IoT security scenarios

Objective:

Work collaboratively in groups of 2-3 to analyze a real-world IoT system. The activity will help you understand the architecture, identify security threats, and explore countermeasures based on professional resources.

Instructions:

1. **Select an IoT Security Scenario:** Choose one of the IoT scenarios from the list below for your group to analyze.
2. **Perform the Following Tasks:**
    - **Architecture**:
        - Sketch a high-level architecture of the system.
        - Include key components (e.g., devices, sensors, communication channels, backend systems).
        - Highlight user interactions and data flows.
    - **Security Threats**:
        - Identify **2-3 security threats** applicable to the chosen scenario.
        - Provide brief descriptions of how each threat could compromise the system.
    - **Security Measures**:
        - Find and recommend **security measures** or **good practices** to address the identified threats.
3. **Prepare a Presentation:**
    - **Presentation**:
        - Present your findings in **5–10 minutes**.

List of IoT Security Scenarios

1. Network of Charging Stations for Electric Vehicles (EVs)

- Example: A public network of EV charging stations connected to a central management system for processing payments, monitoring energy usage, and updating firmware.
- Focus on:
    - Threats such as unauthorized access to charging stations, tampering with firmware, or denial-of-service (DoS) attacks.
    - Impacts on user data privacy, station availability, and potential damage to the power grid.
    - Countermeasures like secure communication protocols, access control mechanisms, and firmware integrity checks.

2. Remote Patient Monitoring System

- Example: Wearable IoT devices for cardiac monitoring, collecting real-time data and transmitting it to the hospital's information system (HIS) for diagnosis and alerts.
- Focus on:
    - Threats such as man-in-the-middle attacks during data transmission, unauthorized access to patient records, and device tampering.
    - Impacts on patient privacy, medical outcomes, and potential loss of trust in healthcare systems.
    - Countermeasures like end-to-end encryption, strong authentication mechanisms, and device firmware security.

3. Delivery of Goods via Drones

- Example: A fleet of autonomous drones used by logistics companies to deliver packages to customers, communicating with a central control system for navigation and updates.
- Focus on:
    - Threats like GPS spoofing, jamming of communication signals, and unauthorized control of drones.
    - Impacts on package security, operational disruptions, and public safety risks.
    - Countermeasures such as secure communication protocols, anti-spoofing GPS mechanisms, and geofencing technologies.

4. Traffic Light Control System in a Smart City

- Example: IoT-enabled traffic lights connected to a city's traffic management system to optimize traffic flow and reduce congestion.
- Focus on:
    - Threats such as signal tampering, denial-of-service attacks, and unauthorized changes to traffic control algorithms.
    - Impacts on public safety, emergency response times, and economic costs due to traffic disruptions.
    - Countermeasures including network segmentation, real-time monitoring, and firmware security updates

5. Smart Building Automation System

- Example: IoT devices managing HVAC systems, lighting, access control, and energy monitoring in a commercial building.
- Focus on:
    - Threats such as unauthorized access to building systems, denial-of-service attacks, and data breaches from connected sensors.
    - Impacts on occupant safety, operational continuity, and energy efficiency.
    - Countermeasures like role-based access control, data encryption, and secure IoT gateways.

Deliverable

1. **Presentation**:
    - Overview of the system.
    - Key findings and recommendations.