Building Blocks Towards a Trustworthy NFV Infrastructure

IRTF NFVRG

Adrian L. Shaw <adrian.shaw@hp.com>

Hewlett-Packard Laboratories / July 22nd, 2015

Why security and trust?

- Big requirement for critical infrastructures
- Security is not just about ACLs and crypto
- Workflows and service lifecycles
- Need for continual compliance monitoring
- Quick remediation

- Assurance requires strong visibility and infrastructure transparency

Where were we before?

Cloud

- General purpose
- Difficult to generally automate
- Compute and storage centric
- Administrators
- Multiple owners and tenants

- Generally broad and difficult

NFV

- Very specific purpose
- Controlled software
- Focused orchestration
- I/O centric
- Operator + some customers

- Opportunity for focused security

Trusted Computing and Remote Attestation

- Trusted computing: checking if platform executes expected SW
- Enforced through a component isolated from the software
- Measurement log signed by secure identity and verified remotely
- Remote verifier must have measurements of all expected software and configurations
- Different roots of trust: Measurement, storage, recovery, etc
- General requirement for a root of trust:
  - Secure storage
  - Protected memory
  - Shielded execution
  - Cryptographic engine

Hardware-based Roots of Trust

- Minimum piece to be trusted in order to achieve security property
- Why hardware?
  - Identity in hardware helps prevent ID forgery and SW-based attacks
  - Small functionality and immutability give high assurance
  - A small chip is often more reliable than someone else’s Python script
- Bind identity to platform
- Standards
  - Trusted Platform Module (TPM) and Trusted Computing Group (TCG)
    - Other HW roots of trust: Intel TXT, AMD SVM, ARM TrustZone + PUFs
  - Provisioning & authentication: IEEE 802.1AR Secure Device Identity

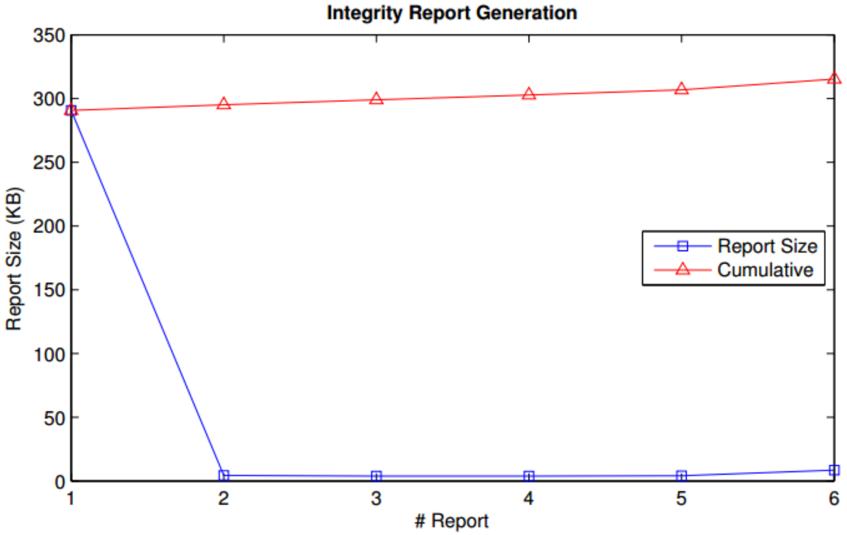
Building blocks

- Platform boot time integrity
  - Verified boot – only allow signed software components
  - Trusted boot – reports the version of each software in boot chain
- Load time inspection
  - Linux IMA – measure each program and report to TPM before executing
    - Measures high integrity files e.g. readable by root user
  - Linux EVM – measures integrity of file-system permissions
- Network integrity
  - Bind platform certificates to root of trust
  - Configuration measurement (e.g. SDN VLANs, MACSEC context)

IMA: Host-level attestation

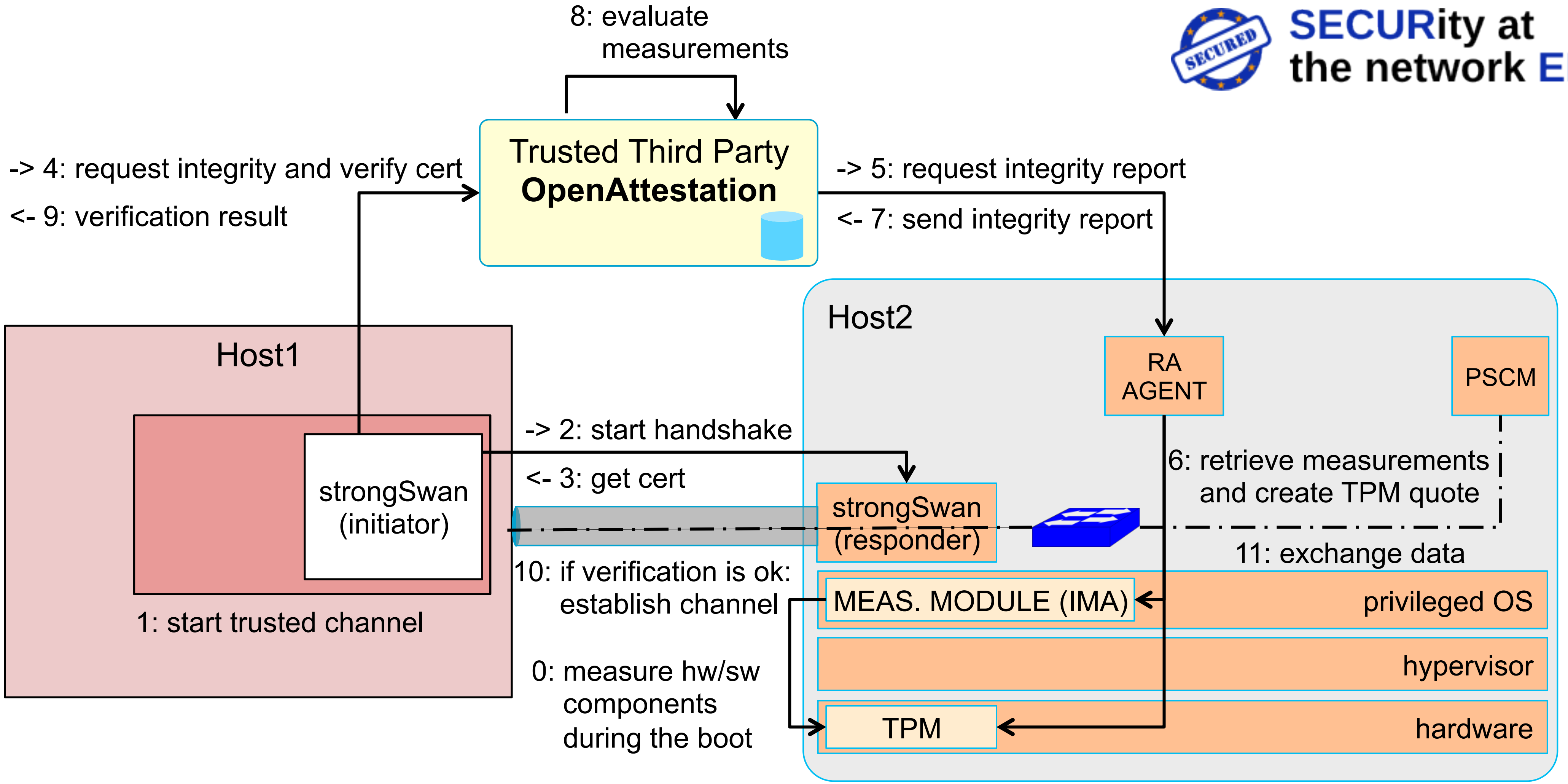
- Measures and reports to the TPM every time the kernel loads:
  - Executable programs
  - Shared libraries
  - Files readable by high integrity (e.g. Root user)
- Flexible appraisal strategy
  - SHA-1/SHA-256 measurements
  - Signature-based verification
- Overheads
  - Speed of verification
  - Integrity report size: “Virtualized security at the network edge” – Montero et al

SECURity at the network EDge

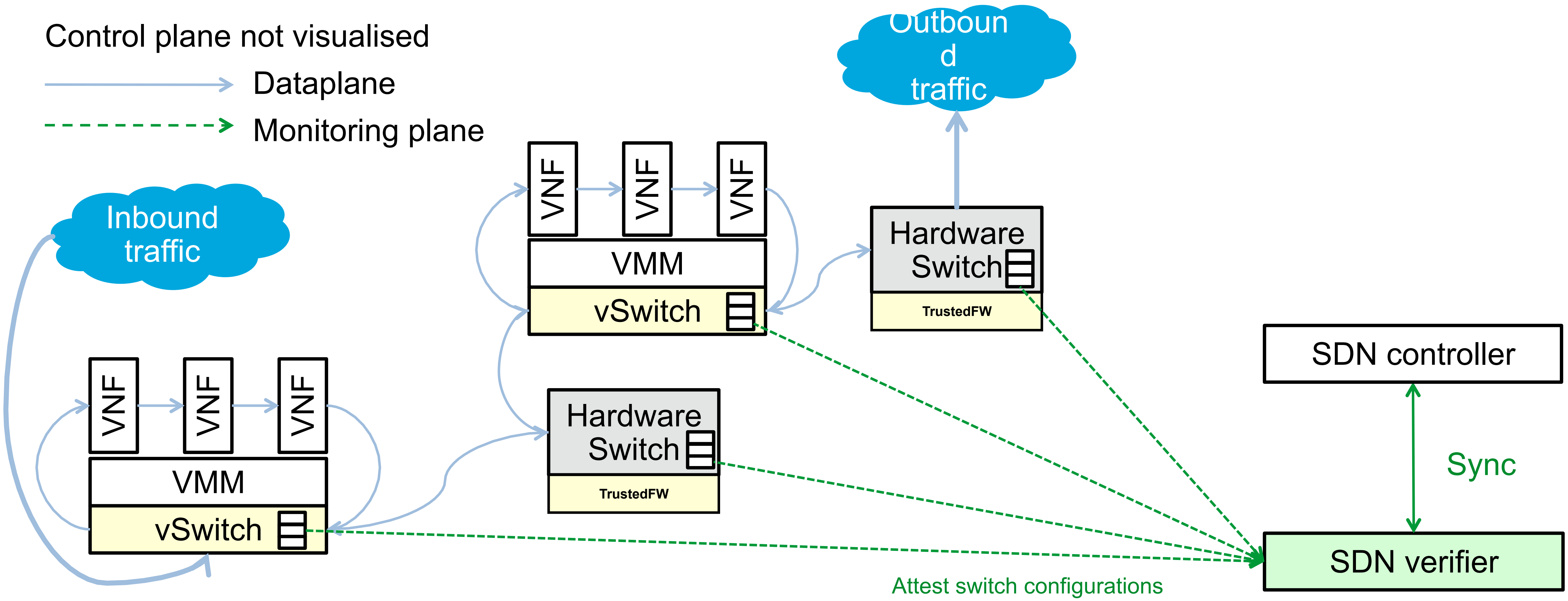


Trusted channel establishment

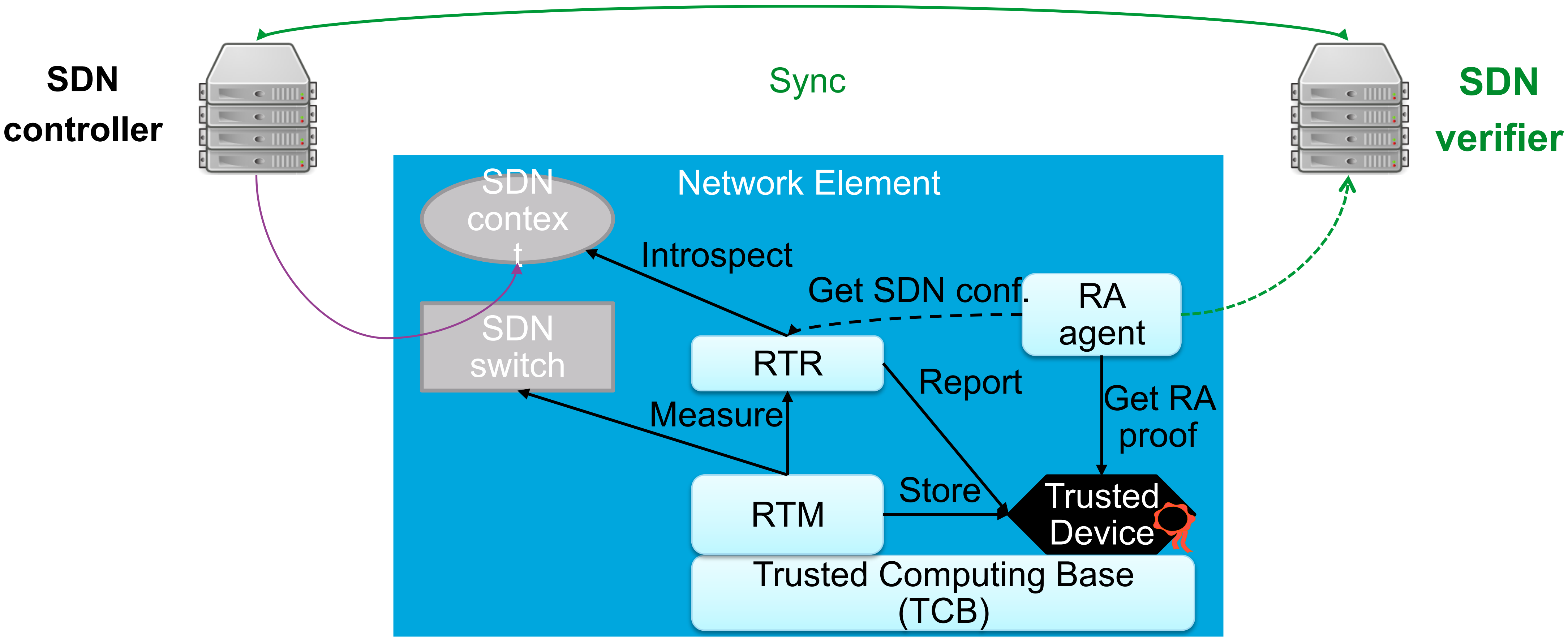
SECURity at the network EDge



Compliance monitoring of SDN

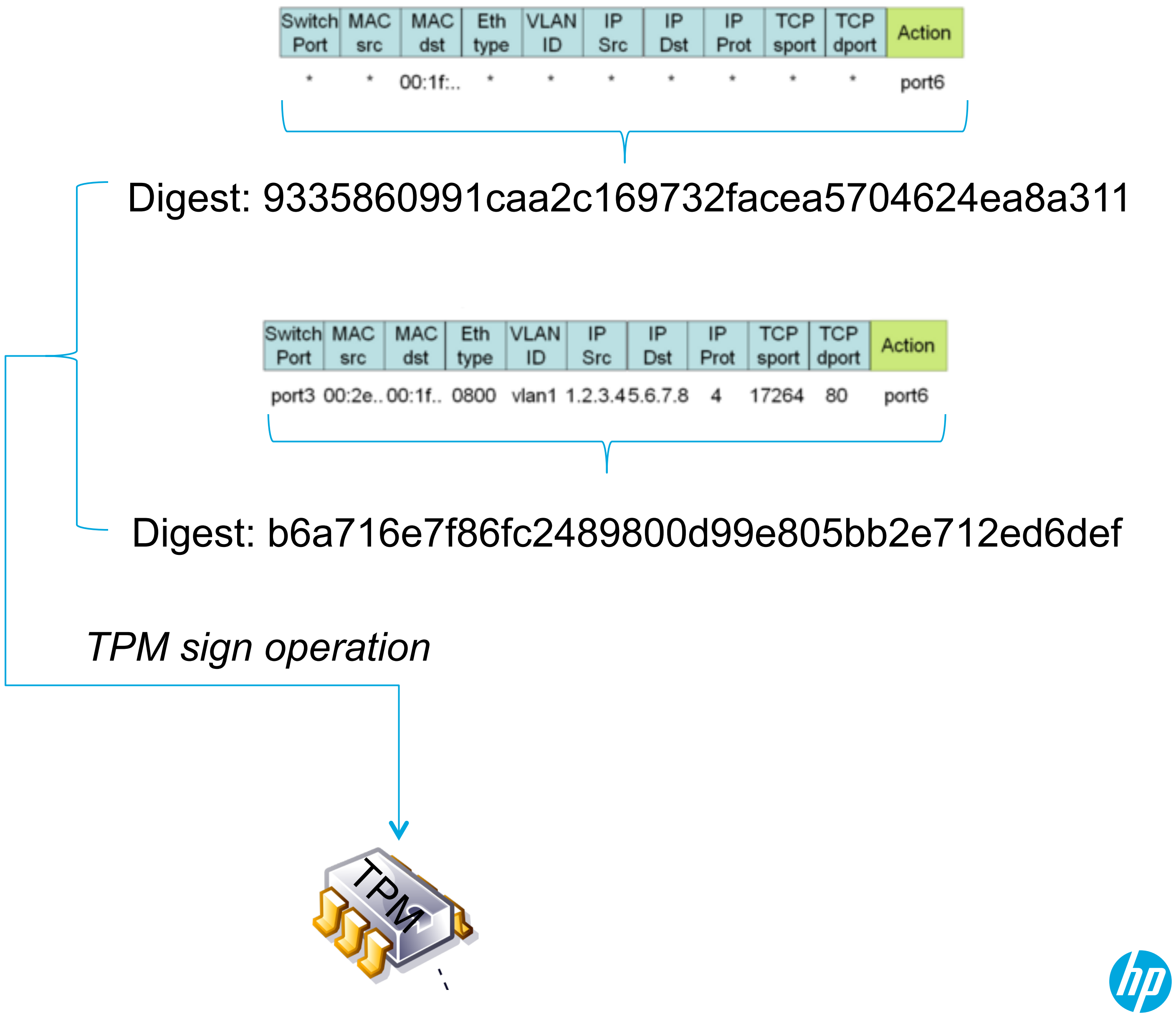


Remote Attestation of a Network Element



SDN attestation report

- Attestation requests context
- TCB includes reporting agent
- Report covers
  - Header matches for L1, L2, L3, L4
  - Action
  - Priority
  - Surrounding DP configuration
- Report signed by the TPM
- Prototyped on HW
  - SNMP-based, thinking of appropriate monitoring protocol



Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
*	*	00:1f:..	*	*	*	*	*	*	*	port6

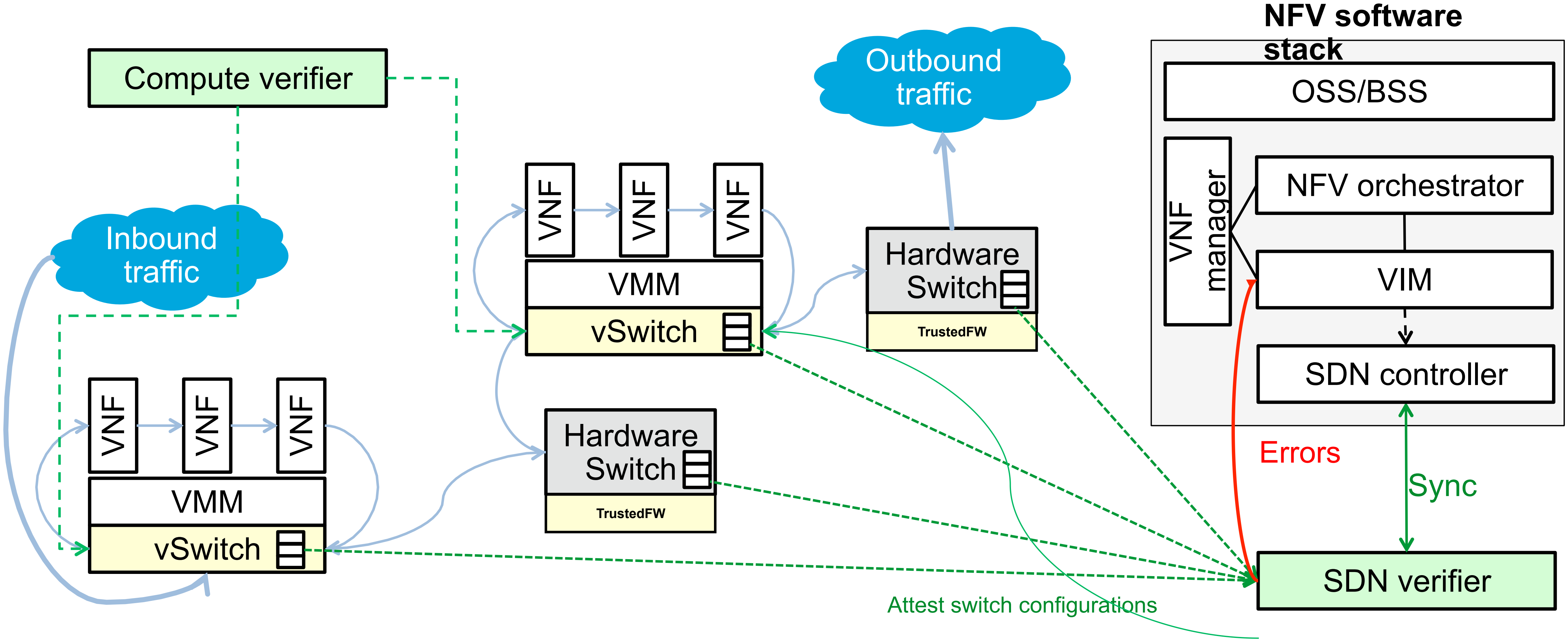
Digest: 9335860991caa2c169732facea5704624ea8a311

Switch Port	MAC src	MAC dst	Eth type	VLAN ID	IP Src	IP Dst	IP Prot	TCP sport	TCP dport	Action
port3	00:2e..	00:1f..	0800	vlan1	1.2.3.4	5.6.7.8	4	17264	80	port6

Digest: b6a716e7f86fc2489800d99e805bb2e712ed6def

TPM sign operation

Compliance monitoring for NFV



Takeaways

- Great opportunity for TC to work for NFV
  - Operator more likely to know expected software images and configurations
  - Different building blocks can be applied for varying levels of integrity
- Ethemeral configurations (e.g. SDN) need monitoring
  - Data plane security – alert on unauthorised change
- Other needs:
  - Control plane security – separation of concerns between SDN applications
- Stateless infrastructure deployment
  - Better for attestation of compute nodes without too many ringing alarm bells

Thank you

adrian.shaw@hp.com