CSE 509 Class Note for 4/12

Terra Goals

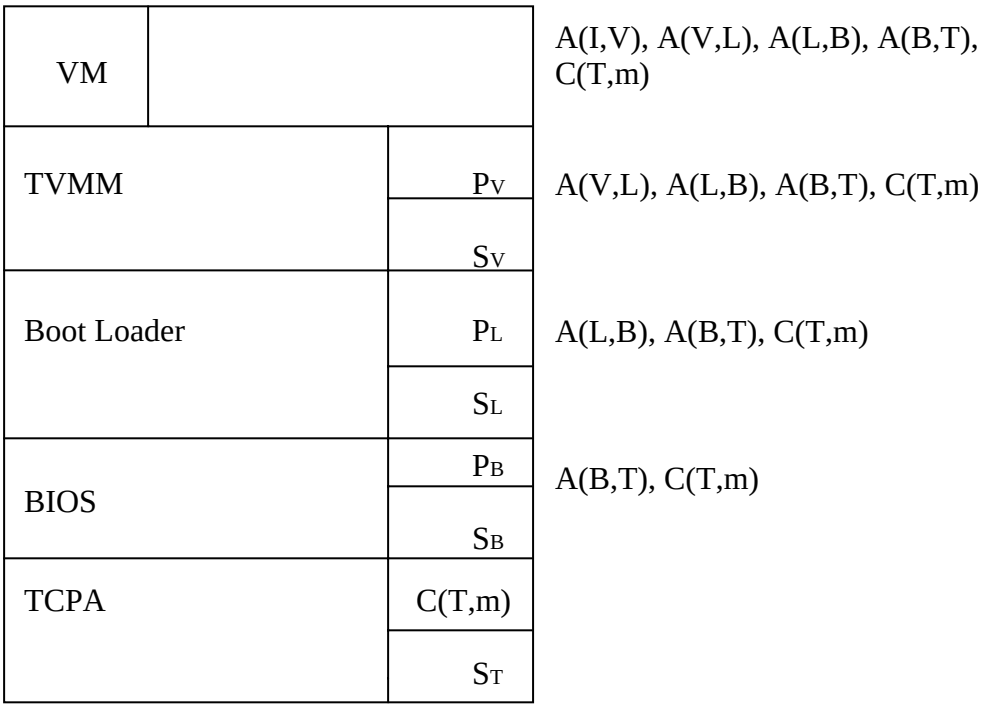
- root secure
- remote attestation
    - requires trusting
        - TCPA hardware security
        - Entire software stack
        - Software security of entire stack
        - Hardware manufacture
        - Software makers
        - Other hardware hacks

- Remote Attestation
    - Act of proving to a remote party what software you are running
      → add special tamper-proof HW to machine

    - Bios obtains certificate from TCPA stating that BIOS is running

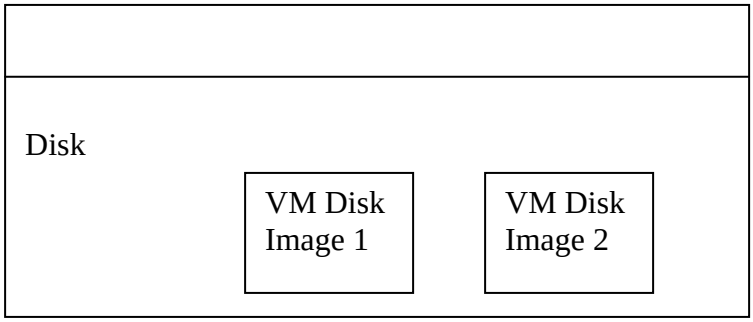
Identity of BIOS = hash(BIOS machine code)
→ must not has mutable parts of BIOS
→ Sign binary image and then run.

Note. $A(B,T) = Sig(S_T , P_B || h(B))$

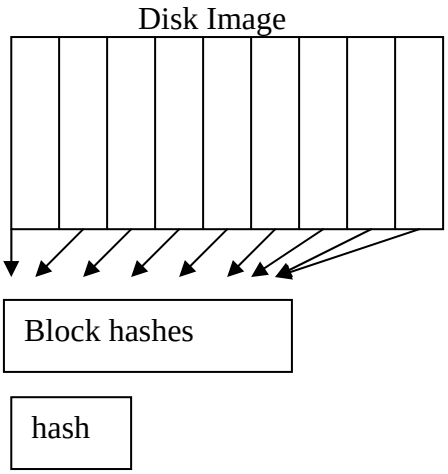


C(T,m) → certificate from m that P_T is public key of TCPA hardware.

Virtual machine

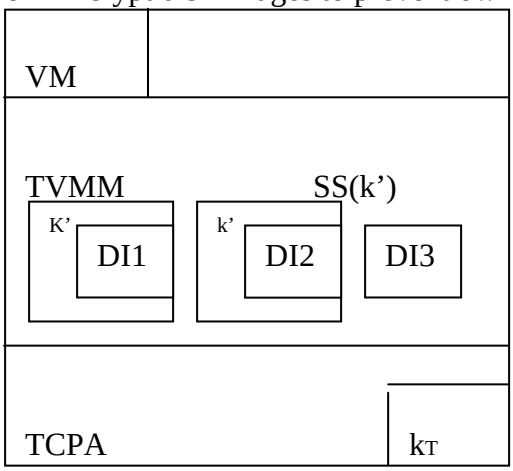


Attesting to large disk images



1. load hash table and master hash
2. verify master hash against hash table
   on page load → compare hash of page to entry in table

- Root Secure
  - Encrypt disk images to prevent owner from seeing contents



- cannot store key on disk (unencrypted)

- sealed storage

$SS(m) = E(k_T, h(requestor||m)$

→ may also prevent tampering of disks using MACs.