Trusted Path Routing

Sensitive flows bypass insecure / potentially compromised network devices

- Boot integrity not verified
- Actively exhibits Indicators of Compromise
- Software isn’t patched
- Doesn’t have hardware cryptoprocessor
- Currently unattested

End User
- Finance
- Military
- Government
- Medical
Trusted Path Routing - Centralized

Take the green path to/from subnet { }

<attestation> Event Stream subscription

Verifier
Use `<boot-verified>` topology for subnet `{}`

* If Composite Evidence appraises `<boot-verified>`, add link to `<boot-verified>` L3 topology
<attestation> Event Stream

• Fresh, streaming Evidence
  • Based on draft-ietf-rats-yang-tpm-charra & YANG subscriptions (RFC-8639)

• YANG Notifications
  • <tpm12-attestation>
  • <tpm20-attestation>
  • <tpm-extend>

  Objects defined in draft-ietf-rats-yang-tpm-charra

  Measurements which have extended a PCR

• <replay> of all Notifications since boot

• Verifier can subscribe to PCRs / Notifications of interest via XPATH

• Extensible with other Notifications
### Extensible high level abstraction via YANG identities
- `<compromised>`
- `<unverified>`
- `<boot-verified>`
- Refinement/extension?

### Mappable to more formal and non-IETF constructs

### Passport can contain a set of trustworthiness levels

#### Figure 2: Attested Objects

draft-fedorkow-rats-network-device-attestation

<table>
<thead>
<tr>
<th>Function</th>
<th>Allocated PCR #</th>
<th>Code</th>
<th>Configuration</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIOS Static Root of Trust, plus embedded Option ROMs and drivers</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Pluggable Option ROMs to initialize and configure add-in devices</td>
<td>2</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Boot Manager code and configuration (UEFI)</td>
<td>4</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Vendor Specific Measurements</td>
<td>6</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Secure Boot Policy. This PCR records keys and configuration used to validate the OS loader</td>
<td>7</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS Loader (e.g GRUB2 for Linux)</td>
<td>8</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Reserved for OS (e.g. Linux IMA)</td>
<td>10</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

...
Composite Evidence

- Attester distribution of provably fresh appraisals