1 FLICKER

1.1 Remote Attestation

How does one prove to a remote party that some predetermined code was run on a particular set of inputs? We use the TPM’s \textit{extend} functionality to achieve this.

- We enter the PAL (Piece of Application Logic) by invoking the SKINIT instruction, which resets the system state (clears registers etc.) and does an \textit{extend(PAL)}.
- The PAL does \textit{extend(input)}, \textit{extend(output)} and \textit{extend(0)}.
- When the remote party asks for a quote, the system returns \text{Sig} (S_{tpm}, h || \text{NULL}). The PAL also returns the output for the party to verify.

1.2 Can the PAL be trusted?

Not always.

1.3 What can we do to keep it safe?

Sandbox it. e.g An inline reference monitor. We can prevent special instructions, and also limit the execution time by enforcing a limit on the number of jumps.

1.4 Differences between FLICKER and TERRA

<table>
<thead>
<tr>
<th></th>
<th>Flicker</th>
<th>Terra</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup time is high</td>
<td>VM overhead</td>
<td>Large TCB</td>
</tr>
<tr>
<td>Small TCB</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS agnostic</td>
<td></td>
<td>Software configuration needs to be agreed upon</td>
</tr>
</tbody>
</table>

November 29, 2010