Device security

- 1.1 What does "root of trust" mean? What attacks are prevented by using a "root of trust"?
- 1.2 What is/are the cryptographic primitive(s) used to create a "root of trust"? Explain its/their purpose(s).
- 1.3 Describe the steps needed to perform a firmware update.
- 1.4 Give two/three benefits for using a trusted environment? Explain these benefits from a security point of view.

Device security

1.1 What does **root of trust** mean? What attacks are prevented by using a **root of trust**?

Device security

1.1 What does **root of trust** mean? What attacks are prevented by using a **root of trust**?

Roots of trust (RoT) is a set of functions usually stored in a trusted computing module that is always trusted by the computer's operating system.

RoT prevents rootkits, prevents unauthorized tampering with storage drives, prevents unauthorized firmware modifications

Device security

1.2 What is/are the cryptographic primitive(s) used to create a "root of trust"? Explain its/their purpose(s).

Device security

1.2 What is/are the cryptographic primitive(s) used to create a "root of trust"? Explain its/their purpose(s).

- **Hash functions:** A hash function is a unidirectional function used to fingerprint data. In the context of RoT it's used for verifying data integrity.
- **Digital signatures (DS)**: Are a particular application of public key cryptography where keys are used to certify that a message is linked to a specific key. In RoT context DS are used to authenticate data and certify its origin. DS are used to sign data MACs, not the data itself.

Question

- What properties does the root hash provide?

Question

- What properties does the root hash provide?
  - Platform integrity - i.e., assurances that the software running on the device has not been modified by unknown parties.

Question

- What properties does the root hash provide?
  - Platform integrity - i.e., assurances that the software running on the device has not been modified by unknown parties.
- How can we provide authentication to the data?

Question

- What properties does the root hash provide?
  - Platform integrity - i.e., assurances that the software running on the device has not been modified by unknown parties.
- How can we provide authentication to the data?
  - Use a key to sign the root hash

Question

- What properties does the root hash provide?
  - Platform integrity - i.e., assurances that the software running on the device has not been modified by unknown parties.
- How can we provide authentication to the data?
  - Use a key to sign the root hash
- Can this method be applied to all types of partitions? Why?

Question

- What properties does the root hash provide?
  - Platform integrity - i.e., assurances that the software running on the device has not been modified by unknown parties.
- How can we provide authentication to the data?
  - Use a key to sign the root hash
- Can this method be applied to all types of partitions? Why?
  - Just to read-only. Read-write partitions' HASH values would change whenever data is modified.

Device security

Describe necessary steps to perform a firmware update

Device security

Describe necessary steps to perform a firmware update

1. Boot in a secure/trusted mode

Device security

Describe necessary steps to perform a firmware update

1. Boot in a secure/trusted mode
2. Check the signature of the firmware update using trusted ROM key

Device security

Describe necessary steps to perform a firmware update

1. Boot in a secure/trusted mode
2. Check the signature of the firmware update using trusted ROM key
3. Install firmware update

Device security

Describe necessary steps to perform a firmware update

1. Boot in a secure/trusted mode
2. Check the signature of the firmware update using trusted ROM key
3. Install firmware update
4. Update the bootloader to match the new firmware

Device security

Describe necessary steps to perform a firmware update

1. Boot in a secure/trusted mode
2. Check the signature of the firmware update using trusted ROM key
3. Install firmware update
4. Update the bootloader to match the new firmware

Any thing else?

Device security

Well…

Firmware downgrade attacks: installing an older firmware which might have (known) vulnerabilities.

Give some solutions to prevent this!

How to prevent a rollback attack?

- Counter based version control
- Blacklist/Whitelist based version control
- eFuses
- Apple nonce based protocol (i.e. APTicket): random unique value generated at every restore and signed by Apple
- …

Device security

1.4 Give two/three benefits for using a trusted environment? Explain these benefits from a security point of view.

Device security

1.4 Give two/three benefits for using a trusted environment? Explain these benefits from a security point of view.

1. Prevent rootkits and malicious code from taking control of the device by checking the integrity of the bootloader…
2. Prevent unauthorised modification/use of a device by digitally signing the firmware…
3. Protect data on the device by encrypting…
4. Protect sensitive data: cryptographic keys, credit cards, personal data, … by making sure it's not released to the OS unless specific conditions are met…