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

- Remote Attestation
  o Act of proving to a remote party what software you are running
    → add special tamper-proof HW to machine
  o 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. \( A(B,T) = \text{Sig}(ST, PB \parallel h(B)) \)

<table>
<thead>
<tr>
<th>VM</th>
<th>A(I, V), A(V, L), A(L, B), A(B, T), C(T, m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>TVMM</td>
<td>( PV )</td>
</tr>
<tr>
<td></td>
<td>( SV )</td>
</tr>
<tr>
<td>Boot Loader</td>
<td>( PL )</td>
</tr>
<tr>
<td></td>
<td>( SL )</td>
</tr>
<tr>
<td>BIOS</td>
<td>( PB )</td>
</tr>
<tr>
<td></td>
<td>( SB )</td>
</tr>
<tr>
<td>TCPA</td>
<td>( C(T, m) )</td>
</tr>
<tr>
<td></td>
<td>( ST )</td>
</tr>
</tbody>
</table>

\( C(T, m) \rightarrow \text{certificate from m that Pr is public key of TCPA hardware.} \)
Virtual machine

Directory

VM Disk Image 1
VM Disk Image 2

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

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

may also prevent tampering of disks using MACs.