CS987-Final

● Graded

Student

Mohammed Jawed

Total Points

50 / 50 pts

Question 1

OT Security Essentials

15 / 15 pts

Part (i)

✓ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Part (ii)

✓ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Part (iii)

✓ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Question 2

Risk Assessment

15 / 15 pts

Part (i)

✓ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Part (ii)

✓ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Part (iii)

✓ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Question 3

IACS Security Life Cycle

10 / 10 pts

✓ **+ 10 pts** Correct

+ 8 pts Minor mistakes

+ 5 pts Partial correct

+ 2 pts Attempt

+ 0 pts Incorrect/Not attempted

Question 4

Risk vs. Security Control Tradeoff

10 / 10 pts

Part (i)

✓ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Part (ii)

✓ **+ 5 pts** Correct

+ 3 pts Partially correct

+ 0 pts Incorrect/Not attempted

Q1 OT Security Essentials

15 Points

(i) Enumerate top 3 cyber threats faced by OT environments in today's threat landscape? (Top 3 according to your understanding of the threat environment)

Following are the top 3 cyber threats faced by OT environments(I have added examples similar to prof. Shukla's, sir),
1. Ransomware Attacks: Ransomware has become a big problem for OT environments. It can halt operations completely and cause massive financial damage, like what happened with Norsk Hydro.
2. Unauthorized Remote Access: I would identify that attackers exploit misconfigured firewalls and weak remote access controls to break into OT systems monitored remotely.
3. Supply Chain Attacks: I would assess the risk of attackers using vulnerabilities in third-party vendors or software to infiltrate OT systems, similar to the SolarWinds attack happened and i would not like to repeat it in my OT env.

(ii) For each of the 3 cyber threats you enumerated above, what are the mitigating controls that you would implement in order to reduce the risk associated with the threat?

1. Ransomware Attacks: I would set up regular offline backups, enforce strict access controls, and segment the network to isolate OT systems. I would also deploy EDR solutions and update software frequently to close vulnerabilities.
2. Unauthorized Remote Access: I would secure remote access using MFA, configure firewalls properly, and use encrypted VPNs. I would also monitor remote access logs regularly to catch unusual activity of course i will log monitoring tools in place, minimum human intervenes.
3. Supply Chain Attacks: I would assess vendor risks, keep third-party software updated, and restrict vendor access to critical OT systems. I would also implement application whitelisting to block unauthorized software.

(iii) Why is encryption not common in the communications between OT devices such as between sensors to PLCs or between PLCs and SCADA?

Encryption is not common in OT device communications because OT systems prioritize low latency and high reliability, which encryption can impact. Many OT protocols were designed years ago without security in mind and lacked built-in encryption. Additionally, the resource-constrained nature of many OT devices, such as sensors and PLCs, makes it challenging to implement encryption without affecting performance.

Q2 Risk Assessment

15 Points

Suppose your friend runs a small factory where he has a 4-stage assembly pipeline each stage being controlled by separate PLCs, and the PLCs communicate with a SCADA system on one side and with sensors and actuators on the other side. The PLC and SCADA are communicating over a local LAN network (as against point-to-point connection). The LAN is isolated from the enterprise LAN with a firewall. Your friend asks you to do a cyber risk assessment of the factory. Answer the following questions in that context:

(i) Enumerate a list of cyber threats to this small factory?

1.Unauthorized Access: Attackers exploit weak authentication on the LAN or PLCs to take control of the assembly pipeline.
2.Ransomware: Ransomware targeting the SCADA system or PLCs disrupts operations and halts production.
3.Network Spoofing or MITM Attacks: Attackers intercept or alter communications between PLCs and the SCADA system on the LAN.
4.Malware Injection: Malware enters through infected USB drives or engineering laptops connected to the LAN.
5.Insider Threats: Malicious or careless employees compromise system security by bypassing firewalls or introducing vulnerabilities.
6.Denial of Service (DoS): Attackers overload the LAN, disrupting communication between PLCs and SCADA systems.
7.Supply Chain Exploits: Vulnerabilities in third-party software or firmware of PLCs or SCADA systems are exploited by attackers.

(ii) Explain how you would estimate the likelihood of these threats being realized on this set up?

To estimate the likelihood of these threats,
1. Evaluate Existing Vulnerabilities: I would assess vulnerabilities in the LAN, SCADA, and PLC systems, such as weak authentication or outdated firmware. These vulnerabilities increase the probability of a successful attack.
2. Analyze Threat Exposure: I would consider factors like how often external devices (e.g., USBs or laptops) are connected and the effectiveness of firewall configurations. Frequent exposure to external devices or poorly configured firewalls raises the likelihood of threats.
3. Review Historical Incidents: I would examine past incidents in similar setups to understand how often such threats have materialized in comparable environments.
4. Assess Security Controls: I would evaluate the strength of existing controls,

such as network segmentation and access restrictions. Weak controls would indicate a higher likelihood of threats.

(iii) How would you estimate the overall cyber risk to the factory?

1. Identify Threats and Vulnerabilities: I would list the key threats (e.g., ransomware, unauthorized access) and map them to specific vulnerabilities in the factory setup, such as weak firewall configurations or unpatched PLC firmware.
2. Evaluate Likelihood and Impact: I might consider assigning a likelihood score to each threat using past incident data, exposure levels, and existing controls. Then, I would assess the potential impact on production, financial losses, and safety.
3. Calculate Risk: Using a risk formula, I would multiply the likelihood of each threat by its potential impact (Risk = Likelihood × Impact) to quantify the risk for each scenario.
4. Summarize in a Risk Matrix: I would use a risk matrix to present the combined results, categorizing risks as high, medium, or low based on their scores. This makes it easy to see the overall risk level and prioritize mitigation efforts.
5. Factor in Mitigation Measures: Reevaluate the risks considering current controls like firewalls and isolation, and adjust the overall risk level accordingly.

Q3 IACS Security Life Cycle

10 Points

IACS Cyber Security Life Cycle has multiple phases.
(i) What are these different phases?

The IACS Cybersecurity Lifecycle consists of the following phases:

1. Assess Phase: Identifies and evaluates risks through high-level and detailed risk assessments, and classifies assets into security zones or conduits.
2. Develop and Implement Phase: Defines policies, selects countermeasures, and implements technical and non-technical controls to achieve the target security level.
3. Maintain Phase: Audits and tests countermeasures regularly, updates policies, and adapts to new threats to ensure security levels are maintained.
4. Continuous Processes: Monitors the Cybersecurity Management System (CSMS), conducts regular training, and improves processes based on audit findings and incident reviews.

(ii) What are the activities involved in each of these phases?

1. Assess Phase:
- Perform high-level and detailed risk assessments to identify threats and vulnerabilities.
- Allocate assets to security zones or conduits based on their criticality.

2. Develop and Implement Phase:
- Define cybersecurity policies and select appropriate countermeasures.
- Train personnel to implement and maintain these measures effectively.

3. Maintain Phase:
- Conduct regular audits and tests to ensure controls meet security objectives.
- Update cybersecurity policies and measures based on new threats and audit findings.

4. Continuous Processes:
- Monitor incident logs and cybersecurity metrics for anomalies.
- Update the CSMS and conduct regular staff training.

Q4 Risk vs. Security Control Tradeoff

10 Points

Cyber Security risk can be reduced by tightening control on the systems, people and processes. However, such tightening has costs associated with it. As a result, one cannot go on tightening indefinitely to reduce cyber risk.

(i) How does one arrive at a trade-off?

Following are few main points i will consider to arrive at a trade-off:
1. Assess Risk vs Cost: I evaluate the likelihood and impact of potential risks and compare them to the costs of implementing controls. Using a risk matrix helps visualize where additional controls are justified.
2. Find Optimal Security Level: I would identify where the cost of additional controls equals the risk reduction. Beyond this point, further controls would have diminishing returns and may not be cost-effective.

(ii) What are the considerations as a cyber security professional you should have when deciding on the trade-off point?

When deciding on the trade-off point, I would consider:
1. Criticality of Assets: I would prioritize securing critical assets, such as the SCADA system in an OT setup, where disruptions could lead to operational or safety risks.
2. Risk Tolerance: I would align the level of controls with the organization’s risk appetite, ensuring risks are reduced to an acceptable level without overburdening resources.
3. Cost vs. Benefit: I would compare the cost of implementing additional controls with the potential impact and likelihood of a cyber incident to find a balance.
4. Operational Impact: I would ensure controls do not hinder productivity or create unnecessary delays in the operational environment.
5. Compliance Requirements: I would ensure any controls implemented meet industry regulations/standards to avoid non-compliance penalties.