Untrusted Platforms: Software provider doesn’t trust owner of hardware on which application runs

- Cloud Computing
- Digital Rights Management
- Proprietary software: ex: wifi hardware & driver
- Smart Grid: ex: the meter is in user’s house, the power company may not trust the meter’s proof (secret)
- Online Gaming
- E-voting

Remote Attestation:

Prove to remote party that you are running a specific program.

At the start time, the software may be safe, but it may run some dangerous codes later on.

Secure Attestation

Before transfer Terra from the disk to the memory, it will build a Hash Table first.

We cannot find another program with the same hash.

Process:

- The iTunes wants to be certified, first generateds a public/private key pair.
- iTunes passes its public key to Terra.
- Terra generates and signs a certificate containing $S_T$ and the binding of iTunes’ public key to the hash.
The remote server verifies that the lowest certificate in the chain (\(C_H\)), certifying the hardware, is from a trusted certificate authority and that the certificate has not been revoked.

- It verifies that all hashes in the certificate chain are on the remote server’s list of authorized software.
- It verifies that the hash of the iTunes’ attested storage, provided in the topmost certificate, is on a list of authorized applications.
- At the end, both parties share a secret session key. Otherwise, a malicious user could wait for attestation to complete, then reboot the machine into an untrusted state without the remote server’s knowledge.

If the attacker replaces the Terra, Apple Store will know it.

1) Identity of the software the Apple store is keeping to know
2) Independent decision whether Terra is replaced or not.

It is cheap for us to generate \(P_{H'}\), but it is expensive for the attacker to guess \(P_{H'}\).

Other examples:

- District Voting Center
- Gaming
Hash Function is standard. There are several standard hash functions. In the protocol, the Terra will tell the Apple Store which standard function it is using.

When starting iTunes VM, it will load the list to the memory.

Whenever Terra reboot, it will generate a new pair of secure sequence.