Homework Assignment 6: Mobile and Embedded Device Security

1. What are the differences between tablets, smartphones, wearables, and web-based computers?

2. Name and describe at least three connectivity methods used by mobile devices.

3. Compare BYOD, COPE, and CYOD enterprise deployment models. What are the pros and cons of each?

4. Identify two risks associated with mobile device vulnerabilities and explain why they are serious concerns.

5. What are two examples of connection-based vulnerabilities and how can they be exploited?

6. Explain what sideloading is and why it poses a security risk.

7. Describe three mobile device protection features that can help if a device is lost or stolen.

8. What is containerization, and how does it help secure data on a mobile device?

9. What are the differences between MDM, MAM, MCM, and UEM in managing mobile devices?

10. Define what an embedded system is and give two examples of devices that use embedded systems.

11. What is a field-programmable gate array (FPGA), and how is it used in embedded systems?

12. What security risks are associated with Internet of Things (IoT) devices?

13. What challenges arise when trying to use cryptography on embedded or IoT devices?

14. List three steps that can be taken to harden SCADA or ICS environments.

15. What is the difference between static and dynamic code analysis, and why are both important in secure software development?