IoT Security and Privacy

Secure Bootstrapping

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. Trust in a human is often based on identity. (Yes/No)

2. Code identity can be achieved through a cryptographic hash over just the source code of the software. The calculation of the code identity is often called measurement. (Yes/No)

3. We measure a software after it starts. (Yes/No)

4. These measurements of booting software form chain of trust. (Yes/No)

5. Who or what measures the first piece of code S_1 is the root of trust. (Yes/No)

6. Trusted boot is the same as secure boot. (Yes/No)

7. Measuring code identity is sufficient to guarantee security. (Yes/No)

8. Secure boot halts the boot process if unauthorized code is detected. (Yes/No)

9. IBM 4758 family of cryptographic co-processors have Tamper-responding storage in battery-backed RAM (BBRAM). (Yes/No)

10. In full disk encryption, the disk encryption keys can be sealed to measurements representing the user's operating system. (Yes/No)

11. In attestation, a remote party (verifier) would like to learn the security status of a local system (attestor). (Yes/No)

12. We can build perfect secure software. (Yes/No)

13. The root of trust can be built upon secret private key embedded in hardware. (Yes/No)

14. To achieve tamper resistant and tamper-responding properties, we can use packaging for resisting and responding to physical penetration and fluctuations in power and temperature. (Yes/No)

15. A TPM chip is tamper resistant. (Yes/No)

Essay question

1. We may use certificate chains to secure measurements. Please introduces how it works.

2. Please discuss how TPM-Based measurement uses hash chains to secure measurements.

3. Please introduce the BitLocker boot process. How is the whole disk encryption key is obtained?

4. Please discuss the TPM-Based attestation protocol.

5. What is cuckoo attack against TPM attestation?

6. Please design a strategy so that changes to the IoT firmware can be detected by the IoT device itself. Please discuss what to do next after the detection of the firmware in terms of IoT security.