Trusted Path Routing

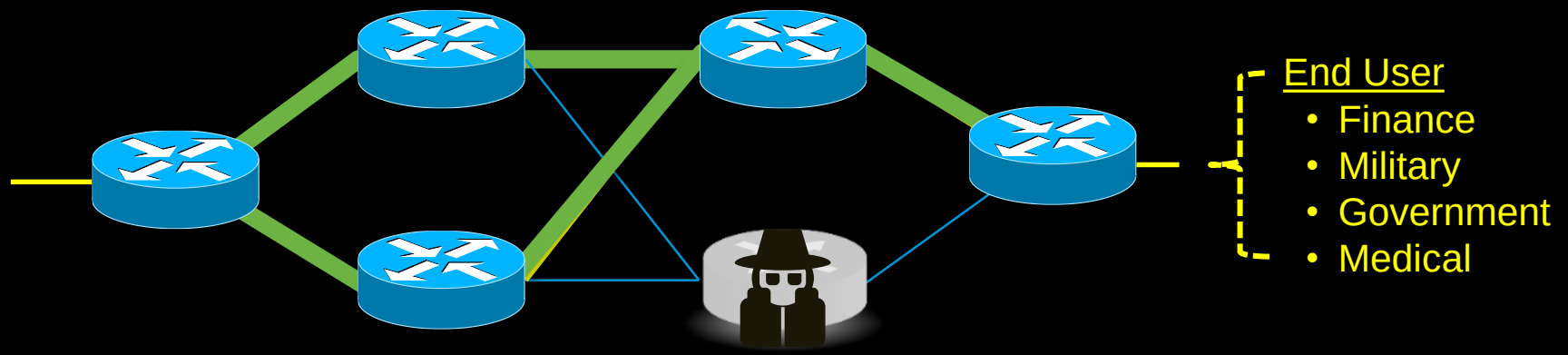
draft-voit-rats-trusted-path-routing-01

RATS Interim
31 March 2020

Eric Voit
evoit@cisco.com
Cisco Systems, Inc.

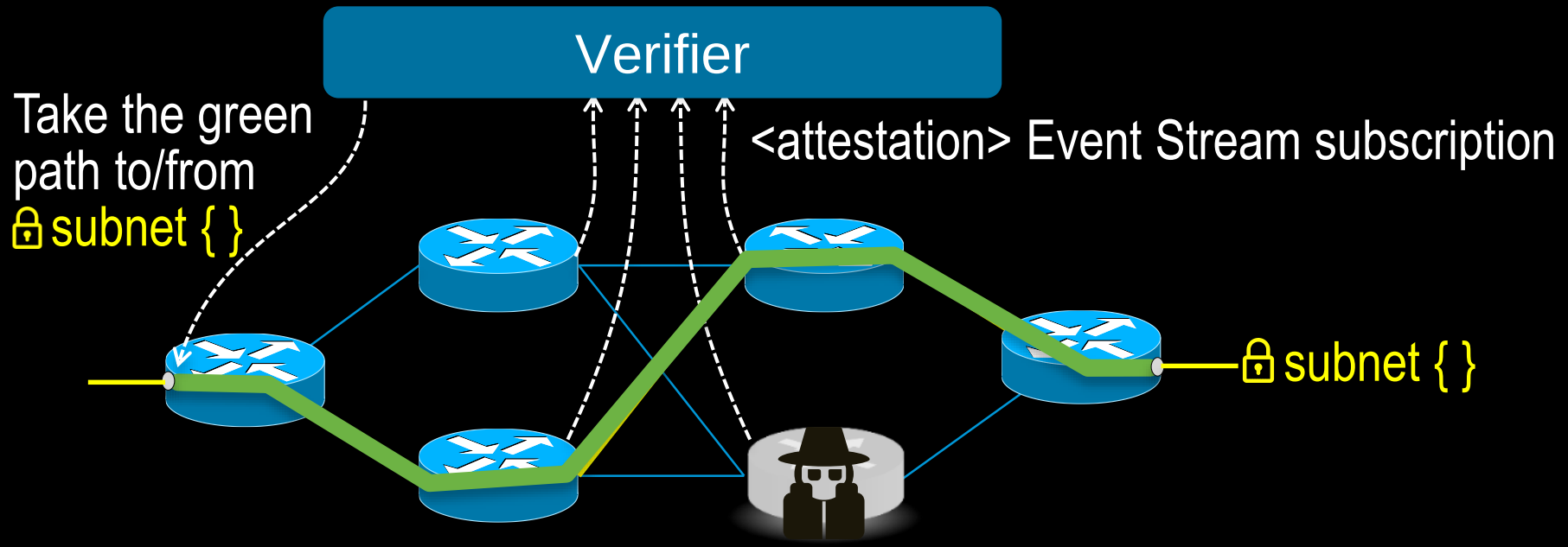
Trusted Path Routing

Sensitive flows bypass insecure / potentially compromised network devices

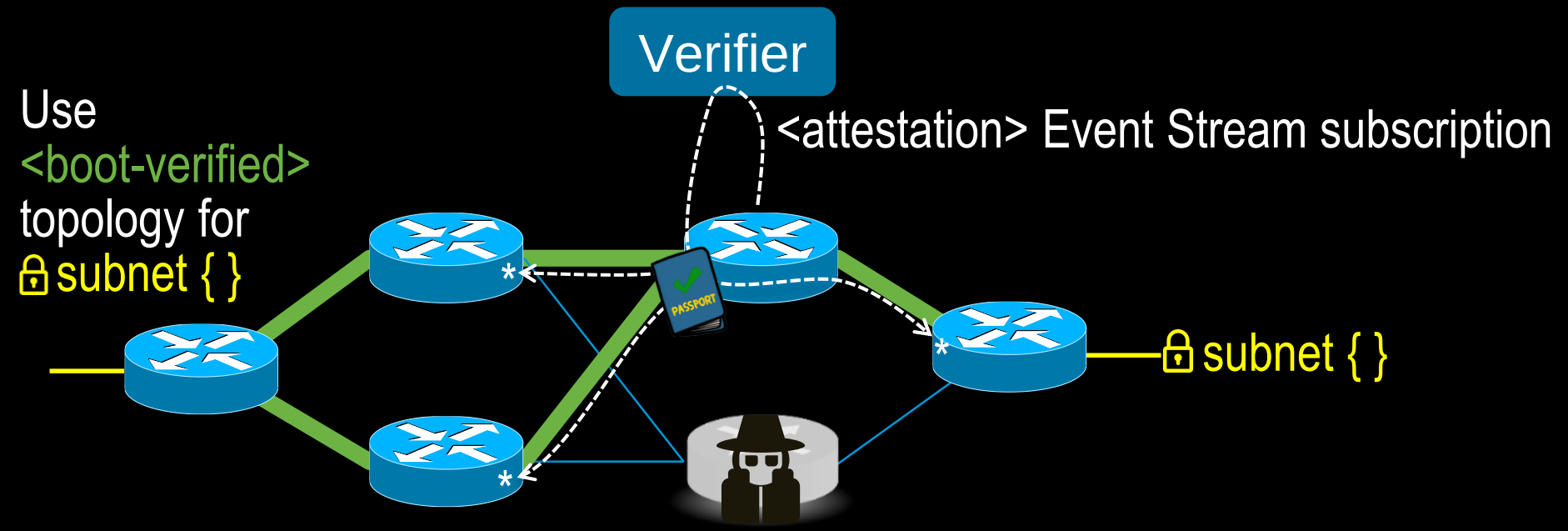


- Boot integrity not verified
- Actively exhibits Indicators of Compromise
- Software isn’t patched
- Doesn’t have hardware cryptoprocessor
- Currently unattested

Trusted Path Routing - Centralized



Trusted Path Routing - Distributed



* 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>

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

  - <tpm-extend>

  } 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

Router/Switch Trustworthiness Level

- 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

Function	Allocated PCR # Code	Allocated PCR # Configuration
BIOS Static Root of Trust, plus embedded Option ROMs and drivers	0	1
Pluggable Option ROMs to initialize and configure add-in devices	2	3
Boot Manager code and configuration (UEFI uses a separate module to implement policies for selecting among a variety of potential boot devices). This PCR records boot attempts, and identifies what resources were used to boot the OS.	4	5
Vendor Specific Measurements	6	6
Secure Boot Policy. This PCR records keys and configuration used to validate the OS loader		7
OS Loader (e.g GRUB2 for Linux)	8	9
Reserved for OS (e.g. Linux IMA)	10	10

Figure 2: Attested Objects
draft-fedorkow-rats-network-device-attestation

Composite Evidence

- Attester distribution of provably fresh appraisals