Untrusted Platforms

Software Provider doesn’t trust owner of HW

- Cloud computing
- Digital Rights Management
- Proprietary software
- Online Gaming
- E Voting
- SmartGrid

Remote Attestation:

Prove to remote party that you are running specific program. Example: proving that smartgrid is running the software that they installed.

Digital Rights Management:

The downloading software should respect rights management policy before the movie is allowed to be downloaded.

Trusted Hardware:

\[
\left( PH, SH \right)
\]

Trusted Hardware
The trusted Hardware has a Private Key that is secure. That is, even the owner of hardware cannot access it.

\[ Ci = \text{Cert}(ST, \Pi || h_1) \]
\[ CT = \text{Cert}(SH, PT || h) \]
\[ CH = \text{Cert}(SD, PH) \]

- Secure Attestation is a boot process
- Apple Stores verifies 2 things.
  - Identity of software running
  - Whether you are running right software or not
- Apple receives \( Ci, CT, CH \) and it verifies the hash of Terra in CT and also verifies the hash of iTunes stored in Ci. If everything is OK, it encrypts the music with Public Key of iTunes. Pi and Si are generated on the fly by iTunes.
Verifying the hash later

- We can verify the hash later. Terra can store hash of individual pages of iTune.
- Hashes are checked on demand
- This way, application can start early.
- When it accesses a page that hasn’t got correct hash, it kills the application