Master 2 IoT Security and Cybersecurity

Evaluation Exam – Model Solution

Academic Year 2025–2026

Section A: Multiple Choice Questions

Question	**Correct Answer**
Q1	**b)** A group of compromised devices under remote control
Q2	**b)** Client/Server (REST)
Q3	**a)** Unauthorized firmware updates
Q4	**b)** Protect data confidentiality and integrity
Q5	**c)** Middleware layer
Q6	**b)** Updating device code with improved security measures
Q7	**d)** Hydra
Q8	**b)** User credentials
Q9	**b)** It can use certificates, tokens, or passwords
Q10	**a)** Discovering active hosts and open ports

Section B: Short Answer Questions

Q1. Definition of IoT Cybersecurity

IoT cybersecurity refers to the set of technologies, policies, and practices used to protect IoT devices, networks, and the data they generate from cyber attacks, unauthorized access, and data breaches.

Q2. IoT Communication Protocols and Weaknesses

- **MQTT**: Vulnerable to DoS attacks if authentication and rate limiting are not enforced.
- **CoAP**: Susceptible to replay and spoofing attacks when DTLS is not enabled.
- **HTTP**: High overhead and vulnerable to eavesdropping if used without TLS.

Q3. Symmetric vs Asymmetric Encryption

Symmetric encryption uses a single shared secret key and is lightweight and fast, making it suitable for constrained IoT devices, while asymmetric encryption uses public/private key pairs, providing stronger authentication but at higher computational cost.

Q4. Role of IDS in IoT Networks

Intrusion Detection Systems monitor network traffic and device behavior to detect anomalies, attacks, or unauthorized access attempts, allowing early detection and response to security incidents.

Q5. Replay Attack

A replay attack occurs when an attacker captures valid communication packets and retransmits them to gain unauthorized access; it can be mitigated using nonces, timestamps, and session tokens.

Q6. IoT Monitoring Tools

- **Wireshark**: Captures and analyzes network traffic.
- **Prometheus**: Collects system and service metrics.
- **Grafana**: Visualizes monitoring data through dashboards.

Section C: Practical and Problem-Solving

Q1. MQTT Communication vs DoS Attack

Metric	**Normal MQTT**	**Under DoS Attack**
CPU Usage	Low and stable	High and unstable
Latency	Minimal	High message delay
Availability	Broker responsive	Broker may crash or refuse connections

Q2. Code Analysis and Vulnerabilities

Logic Explanation: The code repeatedly publishes temperature data to an MQTT broker without authentication or encryption, using QoS 0.

Vulnerabilities:

- No authentication or authorization
- Unencrypted communication on port 1883

Security Improvements:

- Enable TLS on port 8883
- Use client authentication with certificates or credentials

Q3. Role of PKI in IoT Authentication

Public Key Infrastructure (PKI) enables secure authentication by using public/private key pairs and digital certificates issued by a trusted Certificate Authority (CA), forming a trust chain that verifies device identity and prevents impersonation.

Q4. Smart Home Attack Vectors and Mitigations

- **Attack Vector:** Man-in-the-Middle attack on local broker **Mitigation:** Enforce TLS encryption and certificate validation
- **Attack Vector:** Weak authentication on sensors **Mitigation:** Strong credentials and mutual authentication