IoT Security and Privacy

TrustZone

Instructions:

1. Note: Blue text points to a web link. Ctrl + Click to follow link.
2. Answers to all questions must be put into **ONE** document. That is, every time, each student can only submit one report document, answering all questions of this assignment.
3. Students must put answers following each question in this assignment. The instructor will not grade a report with only answers in it and the student gets zero for such an assignment. An assignment report must include original questions.
4. Students MUST submit the finished assignment in either Microsoft Word or pdf format. The doc must be submitted as ONE standalone file and cannot be tarred or zipped into a container.

Review questions:

1. We can counter all possible attacks. (Yes/No)

2. SoC refers to System on a chip. (Yes/No)

3. A risk analysis outcome can be that probability of an attack too low to be worth defending. (Yes/No)

4. Class-break attacks refer to attacks that break a whole generation, or class, of devices. (Yes/No)

5. Since security features may not implement product specific functionalities, they are not important to manufacturers. (Yes/No)

6. Every device can be broken. (Yes/No)

7. TrustZone is for system-wide security and protects any part of the system. (Yes/No)

8. In TrustZone, any SoC hardware and software resources exist in two worlds: secure world and normal (non-secure) world. (Yes/No)

9. In TrustZone, a single ARM core of some version can execute code from both normal world and secure world in a time sliced fashion. (Yes/No)

10. All ARM chips support TrustZone. (Yes/No)

11. Monitor mode of TrustZone is responsible for switches between secure world and normal world. (Yes/No)

12. In secure boot, the public key of the vendor can be stored in a device for authenticating software and should be kept confidential. (Yes/No)

13. Monitor mode of TrustZone is a gatekeeper that manages the switches between the Secure World and Non-secure World. (Yes/No)

14. The public key for the root of trust can be stored in On-SoC One-Time-Programmable (OTP) hardware. (Yes/No)

15. ARM provides a standardized software API, called the TrustZone API (TZAPI). (Yes/No)

Essay question

1. Please introduces how a secure system with TrustZone boots.

2. Please discuss how TrustZone can be used to secure an IoT device.