ICS / SCADA Cybersecurity

**Protocols:**

**Modbus**: TCP port 502

* Created as a serial-based protocol to be utilized with its programmable logic controllers (PLCs)
* Most common ICS protocol
* Now the serial-based protocol is encapsulated inside of a TCP header and transmitted over ethernet
* Modbus packet frame contains 2 sections
  + Application Data Unit (ADU)
    - Address
    - PDU
    - Error Checking Method
  + Protocol Data Unit (PDU)
    - Function code
    - Data sections

**Ethernet / IP:** TCP and UDP port 44818 or TCP and UDP port 2222

* EtherNet / IP is built on the Common Industrial Protocol (CIP).
* Port 2222 was implemented for implicit and explicit messaging.
  + Explicit messaging is referred to as client/server messaging
  + Implicit messaging is referred to as I/O messages
* The commands, data points, and messages are provided in EtherNet/IP’s CIP frames
* CIP frames include:
  + A CIP Device Profiles Layer
  + Application Layer
  + Presentation Layer
  + Sessions Layer
* The rest of the packet is comprised of EtherNet/IP frames that set up the CIP frames to be transmitted

**DNP3:** TCP port 20000

* Primarily used in power and water utilities in North America.
* Developed for communications between data acquisition systems and remote devices
* Primarily used within Supervisory Control and Data Acquisition (SCADA) for control centers to communicate with remote substations.
* Configured in a master/slave configuration
  + The control center would be the SCADA master
  + Substation would have the remote terminal units (RTUs) inside it
* Designed to traversea variety of mediums
  + Microwave
  + Spread-spectrum wireless
  + Dial-up lines
  + Twisted pair
  + Leased lines

**SIEMENS**

* S7comms, or Step 7 communications
* Implemented on an ISO protocol that is not open and has very tight controls
* For the 200/300 families of PLCs, you can find some basic info about the protocol via a Wireshark dissector

**BACnet**

* One of the largest building automation protocols is BACnet (Building Automation and Control Networks)
* BACnet is an ASHARE standard, number 135.1, and is maintained by ASHARE
* Has defined services that allow building devices to communicate with each other
* Practical application are not limited to HVAC, companies have used building automation protocols to control:
  + Generation units
  + Elevators
  + Lighting controls
  + Fire suppression and alarm systems
  + Access control systems

**Modbus Protocol Types:**

**Modbus RTU:**

* Serial communication protocol that connects different devices on the same network

**ModbusTCP:**

* Uses TCP/IP protocols to communicate via an Intranet or Internet environment
* The Modbus device can be connected using an Ethernet port on the gateway
* We can make a query using any standard Modbus Scanner to extract the value from a Modbus device
* All requests are sent via TCP/IP on port 502
* Modbus protocol defines a PDU hat is independent of the underlying communications layer
* Modbus TRU is the most commonly used and is a binary representation of the PDU with addressing before the PDU
* Modbus ASCII is a representation of the same PDU using all printable characters

**Modbus Recon:**

* Positioned at layer 7 of the OSI model
* Provides client/server communication
* The device requesting the information is the Modbus Master
* Devices supplying the information are the Modbus Slaves
* In a standard Modbus network, there is one Master and up to 247 Slaves
  + Each with a unique Slave Address from 1 to 247
* The client (also known as the Master) device initiates a request
* Server (also known as Slave) replies
* Ex: when a Human Machine Interface (HMI) workstation requires a value from a PLC it sends a request message to start the data transfer process
  + The device running the HMI is the client/master
  + PLC is server/slave

**Data Diode:**

* Unidirectional gateways control the directional flow of information
* Direction can be changed on a schedule or by configuration setting
* Does a good job of keeping bad guys out
* Downside to unidirectional gateways is that administering devices on the other side can become tricky if not impossible
* Great for physically separating your critical systems from the outside world while still allowing information to flow up to your enterprise systems

**What to Monitor:**

* Security Events generated by security and infrastructure products:
  + Network or host-based firewalls
  + Network routers and switches
  + Malware prevention systems
  + Intrusion detection and prevention systems
  + Application monitors
  + Ideally any event generated by a security device should be relevant
* System logs:
  + Useful for tracking the status of devices and the services that are running
  + Tracks when patches are (or are not) applied
  + Useful for determining the general health of an asset
  + Validating that approved ports and services are running
  + Valuable in tracking which users (or applications) have authenticated to the asset
* Application logs:
  + Can provide a record of the activities relevant to applications running on top of the operating systems
  + Can indicate when an application is executed or terminated
  + Who logs into the application
  + Specific actions performed by users once logged