Compromise trustworthy visibility in working systems
Remote ATtestation ProcedureS (RATS) BOF
IETF #103

Eric Voit
Principal Engineer – Cisco Systems, Inc.
evoit@cisco.com
Nov-2018
Agenda

• Remotely attesting switches and routers
• ~ Demo
Remotely attesting switches and routers

**Known Good Value** — *is it correct?* - compare attested measurement against verifiable known good value

**Imprint Value** — *has it changed?* - compare attested measurement against initial snapshot value

**Event Occurrence** — *did it happen?* – monitor device for attested events that should not occur
More than just at Boot time

Platform  Verification of the secure boot and the identity of the device.
Software  Checks of the software files and in-memory contents. Logs.
Hardware  Inventory of hardware components as expected.
Configuration  Unexpected changes in the device configuration? Logs.

Asynchronous!

- Inserted hardware
- ACL configuration
- Filtered Syslog entries
- Configured keys
- Users, and their permissions
- Checksum of software binaries
- Running software processes
- Adjacent L2 / L3 neighbors
- Interface state (up/down)
Demo
(Screen-shots of Demo due to time constraints)

<table>
<thead>
<tr>
<th>Device Risk</th>
<th>Hostname</th>
<th>IP Address</th>
<th>Software</th>
<th>Hardware</th>
<th>Config</th>
<th>Platform</th>
</tr>
</thead>
<tbody>
<tr>
<td>High Risk</td>
<td>apic-wa.west</td>
<td>10.122.82.225</td>
<td>✗</td>
<td></td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>High Risk</td>
<td>apic-api-west</td>
<td>10.7.24.3</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td>apic-cisco.com</td>
<td>172.18.151.177</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>High Risk</td>
<td>pbr-edge-3562-1</td>
<td>172.19.103.4</td>
<td>✗</td>
<td>✗</td>
<td>✗</td>
<td></td>
</tr>
<tr>
<td>Low Risk</td>
<td>apic-api-east</td>
<td>10.7.30.200</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OK</td>
<td>apic-cisco.com</td>
<td>10.122.83.24</td>
<td>✗</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
~Demo

(Screen-shots of Demo due to time constraints)

More info
Thank you!