

CSE-509: System Security

Spring'2009

4/13/2009

Lecture Notes: Trusted Computing

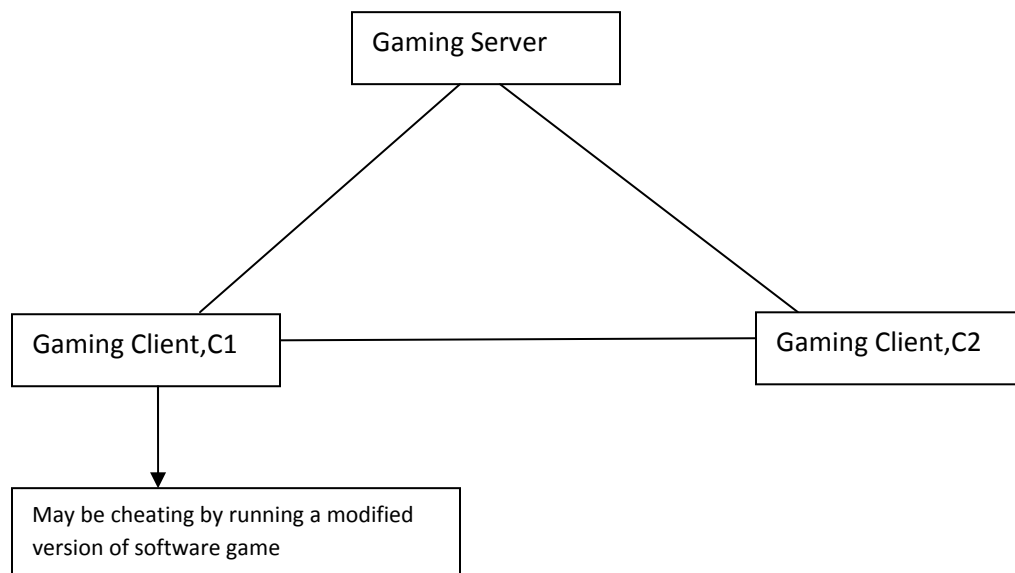
Trusted Computing – “Platform Owner” is not trusted

Application of Trusted Computing

1. Video Games e.g X-BOX where platform owner can modify software/hardware to cheat in online gaming arena
2. Cloud Computing – Online Application distributed among untrusted nodes
3. Online Movie/Content distribution
4. Closed-Box Applications used in Cell phones, wireless drivers used in devices should be tamper resistant which controls the wireless transmitter frequency.
5. Personal Data Management
6. Online Banking on high security application on low security architecture.

Remote Attestation in Trusted Computing

Game Example



Goal: To verify software running on Client Machine C1 using Remote Attestation

The Client C1 has following keys embedded saved in tamper resistant trusted hardware chip :

1. S1 : Private Key
2. P1: Public Key
3. C1: Certificate issued by a CA with Signature on public key P1

The Client C2 has following keys embedded saved in tamper resistant trusted hardware chip :

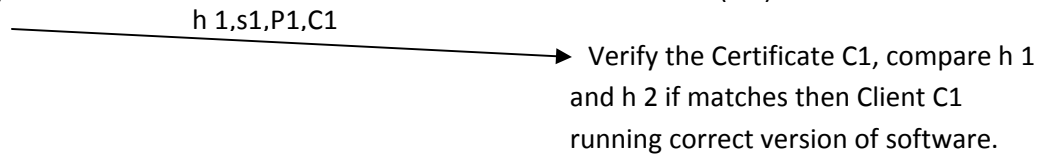
1. S2 : Private Key
2. P2: Public Key
3. C2: Certificate issued by a CA with Signature on public key P2

Client Machine C1

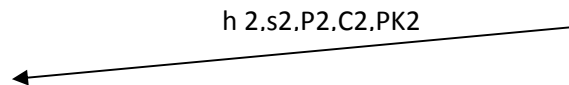
h 1= HASH(CD1)
s 1 = SIG S1 (h 1)

Client Machine C2

h 2= HASH(CD2)
s2 = SIG S2 (h 2)



Genrate PK2 and SK2



Verify the Certificate C1, compare h 1 and h 2 if matches then Client C2 running correct version of software.

Genrate PK1 and SK1

