

**Compromise trustworthy visibility in
working systems**

Remote ATtestation ProcedureS (RATS) BOF

IETF #103

Eric Voit

Principal Engineer – Cisco Systems, Inc.

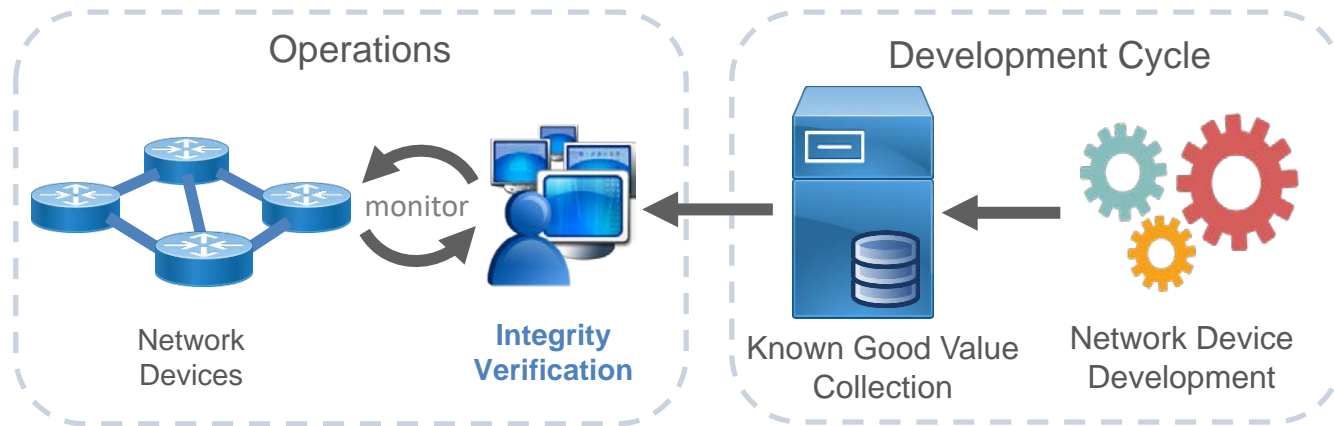
evoit@cisco.com

Nov-2018

Agenda

- Remotely attesting switches and routers
- ~ Demo

Remotely attesting switches and routers



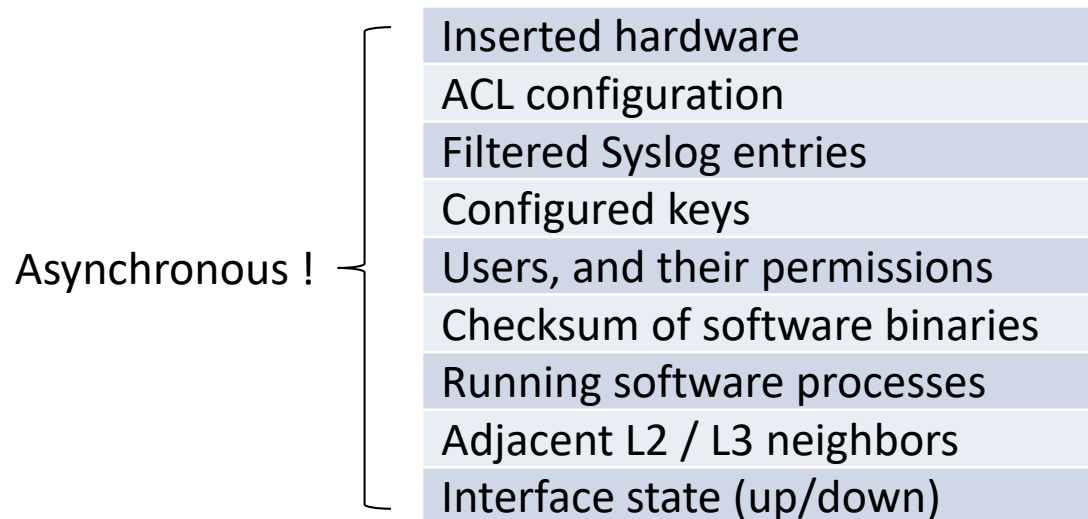
Known Good Value – **is it correct?** - compare attested measurement against verifiable know good value

Imprint Value – **has it changed?** - compare attested measurement against initial snap shot value

Event Occurrence – **did it happen?** – monitor device for attested events that should not occur

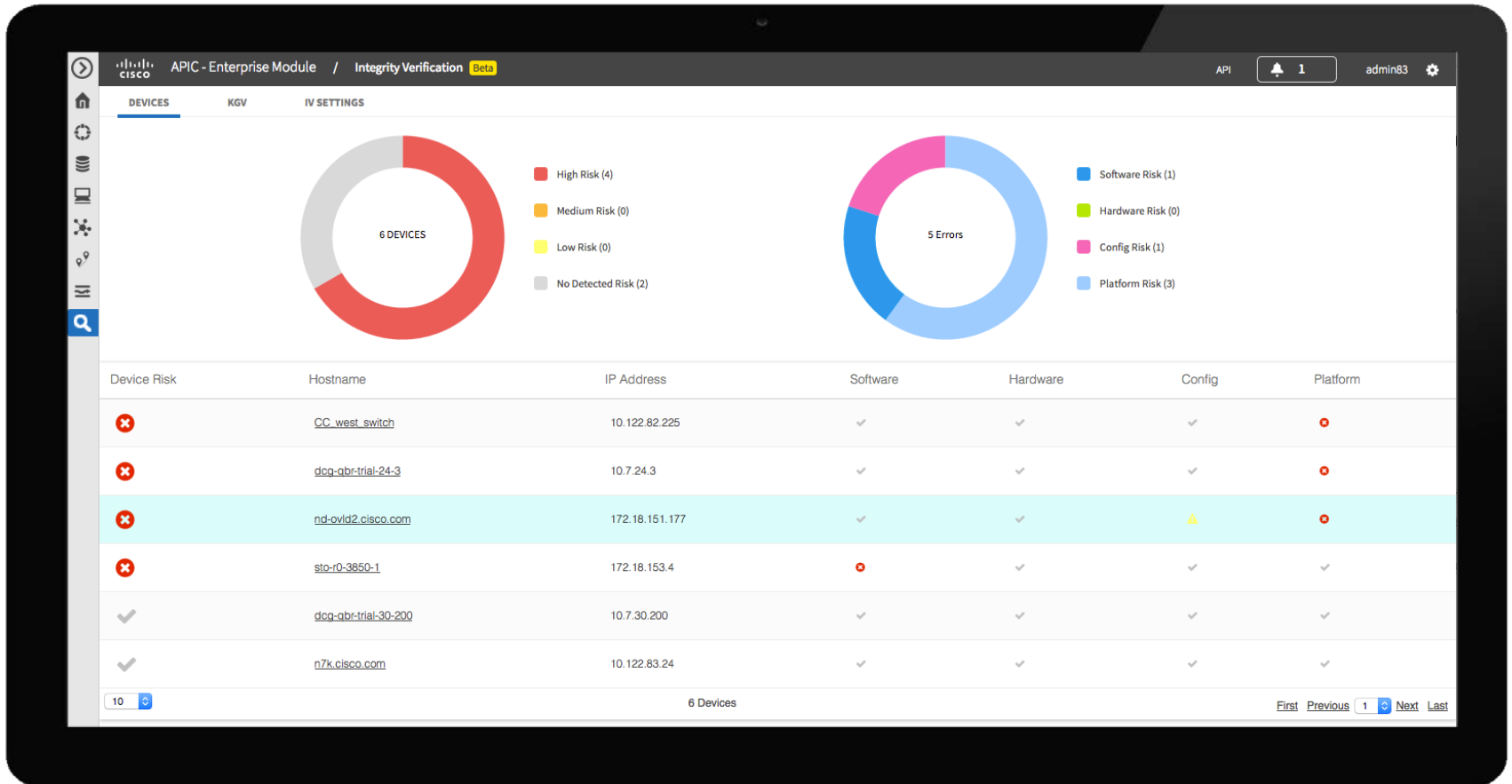
More than just at Boot time

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.



~ Demo

(Screen-shots of Demo due to time constraints)



~Demo

(Screen-shots of Demo due to time constraints)

The screenshot displays a web interface for a Cisco device named 'dcg-qbr-trial-25-246'. On the left, a 'Device Overview' sidebar lists details: Name, IP (10.7.25.246), Product Id (ISR4451-X/K9), Vendor (cisco), and Last Audit (2017-07-10 15:12:42). Below this, a 'Device Risk' section shows a red 'X' icon, indicating a failed assessment. A checklist shows 'Software', 'Hardware', and 'Config' as passed (green checkmarks), while 'Platform' is failed (red 'X').

The main content area has tabs for 'Software', 'Hardware', 'Configuration', and 'Platform'. Under the 'Platform' tab, a table shows the following status:

Platform Integrity Risk Level	High
Platform Integrity Fail Reason	unknown boot0 Measurement
Secure Identity Status	Verified
Boot Integrity Status	Failed

Below the table, a section titled 'Details of FAILED Boot Integrity Assessment' provides further information:

- Fail date:** June 28, 2017 4:53:38 PM UTC
- Failure Reason:** unknown boot0 Measurement
- Boot Integrity Signature Status:** Verified
- Boot Integrity Signature Version:** 1
- Boot Integrity Signature:** 99941DBE008E0FA64A206A9E961CEBF057D962E23F80AEA5F73F8E4242AEC7AD7B7B8ADA044C1037D6F9D9F25AE6D38698A4D1ABDBA010E9DD2EFEFF888C3D29C1C0493678FD2AD879B16FB86F53C96AEF5F129EB84ABB45D39A5482E1B387C4A01FB0F244FA50D792AB66D69E91237ACE5C38C02862F1AD6E03E75AB21F5211709CCB2E39B4C3714F3ED41FE17F37434D3F5EE72E3D1DC2E5D29EA987C50560CC16F7BF929A9FCB80435ACFB80D82A53BA28703836E0C26D481572814113852CFAD5EBFCC5323906ECBC1F5A7273492146B97E1B9D9A7D75E09232B3DCD908133AE33233B2CD0465ECECD61AD85FAF2BAF56D6E180CBF9EF96223F61FC78FA
- Boot Integrity Signature Nonce:** 15924802333735893093
- Boot 0 Status:** Failed
- Boot 0 Version:** F01001R06.03c1d3d202013-01-18

More info

<https://www.cisco.com/c/dam/en/us/td/docs/cloud-systems-management/application-policy-infrastructure-controller-enterprise-module/1-5-x/integrity-verification/user-guide/Cisco-Integrity-Verification-Application-APIC-EM-User-Guide-1-5-0-x.pdf>

Thank you!