Terra TVMM Continuation 4/12

**Terra Goals**
- root secure
- remote attestation

**Remote Attestation**
- Act of proving to remote party what software you are running.
  => add special tamper-proof hardware to machine

Identify of Bios = hash (BIOS machine Code)

\[ A_T^B = \text{Sig} (S_T, P_B \| h(B)) \]

Attestation generated by T for B
must not hash mutable parts of BIOS
=> sign binary image and then run

An idea would be to have OS separate mutable from immutable image, but, good OS have difficult time doing this.

**Attesting to Large Disk Images**

<table>
<thead>
<tr>
<th>Virtual Machine</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disk</td>
</tr>
<tr>
<td>VM Disk Image 1</td>
</tr>
</tbody>
</table>
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.

**Remote Attestation**
- Requires trusting
  - TCPA hardware security
  - Entire software stack
  - Software security of entire stack
  - Hardware manufacturer
  - Other hardware hacks

**Root Secure**
- Encrypt disk images to prevent owner from seeing contents
- Cannot store key on disk (unencrypted)
- May also prevent tampering of disk using MACs
Sealed Storage

\[ SS(M) = E_{KT}(h(requestor) \parallel M) \]