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 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.

Learning Outcomes

- Recognize how network segmentation is an effective form of security.
- Demonstrate how hackers can take advantage of device insecurity to intercept communications.
- Demonstrate that network segmentation restricts a hacker's ability to intercept communications.

Alignment

- 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

Systems

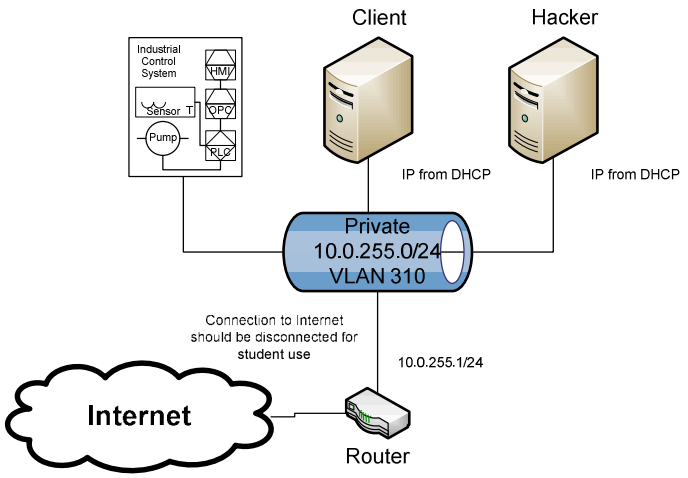
- Windows 10 – Client
- Kali Linux – Hacker
- Virtual Industrial Control System
- pfSense – Router/Firewall

General Lab

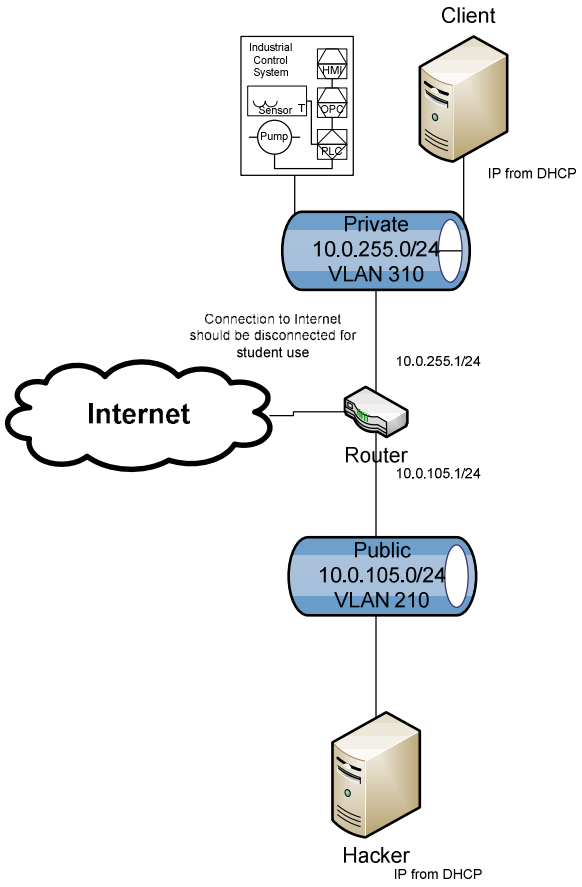
Students will use common security tools to observe how a hacker connected to the same zone as an Industrial Control System (ICS) can easily view and/or modify data being transferred within the ICS. They will then implement network segmentation by moving the ICS and client system to a different network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

Setup and Deploy

Without Zoning



With Zoning



References

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.

Secure Remote ICS Access Using a VPN

Summary

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).

Learning Outcomes

- Explain basic Virtual Private Network (VPN) concepts
- Compare different VPN technologies
- Demonstrate how the use of VPN secures network traffic

Alignment

- NIST 800-46r2 - Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security
    - Overview of Enterprise Telework and Remote Access Security - 2.2.1 Tunneling
- NIST 800-82r2 – Guide to Industrial Control Systems (ICS) Security
    - ICS Security Architecture – 5.10.2 Remote Support Access
    - Applying Security Controls to ICS – 6.2.16.2 Virtual Private Network (VPN)
- NIST 800-114r1 - User's Guide to Telework and Bring Your Own Device (BYOD) Security
    - Overview of Telework Technologies - 2.1 Remote Access Methods

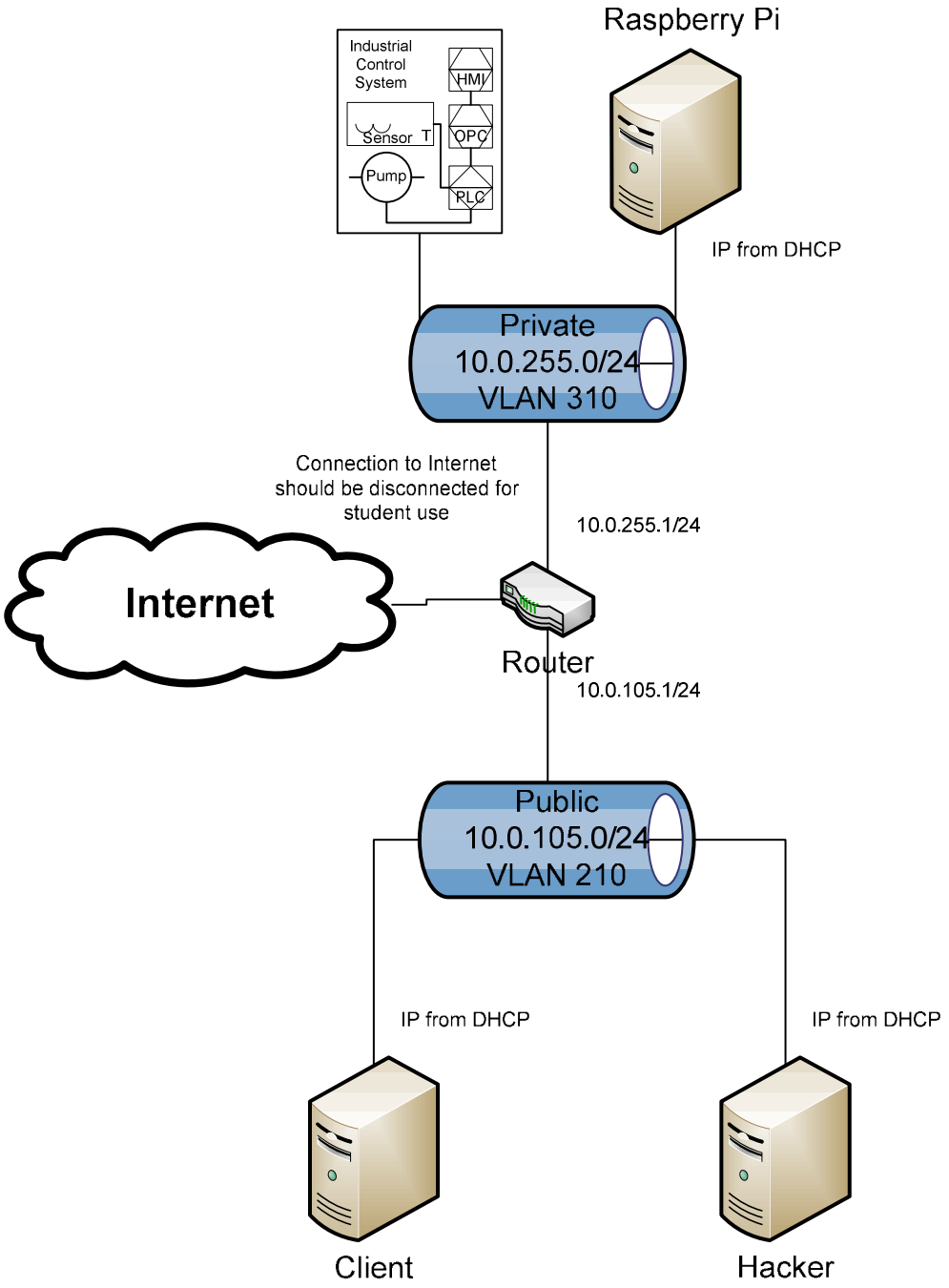
Systems

- Windows 10 – Client
- Kali Linux – Hacker
- Virtual Industrial Control System
- pfSense – Router/Firewall
- Raspberry Pi – SSH Tunnel Endpoint

General Lab

Students will connect to a device located on a remote ICS and use common security tools to observe how easily a hacker can view security credentials and other data which should be kept private. Students will then use a VPN (SSH tunnel) to connect to the same device, this time they will observe that hackers are unable to view the data being transmitted.

Setup and Deploy



References

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.

National Institute of Standards and Technology (NIST) (July 2016). *Guide to Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Security, NIST Special Publication 800-46 Revision 2*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-46r2.pdf.

National Institute of Standards and Technology (NIST) (July 2016). *User's Guide to Telework and Bring Your Own Device (BYOD) Security, NIST Special Publication 800-114 Revision 1*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-114r1.pdf.

OPC Server Security

Summary

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.

Learning Outcomes

- Explain the purpose for OPC.
- Discuss the security problems present in OPC classic.
- Describe the security improvements made in OPC-UA
- Demonstrate how hackers can attack OPC servers, communication and their host operating systems.

Alignment

- ICS-CERT – Security Implications of OPC, OLE, DCOM and RPC in Control Systems
- NIST 800-82r2– Guide to Industrial Control Systems (ICS) Security
    - ICS Security Architecture – 5.8.10 Distributed Component Object Model (DCOM)
- OPC Foundation – Practical Security Recommendations for building OPC UA Applications
    - Defense in Depth – Secure Industrial 4.0 Communications using OPC UA

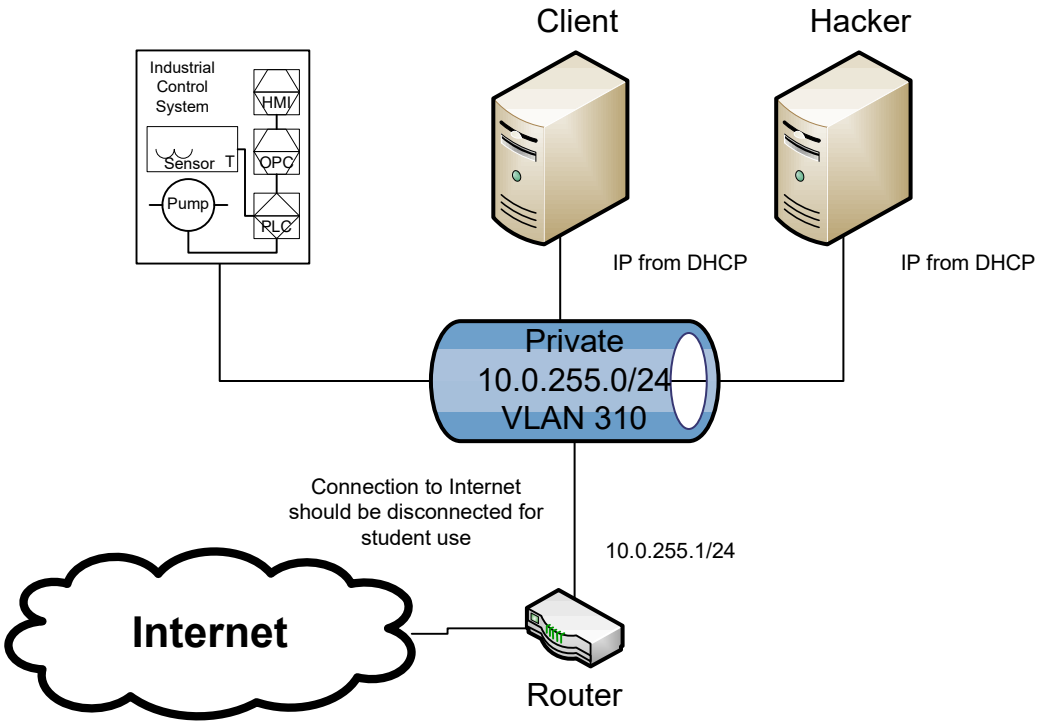
Systems

- Windows 10 – Client
- Kali Linux – Hacker
- Virtual Industrial Control System
- pfSense – Router/Firewall

General Lab

Students will use common security tools to attack a host running an OPC server. They will examine different ways in which the attack could have been prevented. Students will use common security tools to observe situations in which hackers can view and/or modify OPC server traffic. Students will implement measures to encrypt OPC server traffic and verify that those measures are effective.

Setup and Deploy



References

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (2006). *Security Implications of OPC, OLE, DCOM and RPC in Control Systems*. Retrieved from https://www.us-cert.gov/sites/default/files/recommended_practices/Security%20Implications%20for%20OPC-OLE-DCOM-RPC%20in%20ICS_S508C.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.

OPC Foundation. (June 2018). *Practical Security Recommendations for building OPC UA Applications [White paper].* Retrieved from https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Security-Advise-EN.pdf.

Industrial Networking Basics

Summary

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.

Learning Outcomes

- Summarize the history and purpose of industrial network protocols.
- Discuss the basics and security concerns associated with Modbus TCP/IP.
- Discuss the basics and security concerns associated with PROFINET.
- Discuss the basics and security concerns associated with Ethernet/IP.
- Utilize common security tools to examine industrial protocols in action.

Alignment

- NIST 800-82r2 – Guide to Industrial Control Systems (ICS) Security
    - 2.3 ICS Operation and Components
- ICS-CERT
    - ICS Advisory (ICSA-17-101-01) – Modbus Vulnerability
    - ICS Advisory (ICSA-19-283-02) – PROFINET Vulnerability
    - ICS Advisory (ICSA-13-011-03) – Ethernet/IP Vulnerability

Systems

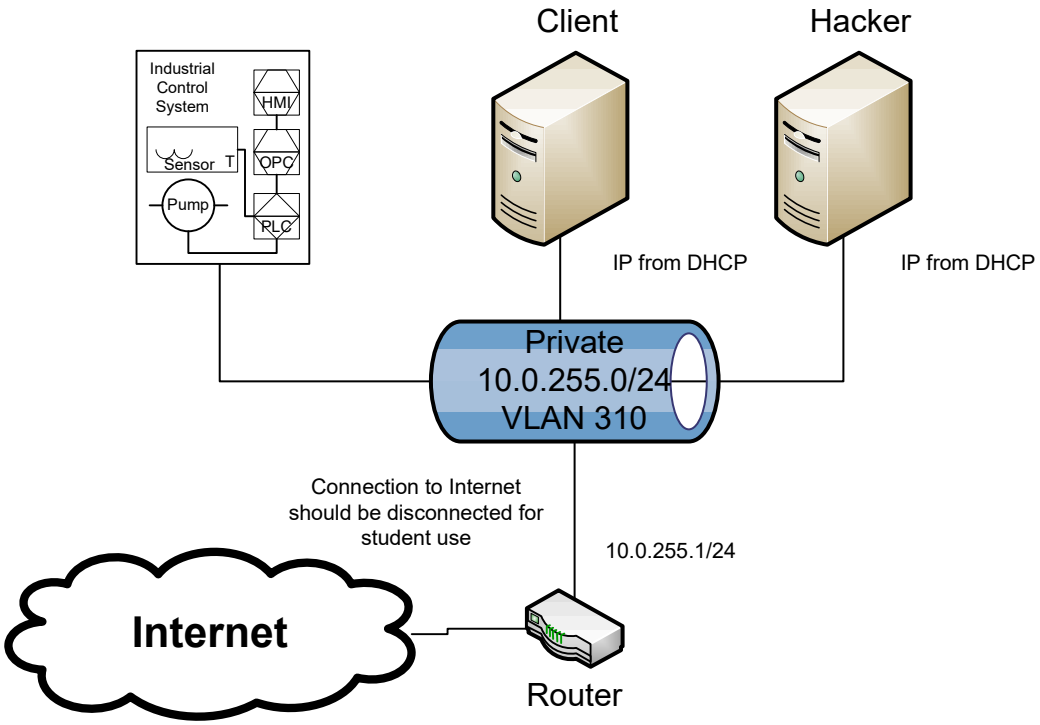
- Windows 10 – Client
- Kali Linux – Hacker
- Virtual Industrial Control System
- pfSense – Router/Firewall

General Lab

Students will transfer data to and from a virtual industrial device using Modbus TCP/IP, PROFINET and Ethernet/IP protocols. While doing this they will use common security tools to capture and/or manipulate the data while in transit.

Setup and Deploy

Basic System and Network Diagram



References

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (April 2017). *ICS Advisory (ICSA-17-101-01) Schneider Electric Modicon Modbus Protocol*. Retrieved from https://www.us-cert.gov/ics/advisories/ICSA-17-101-01.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (February 2019). *ICS Advisory (ICSA-13-011-03) Rockwell Automation ControlLogix PLC Vulnerabilities*. Retrieved from https://www.us-cert.gov/ics/advisories/ICSA-13-011-03.

Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) (April 2020). *ICS Advisory (ICSA-19-283-02) Siemens PROFINET Devices (Update E)*. Retrieved from https://www.us-cert.gov/ics/advisories/ICSA-13-011-03.

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.

Using IDS/IPS to Identify or Prevent Industrial Network Attacks

Summary

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.

Learning Outcomes

- Explain the difference between an Intrusion Detection System (IDS) and an Intrusion Prevention System (IPS).
- Discuss the usage cases that would make the use of an IDS more appropriate than the use of an IPS.
- Describe why signature based and anomaly-based IDS/IPS differ in performance and functionality.
- Demonstrate how an IDS/IPS can be used to protect industrial devices such as PLCs or OPC servers.

Alignment

- NIST 800-53r4 – Security and Privacy Controls for Federal Information Systems and Organizations
    - SI-4 – Information System Monitoring
- NIST 800-82r2 – Guide to Industrial Control Systems (ICS) Security
    - ICS Security Architecture – 5.2 Boundary Protection
- NIST 800-94 – Guide to Intrusion Detection and Prevention Systems (IDPS)
    - 2 – Intrusion Detection and Prevention Principles
    - 3 – IDPS Technologies
- ICS-CERT – Recommended Practice: Improving Industrial Control System Cybersecurity with Defense-in-Depth Strategies
    - 2.5.1 – Perimeter Security
    - 2.7.1 – Intrusion Detection and Prevention Systems

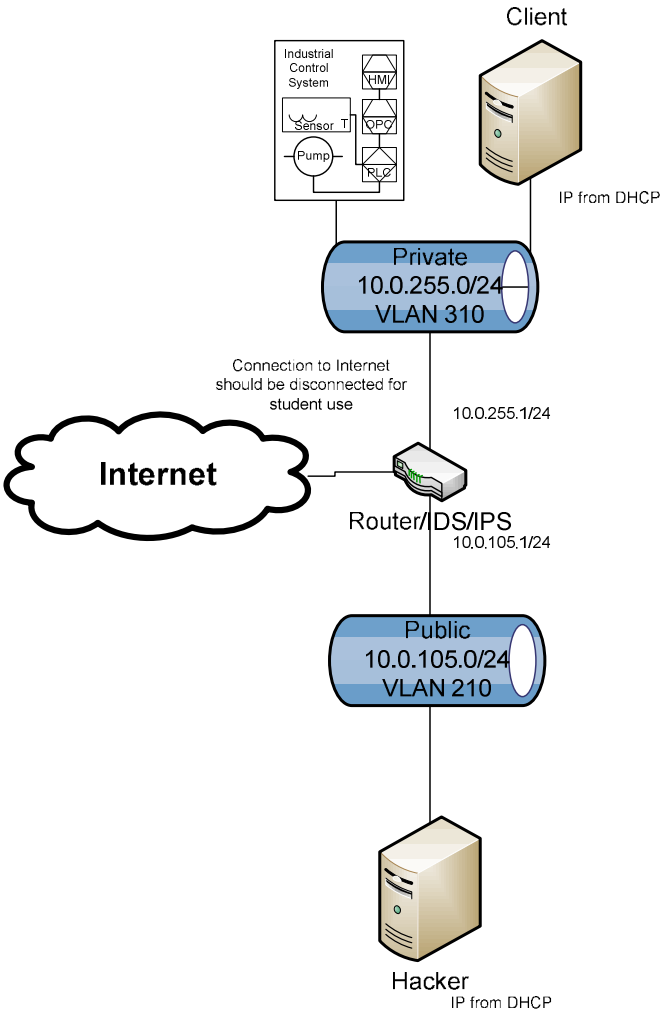
Systems

- Windows 10 – Client
- Kali Linux – Hacker
- Virtual Industrial Control System
- pfSense – Router/Firewall/IPS/IDS

General Lab

Students will start up and perform basic system configuration on an Intrusion Detection System (IDS). Students will use common security tools to attack systems on an Industrial Control System network and view the alerts captured on the IDS. Students will then modify the IDS so that it acts as an Intrusion Prevention System (IPS). They will perform the attack on the ICS an second time and observe that, unlike an IDS, the IPS prevents the attack from succeeding.

Setup and Deploy



References

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) (July 2012). *Guide to Intrusion Detection and Prevention Systems (IDPS), NIST Special Publication 800-94 Revision 1 Draft*. Retrieved from https://csrc.nist.gov/CSRC/media/Publications/sp/800-94/rev-1/draft/documents/draft_sp800-94-rev1.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.

Public Key Infrastructure and Industrial Cybersecurity

Summary

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.

Learning Outcomes

- Describe the basics of symmetric encryption.
- Describe the basics of asymmetric encryption.
- Discuss basic Public Key Infrastructure (PKI) concepts.
- Demonstrate how the implementation of PKI can increase the security of industrial networks and devices.

Alignment

- NIST 800-32 – Introduction to Public Key Technology and the Federal PKI Infrastructure
    - 2 – Background
    - 3 – Public Key Infrastructures
- NIST 800-53r4 – Security and Privacy Controls for Federal Information Systems and Organizations
    - SC-17 – Public Key Infrastructure Certificates
- NIST 800-82r2 – Guide to Industrial Control Systems (ICS) Security
    - ICS Security Architecture – 6.2.7 Identification and Authentication
    - IA-5(2) – Authenticator Management – PKI Authentication
- OPC Foundation – Practical Security Recommendations for building OPC UA Applications
    - Defense in Depth – Secure Industrial 4.0 Communications using OPC UA

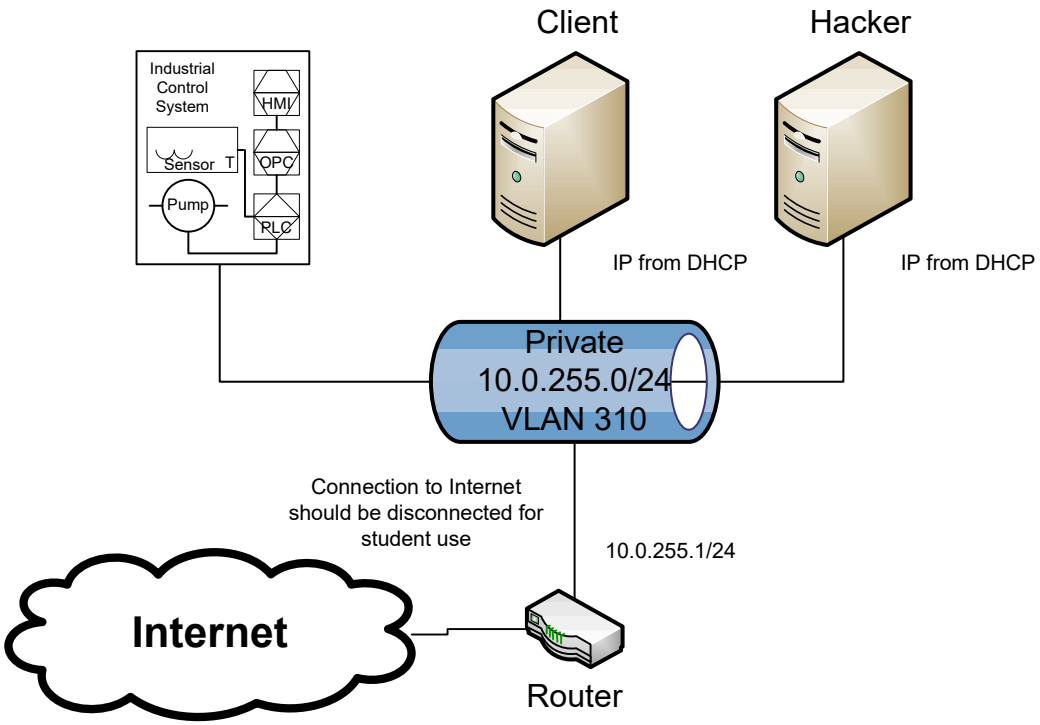
Systems

- Windows 10 – Client
- Kali Linux – Hacker
- Virtual Industrial Control System
- pfSense – Router/Firewall

General Lab

Students will use common security tools to observe security problems that can exist when PKI is not it use in a network. Students will request and issue a certificate. Students will install the certificate on an industrial device. Students will again use common security tools and this time observe that security has increased because of the use of a certificate and PKI.

Setup and Deploy



References

National Institute of Standards and Technology (NIST) (February 2001). *Introduction to Public Key Technology and the Federal PKI Infrastructure, NIST Special Publication 800-32*. Retrieved from https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=151247.

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.

OPC Foundation. (June 2018). *Practical Security Recommendations for building OPC UA Applications [White paper].* Retrieved from https://opcfoundation.org/wp-content/uploads/2017/11/OPC-UA-Security-Advise-EN.pdf.