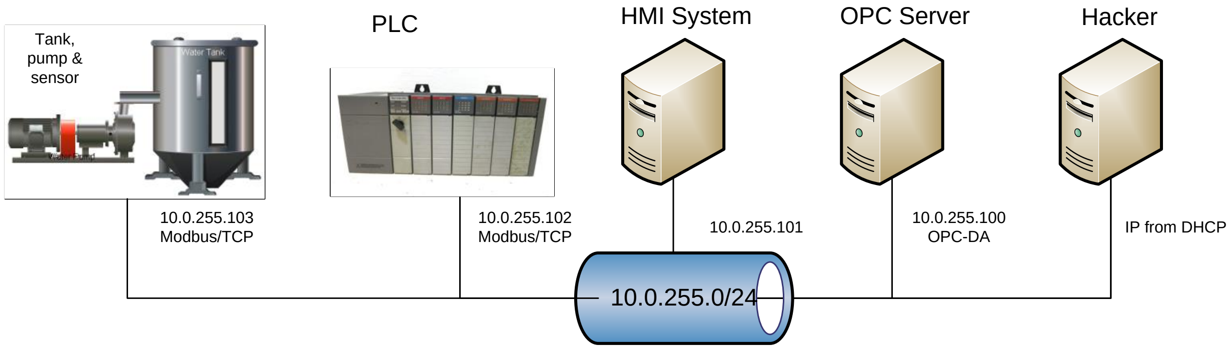
This scenario will make use of a system running Kali Linux running the Wireshark network monitoring software.

General Lab

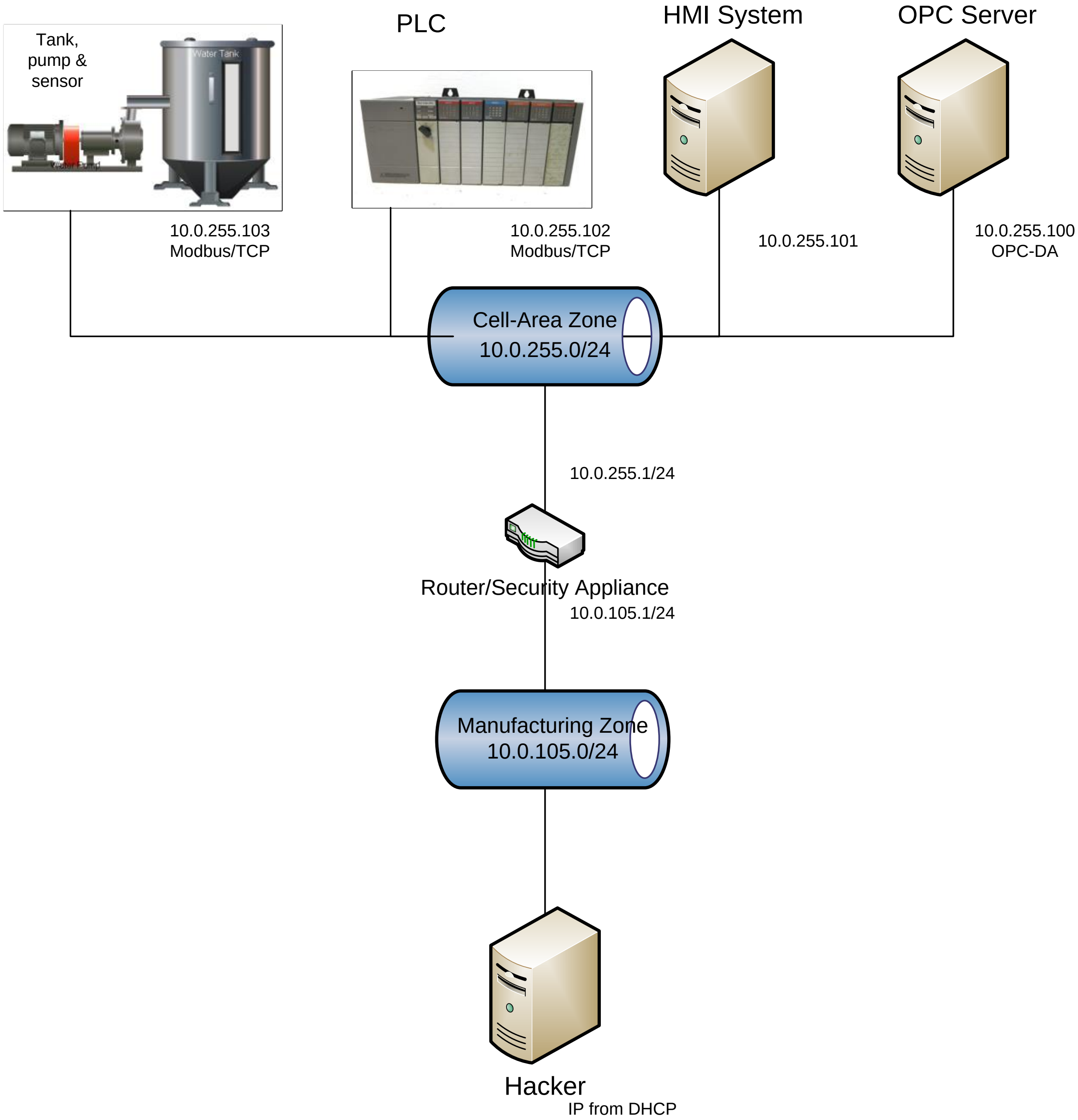
Students will use common security tools to observe how a hacker connected to the same zone as an Industrial Control System (ICS) can easily view and/or modify data being transferred within the ICS. They will then implement network segmentation by moving the ICS and client system to a different network segment. They will then observe that this prevents the hacker from observing or modifying any ICS traffic.

Setup and Deploy

Without Zoning



With Zoning


Tank, pump & sensor
Water Tank
Water Pump
PLC
HMI System
OPC Server
10.0.255.103
Modbus/TCP
10.0.255.102
Modbus/TCP
10.0.255.101
10.0.255.100
OPC-DA
Cell-Area Zone
10.0.255.0/24
10.0.255.1/24
Router/Security Appliance
10.0.105.1/24
Manufacturing Zone
10.0.105.0/24
Hacker
IP from DHCP

For More Information

- NIST 800-53r4 – Security and Privacy Controls for Federal Information Systems and Organizations
  - AC-4 – Information Flow Enforcement
  - SC-7 – Boundary Protection
- NIST 800-82r2 – Guide to Industrial Control Systems (ICS) Security
  - ICS Security Architecture – 5.1 Network Segmentation and Segregation
- SANS Best Practices
  - Secure Network Design: Micro Segmentation
- ICS-CERT Recommended Practice
  - 2.4 ICS Network Architectures

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (September 2016). *Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies*. Retrieved from https://www.us-cert.gov/sites/default/files/recommended_practices/NCCIC_ICS-CERT_Defense_in_Depth_2016_S508C.pdf.

National Institute of Standards and Technology (NIST) (April 2013). *Security and Privacy Controls for Federal Information Systems and Organizations, NIST Special Publication 800-53 Revision 4*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf.

National Institute of Standards and Technology (NIST) (May 2015). *Guide to Industrial Control Systems (ICS) Security, NIST Special Publication 800-82 Revision 2*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf.

Peterson, Brandon. (February 2016). *Secure Network Design: Micro Segmentation.* SANS Institute Information Security Reading Room. Retrieved from https://www.sans.org/reading-room/whitepapers/bestprac/secure-network-design-micro-segmentation-36775.