CS987-Midterm

● Graded

Student

Mohammed Jawed

Total Points

50 / 50 pts

Question 1

PLC and SCADA

5 / 5 pts

✔ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Question 2

Ukraine Power Grid Attacks

5 / 5 pts

✔ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Question 3

Enterprise to OT Attack Path

5 / 5 pts

✔ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Question 4

Third Party Direct Access to OT

5 / 5 pts

✔ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Question 5

Defense in Depth

10 / 10 pts

✔ **+ 10 pts** Correct

+ 8 pts Minor mistakes

+ 5 pts Partially correct

+ 0 pts Incorrect/Not attempted

Demilitarized Zone (DMZ)

10 / 10 pts

✔ **+ 10 pts** Correct

+ 8 pts Minor mistakes

+ 5 pts Partially correct

+ 0 pts Incorrect/Not attempted

Question 7

Threat Modeling

10 / 10 pts

✔ **+ 10 pts** Correct

+ 8 pts Minor mistakes

+ 5 pts Partially correct

+ 0 pts Incorrect/Not attempted

Q1 PLC and SCADA
5 Points

A control system has a controller that receives inputs from sensors and produces output that sends commands to actuators. PLC is one such controller. SCADA is also a controller that is used with PLC often. Explain your own understanding of the differences of their roles in an industrial cyber physical process control.

The PLC In an industrial cyber-physical process plays a direct control role. It receives sensor data, processes it instantly, and sends precise commands to actuators to perform actions like adjusting machinery in real time. we can say PLC focuses on immediate control within the physical process.

On the other hand the SCADA has more of a supervisory role(like in IT companies we have Manager :)). It collects data from multiple PLCs, provides operators with a centralized interface for monitoring, and enables remote adjustments. in short, SCADA ensures high-level oversight, data logging, and coordination across the system.

5 Points

Ukraine had two well publicized attacks on their power grid in 2015 and 2016 which we discussed in our lectures. Please provide 5 bullet point style statements indicating the *most* significant differences between the two attacks from your recollection of the information provided in the lecture materials.

I used Prof. Shukla's live session notes and some references from the book "This is How They Tell Me The World Ends" to address the aforementioned issue.
1. Attack Method: While the 2016 attack employed Industroyer malware to automate commands within the power grid, the 2015 attack used a manual remote control to turn off substations.
2. Malware Used: In 2015, attackers used BlackEnergy malware to gain initial access, then in 2016, they used Industroyer, a malware specifically made for industrial control systems.
3. Impact Scope: The 2016 attack targeted the larger power transmission network, whereas the 2015 attack manually targeted several substations.
4. Restoration Time: In 2015, operators manually restored power in a matter of hours, but the 2016 attack necessitated extensive reconfiguration.
5. Level of Sophistication: The 2016 attack showed higher sophistication with custom-built malware targeting specific power protocols, unlike the primarily remote control-based approach in 2015.

Q3 Enterprise to OT Attack Path
5 Points

We explained through a series of diagrams how an attack on an IT environment in an enterprise can move to the OT network and compromise the cyber physical systems to have a kinetic impact (explosion or malfunction etc). Recall that series of diagrams, and explain in no more than 3 compact sentences what are the most critical elements of such attack paths?

The first step in an attack vector from enterprise IT to OT is for the attacker to compromise the IT network, usually using malware or phishing or even through USB. To get to the OT environment, they then proceed laterally via shared services or unreliable network parts.
Once in the OT environment, they take advantage of ICS vulnerabilities to control cyber-physical systems, which could have kinetic effects like industrial process disruptions or equipment failures.

5 Points

One of the major attack surface in OT infrastructure is provided by the fact that organizations often provide direct access to 3rd party vendors so the vendor can directly configure, patch or update the controllers, sensors etc. This is considered very harmful practice for proper security of OT systems. Please explain in your own words what would be the alternative way to let vendors work on the OT equipment remotely (note that some OT systems are in remote geographical regions and hence need servicing remotely).

I would install a secure, managed access gateway to allow safe remote access to OT equipment by outside vendors. To ensure only authorized access, vendors would connect over a VPN with multi-factor authentication(it can be combination of password and time-based one-time password (TOTP) from an authenticator app). Additionally, I would set up a jump server in a DMZ, which logs all activities, tracking and documenting each session for security audits. This setup limits vendor access strictly to necessary systems, reducing the risks of direct access while enabling essential remote maintenance in a secure, controlled manner.

10 Points

Suppose you have to advice a small factory owner (who has industrial automation to produce some components in a discrete manufacturing plant). He also has some IT for accounting, billing, inventory, payroll etc. He also uses his mobile phone to get visualization of what is happening in his plant floor in real-time. Write 5 bullet points to state what are the most important security measures you would advise him to implement keeping the "defense in Depth" concept in mind?

1) Zone wise separation: Separate IT functions, like billing and payroll, from OT systems to create isolated network zones. This minimizes the risk of an IT breach affecting OT, especially against lateral movement from IT to OT systems.
2) Controlled Access to OT Systems: Require multi-factor authentication (as mentioned in Q4) for anyone accessing OT systems, including mobile users, to ensure only authorized personnel can monitor or control factory operations remotely.
3) Endpoint Security: Deploy anti-malware and regular updates across IT and OT systems, as well as mobile devices used for factory monitoring. Restrict mobile device users from installing non-approved apps, potentially using an MDM solution to enforce these controls.
4) Monitoring and Logging : Set up real-time monitoring and logging on IT and OT networks to quickly detect unusual activity, and include a dashboard for visibility, transparency, and data availability for analysis.
5) Regular Data Backups and Incident Response Plan: Schedule regular backups for critical OT and IT data, and develop a comprehensive incident response plan so the factory can recover quickly from potential disruptions.

10 Points

Explain why the Purdue model in its network architecture has a demilitarized zone? What are the major functions of the DMZ? (Write brief, to-the-point, and in your own words).

n the Purdue Model, the DMZ serves as a security barrier between the IT and control networks. By restricting direct contact, the DMZ lowers the risk of IT-based cyber threats compromising critical OT systems. Its main functions include controlling and monitoring data flow between IT and OT, isolating network traffic to prevent unauthorized access, and hosting secure services like data historians or remote access servers to enable safe information sharing.

Q7 Threat Modeling

10 Points

List 5 different types of attacks that you think are the most likely to occur on a PLC in a power generation plant?

Following are 5 types of attacks which i can think of related to PLC in a power generation plant,
1. Malware Injection via PLC Programming: attackers could modify or insert malicious code directly in the PLC's programming, causing unauthorized actions like disruptions in power generation and potentially leading to shutdowns.
2. Unauthorized Access: malicious actor could gain access to the PLC to change control parameters, risking instability in power output or even equipment damage.
3. Denial of Service : A DoS attack could overwhelm the PLC, stopping it from controlling essential systems like turbines or generators.
4. Replay Attacks: Attackers might replay previous commands to disrupt operations, causing the PLC to repeat actions that destabilize the power supply.
5. Firmware Manipulation: Hackers might tamper with PLC firmware, introducing faulty commands that lead to incorrect power generation and potential safety risks.