Alex Shah
EN.695.741.81.SP25 Information Assurance Analysis
Mod 14 Assignment
May 5, 2025

Part 1:

Supply Chain Risk Management (SCRM) is a tremendous cybersecurity concern for not only IT traditional networks, but for ICS/OT networks and systems as well. Understanding the scope of the Supply Chain Threat is critical.

1.) Describe what supply chain security encompasses and the associated priorities?

Supply chains are subject to risks as multiple industries and nations have their own priorities and potential to be subverted such as in cyber attacks. Supply chain risk management (SCRM) in an ICS/OT environment requires assessing and mitigating risk from multiple suppliers and often has stricter requirements due to the critical nature that ICS/OT systems operate within. ICS/OT systems have limited patch windows in deployment which makes finding vulnerabilities beforehand important. Priorities include authenticating hardware and software components, making sure they are not tampered with or have backdoors, and ensuring that the parts remain accessible and meet required performance standards. Because ICS/OT parts are often used for many years, discovering problems or vulnerabilities in components can be costly and could compromise critical systems sensitive to uptime disturbances. Trustworthiness and transparency are important priorities in choosing suppliers, and if possible redundant suppliers should be sought out. Aspen Cybersecurity notes that over reliance on a particular country or supplier could cause restrictions in obtaining certain parts that could cripple an installation or industry.

2.) Explain what are some of the obstacles to achieve supply chain security?

Reliable and secure supply chains are achieved by transparency, information, and choice according to Aspen Cybersecurity Group. Preventing compromised components for critical applications requires the supplier to be transparent about their sources and processes, and potentially a chain of custody for sensitive components. The purchaser would ideally have information about the processes involved in creating and securing the goods they are purchasing, and be aware of the risks involved in their suppliers' operations. It is also crucial to have alternatives, such as a sourcing materials from a different region. For example, changing trade agreements or risk factors can force companies to find new suppliers. Since governments and agencies often produce regulations independently, and often react slowly, supply chain security could be enhanced by several large scale changes according to Aspen. First, by expanding market competition to afford better access to parts that meet security standards, which helps address customer demand for more secure technology. Also, there should be processes for securing supply chains with better organizational risk management such as increasing security standards and employing more advanced best practices to minimize the chances of vulnerabilities introduced by suppliers. Some other proposed models include security labeling like a certification process to aid consumers, a software bill of materials, and testing centers to independently verify security of certain components.

3.) How do Original Equipment Manufacturers (OEM)/Vendors expose consumers and industrial sectors to risks and potential exploits?

Manufacturers and vendors make design decisions and use dependencies that can introduce vulnerabilities to the customer that are often difficult to detect or modify. Vendors' default settings can provide weak security that are often left in place. According to the INL, many thousands of devices are online and accessible using default passwords available through the user manual that attackers take advantage of as low hanging fruit. This can provide a point of entry that escalates into lateral movement. Vendors are also slow or resistant to acknowledge or patch known vulnerabilities. This is especially important in ICS settings where equipment and software can be used unchanged for years, this opens the door to risks where well established components are used without patches long after vulnerabilities are discovered. While it is the users's responsibility to secure the environment and isolate devices, some challenges can only be fixed by the vendor, and customers must wait for updated firmware to address exploitable flaws in their system. Vendor updates also present issues with the uptime and reliability requirements of an OT environment, and businesses can only hope the supplier performed adequate testing before deployment.

4.) What are four (4) potential supply chain risk management techniques to employ? How would you deploy them?

Employing the latest best practices and security standards can minimize risk when dealing with vendors, since even trusted vendors can be compromised or make mistakes. Though zero trust is impossible to achieve when relying on vendors, there can be some insulation to the effects of compromised components through strong security practices like secure boot and code/driver signing. Next, a continuous verification and testing process can reveal problems and vulnerabilities in components before installing them as long lived components in ICS/OT. Discovering tampering early can save on costs, and regularly performing integrity checks can discover or prevent cyber attacks on critical components. Third, suppliers might be required to perform integrity checks or have the components independently tested. This might also include a chain of custody for critical components. Lastly, oversight and transparency from the supplier should be evaluated with regular security audits and verification that they are adhering to regulations like ISO standards and certifications. The customer should confirm that the integrity checks and results from audits match expectations and the customer should be ready to have backup suppliers or testing services ready.

Part 2:

There are several ICS/OT common protocols used today. Pick four (4) from the following list of protocols: Common Industrial Protocol (CIP), MODBUS, Distributed Network Protocol 3 (DNP3), Profibus (PROcess Field BUS), Profinet (PROcess Field NETwork), Open Platform Communication (OPC), Highway Addressable Remote Transducer (HART), Inter-control Center Communication Protocol (ICCP), and Building Automation and Control Network (BACnet) and do the following; Research each protocol and tell me a bit about it, things like: what are the transmission modes, what are some of the message framing and checking methods used, what are the data and control functions, roles/purposes, implementations/architectures for using them, possible standards, classifications, strengths/weaknesses, and more. Go into a fair bit of detail, more than what appears from the first Google search or document researched. 3-4 paragraphs for each is good.

MODBUS

MODBUS has been used widely since it was introduced in 1979 to work with PLCs and is still in use today for its simplicity and support. It can now communicate over Ethernet as well as serial transmissions to support serial (RTU/ASCII), TCP/IP, and UDP transport. It uses a master/slave or client/server model where the master issues requests that the slave devices respond to in a polling cycle. MODBUS over TCP/IP using Ethernet allows for integration into more modern IT environments but comes at the cost of security where the protocol does not specifically support encryption or authentication methods in polling devices or establishing connections while being integrated into a network where attacks might leverage these weaknesses. While the serial communication methods use checks like CRC and LRC to verify the message integrity, they do not prevent malicious changes. Connections over Ethernet are also vulnerable to injection or manipulation attacks as they lack application layer validation.

MODBUS functions were designed for serial communication with slow transmission speeds when reading from analog devices and direct from registers, making MODBUS able to read and write messages between the server and clients but without any access control or metadata associated with the commands. So anyone with control over the commands on the network can communicate over the protocol and manipulate the devices.

The MODBUS standard defines a Protocol Data Unit (PDU) that includes a byte for the function code, followed by 252 bytes of function data for the slave device to use in responding to the function request defined in the function code. These types of functions might be to read or write units of data from coils, registers, or other data from memory. The slave device then uses a state flow like a state diagram depending on the request, including handling exception codes. The standard also defines an Application Data Unit (ADU) containing a PDU in order to use serial, TCP, and UDP transport to transmit the data across these layers and are tailored to each transport protocol. Each unit includes error checking for reliability, and is formed by concatenating headers and IDs with a PDU to transmit the application code and data to the slave devices over the chosen transport.

While MODBUS is not an advanced protocol and does not have inbuilt security or confidentiality guarantees, it can still be serviceable by using air gapped environments. Though recently this has been less secure, such as with Stuxnet infiltrating an air gapped system by using USB devices. MODBUS does have many drawbacks such as the lack of CIA mechanisms, no way to verify the source of a command received, and the modern integration with Ethernet may pose further integrity violations without carefully designed security measures.

OPC UA

OPC Unified Architecture is a more modern and flexible protocol than MODBUS that supports several transport methods like binary, HTTPS, and MQTT. The OPC work group was founded in 1994 from software and hardware vendors in industrial automation. OPC UA was published in 2006 and attempted to move away from depending on Windows. It supports client/server as well as publish/subscriber models and implements security measures like authentication, signing, and

encryption. The OPC group also defines an information model including types and methods to make integrating with business processes and higher levels of the Purdue model easier. For example business logic can define client specifications which are then sent to the PLC directly using the information model throughout the layers.

Unlike MODBUS, OPC UA includes methods for authentication and encryption which vastly increases security in ICS/OT environments. For example HTTPS transport using REST endpoints can use OAuth2 and other standard authentication methods. Messages are also signed and encrypted using X.509 certificates which enable trust and authentication of message signers and protects messages in transit from being read or manipulated. In addition to the communication layer to establish secure communications, the application layer authenticates users and provides access control methods such as a role based access control scheme that a company might implement and maintain for its employees and contractors. This further enhances security and provides a mechanism to log and audit events as well as detect anomalies such as with an IPS.

However security using OPC UA relies on proper implementation and mismanaged certificates or permissions can still allow an attacker to read and manipulate data as well as control systems. OPC UA seems to be designed for large scale vertical integration and smaller implementations might strip out features for convenience or simplicity that could make the protocol more insecure. There are also existing vulnerabilities that could leak sensitive information, lead to denial of service, or allow for code execution.

PROFIBUS

Similar in age and design to MODBUS, PROFIBUS was designed in Germany in 1987 for serial communication in automation deployments. In hazardous environments, the Process Automation (PA) variant communicates very slowly at 31.25 Kbps, but the power and data lines are the same two wires, which limits the power and speed, but provides assurance that extreme cases (like explosive environments) remain safe, and compared to MODBUS requires no additional containment measures. In PA, the deployment could use a star topology since the speed is limited.

In Decentralized Peripherals (DP), an RS-485 serial connection and powered links/repeaters are used to support up to 32 devices on a single bus and can reach speeds of 12 Mbps. Newer implementations like PROFINET can also use Ethernet and like the other protocols, it can connect and relay data from slave devices like PLCs and sensors. Like MODBUS, PROFIBUS is a simple protocol and includes no direct methods for authentication or encryption. However modern approaches using PROFINET and associated services from the protocol group can use certificates to sign a container file, where the contents can be validated and authenticated. This can remedy some security concerns like the ability to verify that configurations match expectations from a trusted signer.

PROFIBUS communications can be read by anyone with access to the bus line which enables attacks like message injection, and denial of service. Integrating with Ethernet is not inherently safer, and the deployment needs to be segmented from the IT infrastructure to maintain security of the bus contents. Each frame on the line contains synchronization information to keep the serial flow of information in sequence, as well as address and data fields, and CRC integrity checks to verify the contents arrive as expected. Multiple masters can be used by rotating tokens which are passed to avoid

collisions on the serial bus. Cyclic updates can be used to read and write process variables, and it is also possible to read diagnostics and other data acyclicly.

BACnet

BACnet is a building automation system protocol designed by a refrigerant industry group and adopted by ANSI and ISO. It is widely used in “smart” buildings to control lighting, security, and HVAC controls including US government buildings. The protocol represents devices and information as predefined object types to enhance interoperability between vendors and between different product categories.

BACnet can be used over several network types like serial, Ethernet, Zigbee, and ARCnet including over standard IP networks. The BACnet/SC variant increases security at the application layer with TLS encryption (at the transport layer) over WebSockets to protect data in transit, preventing manipulation and device access. This enables existing IP infrastructure to securely add BACnet and more frequently with cloud integrations. While BACnet/SC adoption is ongoing, existing implementations have lagging security. For example, BACnet devices accept unauthenticated messages and misconfiguration can expose devices that may be directly controllable from outside the network.

In a DEFCON presentation in 2019, a security researcher was able to inject JS code into a BACnet device via a web application and use the BACnet code stored in an attached database to achieve persistence. This includes the ability to modify the BACnet device configurations and the code involved in controller applications. When the researcher contacted the BACnet group, he received no reply. In an ICS/OT environment this is an alarming response, and the vulnerable protocol is in widespread use including in government facilities.

Part 3:

Discuss three (3) ICS/OT cybersecurity concerns with the various OT proprietary and open protocols used? Support your reasoning/answer.

Many of the most widely adopted protocols are insecure or do not include security concerns in their design and implementation. MODBUS, PROFIBUS, and BACnet have their origins in older segmented serial connections. However in many ICS/OT environments like automation, modern transport over Ethernet no longer segments the ICS traffic, exposing the traffic to broader access. Without authentication and encryption, anyone who gains the ability to issue commands can read and write to devices which enables an attacker to gather information or perform actions. In the INL document, the group writes that “Common and long-established ICS protocols such as Modbus and DNP3 used throughout the power system have little or no security measures: lacking authentication capabilities, messages may be intercepted, spoofed, or altered, potentially causing a dangerous event in an operations environment”. (INL, 2016).

Even when protocols build methods for secure communications such as OPC UA using certificates and encryption to protect messages, there is room for misconfiguration or even vulnerabilities in the protocol. In some deployments, some features may be disabled for interoperability that cause security concerns, or there may be configuration issues can increase the attack surface. Default security credentials may be used that could leave installations vulnerable to opportunistic

attacks. And in these common and widely used protocols, there are current known vulnerabilities that attackers can leverage to gain access to a critical ICS/OT system. There are numerous vulnerabilities in OPC UA that can render the certificate schemes useless, provide access to sensitive data, or even allow remote code execution. There have also been demonstrated attacks against BACnet and others that are addressed over a period of time by future design decisions that don't remedy or act quickly enough to protect current deployments.

And while there are many protocols to choose from, they mostly rely on master/slave polling where commands are issued and results are gathered. There are few options for implementing access control schemes in existing deployments, as well as for logging and auditing access and diagnostics. There are some protocols like OPC UA that use certificates for authentication, but there are still fewer native options in OT that the IT side of infrastructure rely on for security such as anomaly detection, telemetry, and auditing sessions, contexts, and events. Unless skilled staff are able to integrate the system to access and monitor the OT systems, they operate independently and with limited oversight and transparency. This enables attackers to perform reconnaissance without detection, perform exfiltration and make changes without impacting logs, and prevents operators from performing accurate forensics in the event of an attack. Such events are noted by the INL, which reported "The majority [38%] of incidents were categorized as having an "unknown" access vector. In these instances, the organization was confirmed to be compromised; however, forensic evidence did not point to a method used for intrusion because of a lack of detection and monitoring capabilities within the compromised network." (INL, 2016).

Sources

Aspen Cybersecurity Group. (2020). A national cybersecurity agenda for resilient digital infrastructure. Aspen Institute. Retrieved fro JH Mod 14.

BACnet International. (n.d.). BACnet Secure Connect (BACnet/SC). https://bacnetinternational.org/bacnetsc/

Cisco. (2022, March 16). What is OPC UA and how does it manage security? https://blogs.cisco.com/industrial-iot/what-is-opc-ua-and-how-does-it-manage-security

Claroty. (n.d.). OPC UA exploit framework. GitHub. https://github.com/claroty/opcua-exploit-framework

Control.com. (n.d.). Understanding the OPC UA protocol. https://control.com/technical-articles/understanding-the-opc-ua-protocol/

Control.com. (n.d.). What is the BACnet protocol? https://control.com/technical-articles/what-is-the-bacnet-protocol/

Idaho National Laboratory. (2016). Cyber threat and vulnerability analysis of the U.S. electric sector. Mission Support Center, Idaho National Laboratory. Retrieved from JH Mod 14.

McGee, M. (2019, September 4). BACnet IoT building automation devices vulnerable to attack. ComputerWeekly. https://www.computerweekly.com/news/252468279/BACnet-IoT-building-automation-devices-vulnerable-to-attack

Modbus Organization. (n.d.). MODBUS specifications. https://modbus.org/specs.php

National Instruments. (n.d.). The MODBUS protocol in depth. https://www.ni.com/en/shop/seamlessly-connect-to-third-party-devices-and-supervisory-system/the-modbus-protocol-in-depth.html

OPC Foundation. (n.d.-a). OPC UA reference documentation. https://reference.opcfoundation.org/

OPC Foundation. (n.d.-b). About OPC technologies: OPC UA. https://opcfoundation.org/about/opc-technologies/opc-ua/

Procentec. (n.d.). PROFIBUS DP vs PA: What are the main differences? https://procentec.com/content/profibus-dp-vs-pa-what-are-the-main-differences/

PROFINET & PROFIBUS North America. (n.d.). PROFIBUS technology overview. https://us.profinet.com/technology/profibus/

PROFIBUS & PROFINET International. (2019). PROFINET security guideline. https://www.profibus.com/download/profinet-security-guideline/