Unit 1: Introduction to IoT and Mobile Security & IoT Architecture and Protocols

1. What are the key components of the IoT ecosystem?
2. Why is security important in IoT and mobile devices?
3. Explain the major challenges and vulnerabilities in IoT and mobile environments.
4. Describe the different layers of IoT architecture.
5. What are the communication protocols used in IoT (MQTT, CoAP, etc.)?
6. Explain the security considerations at each layer of the IoT architecture.
7. What are the risks of insecure IoT architecture?
8. Discuss how data confidentiality and integrity are maintained in IoT communications.
9. How do IoT devices authenticate themselves in a network?
10. What role does encryption play in securing IoT networks?
11. What are the threats associated with IoT networks and mobile devices?
12. How do IoT applications ensure secure data exchange?
13. Compare and contrast IoT security challenges with traditional network security.
14. What measures can be taken to prevent unauthorized access to IoT devices?
15. Explain how IoT security frameworks help in risk mitigation.

Unit 2: Mobile Devices in IoT Networks & IoT Device Security

1. What is the role of mobile devices in IoT ecosystems?
2. Explain mobile-to-IoT interactions and their security implications.
3. How are mobile applications integrated with IoT devices and platforms?
4. Describe security measures for IoT devices such as authentication and encryption.
5. What are the access control mechanisms used for IoT security?
6. Explain the significance of firmware and software update mechanisms for IoT devices.
7. What is a secure boot, and why is it important for IoT devices?
8. How does hardware-based security enhance IoT device protection?
9. Explain tamper resistance techniques used in IoT security.
10. How does endpoint security impact mobile and IoT security?
11. What are the risks of outdated software in IoT devices?
12. How can manufacturers ensure IoT device security at the hardware level?
13. Explain how data encryption protects communication between mobile devices and IoT.
14. What are the best practices for securing mobile apps interacting with IoT devices?
15. Discuss the security risks associated with mobile APIs in IoT environments.

Unit 3: IoT Network Security & Mobile App Security for IoT

1. How can IoT communication protocols be secured?
2. What are the common threats to IoT networks, and how can they be mitigated?
3. Explain how TLS/SSL and DTLS secure IoT communications.
4. What is the role of network segmentation and isolation in IoT security?
5. How do DDoS attacks affect IoT networks, and what are the mitigation strategies?
6. What security risks are associated with eavesdropping on IoT networks?
7. How should mobile applications be designed to ensure secure IoT interactions?
8. What are the secure coding practices for mobile application development in IoT?
9. How does API security impact mobile-to-IoT communication?
10. Explain data encryption techniques for securing mobile-IoT interactions.
11. How does firewall configuration help in securing IoT networks?
12. What techniques are used for conducting vulnerability assessments of IoT networks?
13. How do intrusion detection systems (IDS) and intrusion prevention systems (IPS) help secure IoT environments?
14. What are the security challenges in integrating mobile devices with IoT platforms?
15. Explain how security audits are conducted for IoT and mobile environments.

Unit 4: Privacy & Data Protection in IoT and Mobile & IoT and Mobile Threat Landscape

1. What are the major data privacy concerns in IoT ecosystems?
2. How do data protection regulations like GDPR and CCPA apply to IoT security?
3. What are the best practices for securely handling and storing sensitive data in IoT?
4. What are the most common threats and attacks targeting IoT and mobile environments?
5. Explain case studies of major security incidents and breaches in IoT and mobile security.
6. How is vulnerability assessment performed for IoT and mobile devices?
7. What are the key risk management strategies for IoT and mobile security?
8. How does mobile malware affect IoT networks?
9. What tools and techniques are used for analyzing mobile and IoT malware?
10. How is penetration testing performed on IoT and mobile devices?
11. What are the security risks of third-party mobile applications interacting with IoT?
12. How does forensic analysis help in investigating IoT security incidents?
13. How can organizations implement effective security policies for IoT and mobile security?
14. What are the key challenges in responding to security incidents in IoT networks?
15. How do organizations implement disaster recovery plans for IoT and mobile environments?