

Bootstrapping "softwarised" infrastructure trust: from SDN towards NFV

Ludovic Jacquin

Hewlett-Packard Laboratories

< ludovic.jacquin@hp.com >

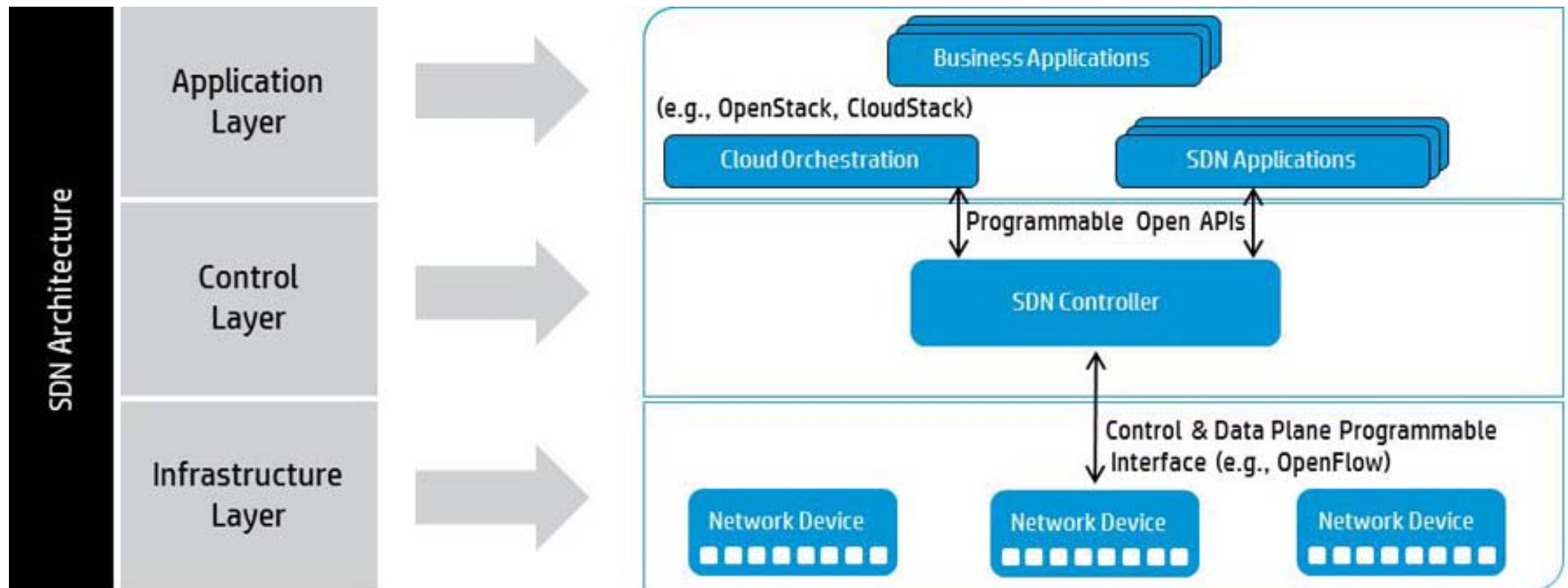
Cybersecurity & Privacy Innovation Forum 2015

Brussels, 28/4/2015



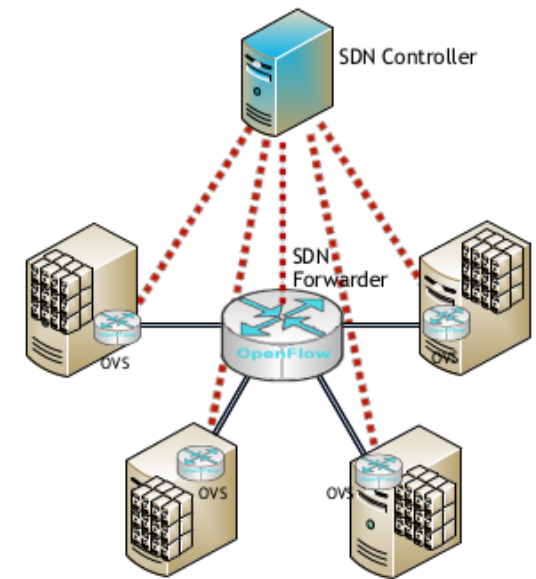
“Softwarisation” of the infrastructure

Empowering the application to change the network topology



Software-Defined Networking in a nutshell

- **split the control and data planes**
 - network elements expose new interfaces
- **centralised control plane in the form of an SDN controller**
 - decisions taken out of the boxes through protocol
 - but the controller has full visibility on the network topology



“Abusing software-defined networking”

BlackHat ‘14, G.Pickett, Hellfire Security

- **infrastructure information disclosure (topology, credentials)**
 - no encryption on northbound API (or turn-off by default)
 - no authentication on northbound API (or weak password)

- **modification of flows/topology via unauthorised access**
 - connect to the targeted network element and kick the genuine controller
 - change to malicious one
 - future suggests growing software attacks

- **deny of Service on the controller**
 - flooding

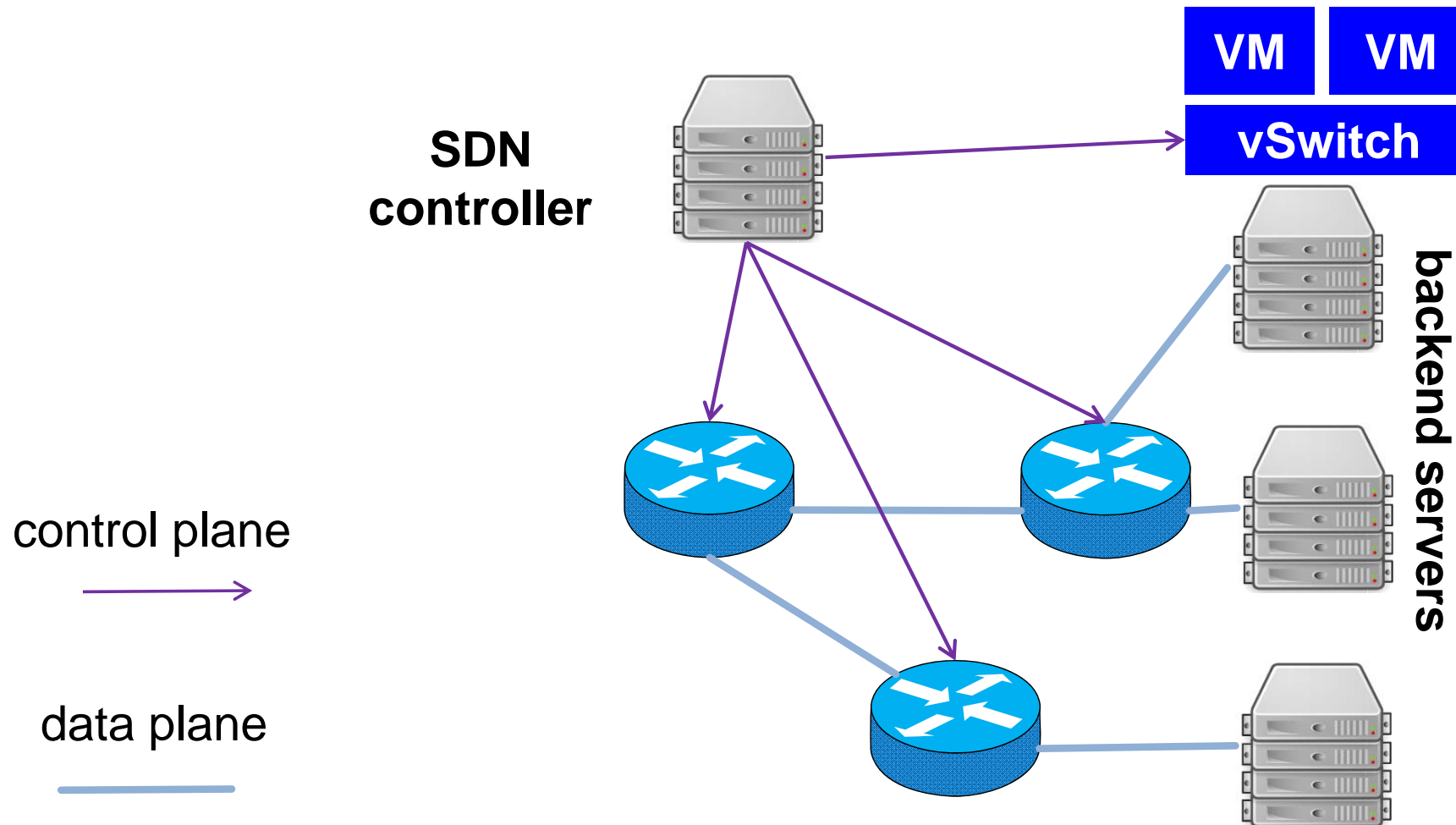
“Softwarised” infrastructure monitoring

Network monitoring needs automation too!

- **hard for administrators to assess the network topology**
 - used to manage switches individually
 - now must manage the topology through the SDN controller
 - loses a lot of observability
- **network now changes dynamically**
 - how can we have more assurance that routing is performed correctly?
- **the SDN controller holds all the information**
 - at large scale, can not be humanly processed

SDN trustworthy monitoring architecture

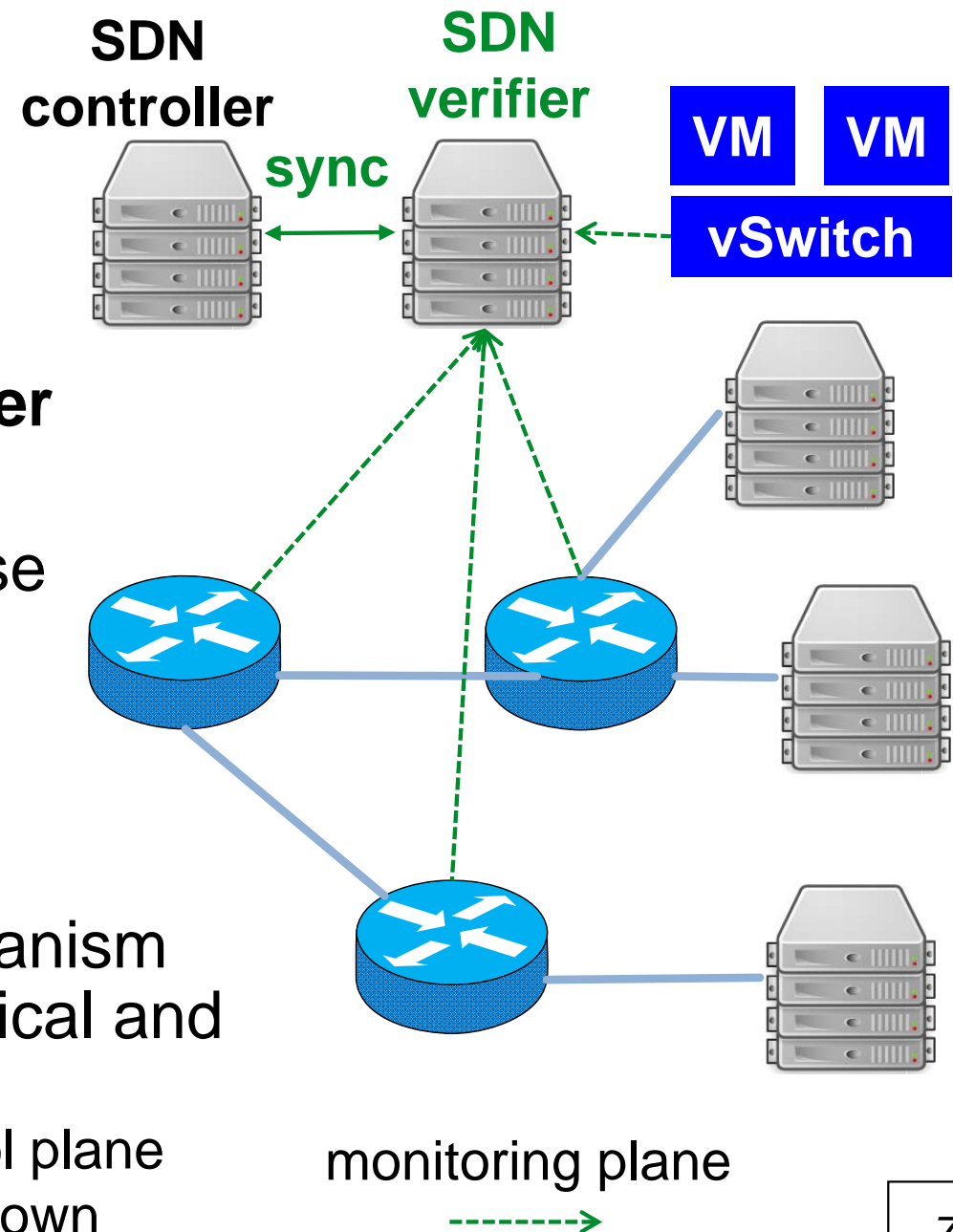
How do we regain trust in this new infrastructure paradigm?



The Vision: automated and trustworthy monitoring for SDN

Introducing the SDN verifier

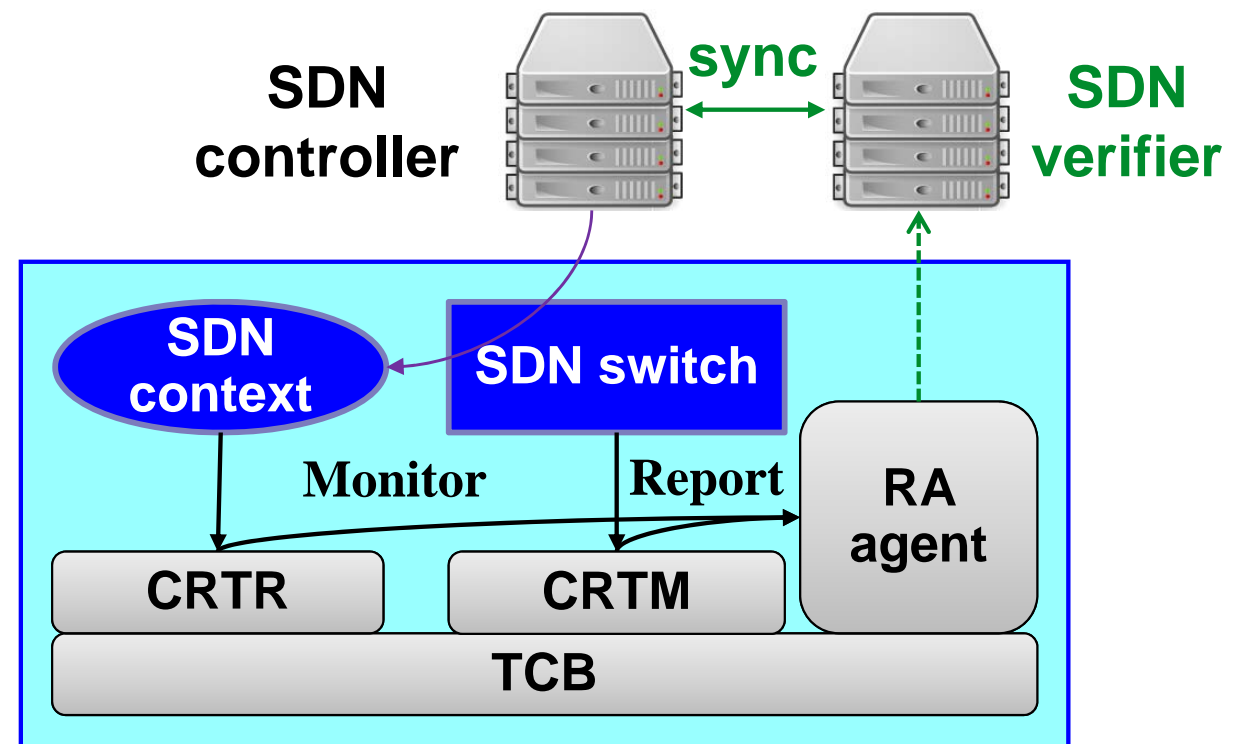
- assess that SDN configuration of switches match the controller expectation
 - out-of-band challenge/response
 - meant for continual attestation
- challenge:
 - build a trusted reporting mechanism for each network device (physical and virtual)



Core Root of Trust for Reporting (CRTR)

Monitoring the SDN rules in a network element

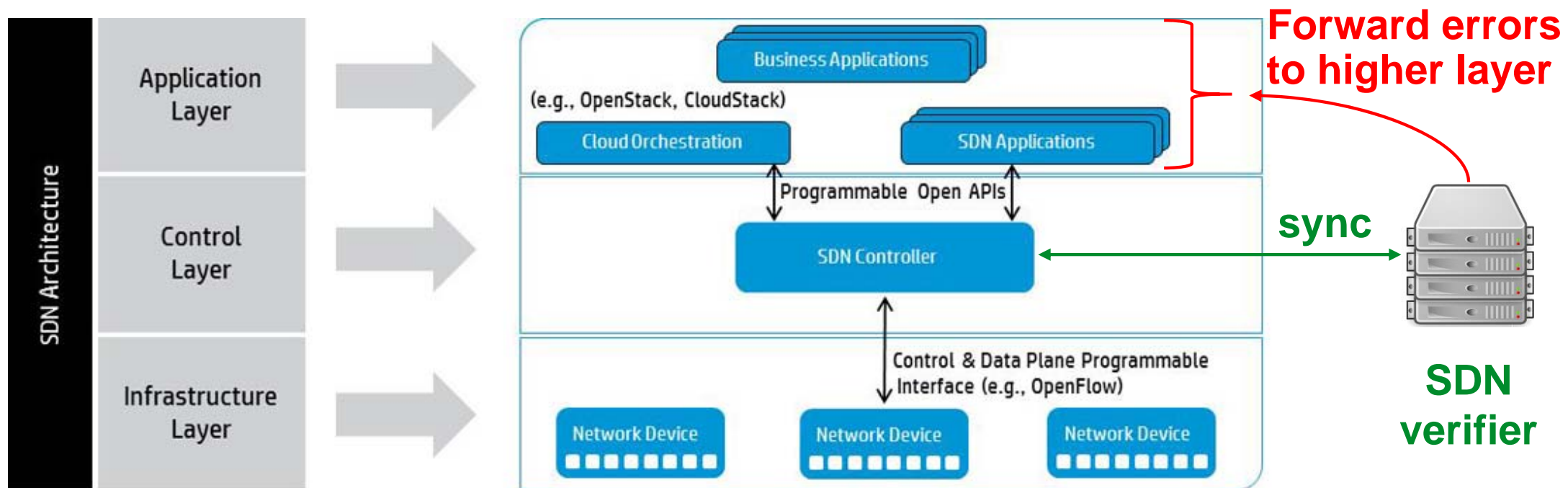
- **introspection of the SDN context:**
 - we need to monitor what is really enforced, not just the protocol
- **the SDN “switch” still needs to be attested**
- **remote attestation must be possible by the SDN verifier**
- **prototype:**
 - rely on TPM
 - software stack
 - SDN rules enforced



Next steps: closing the loop

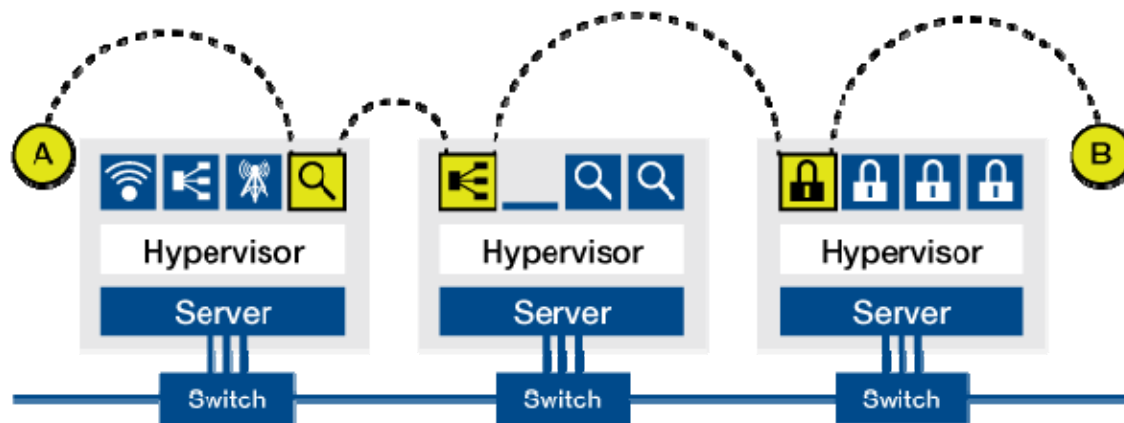
Acting on a misbehaving network elements

- **automated response**
 - pass the information to the application layer
 - application layer has the visibility to handle the error, e.g. quarantining a faulty switch

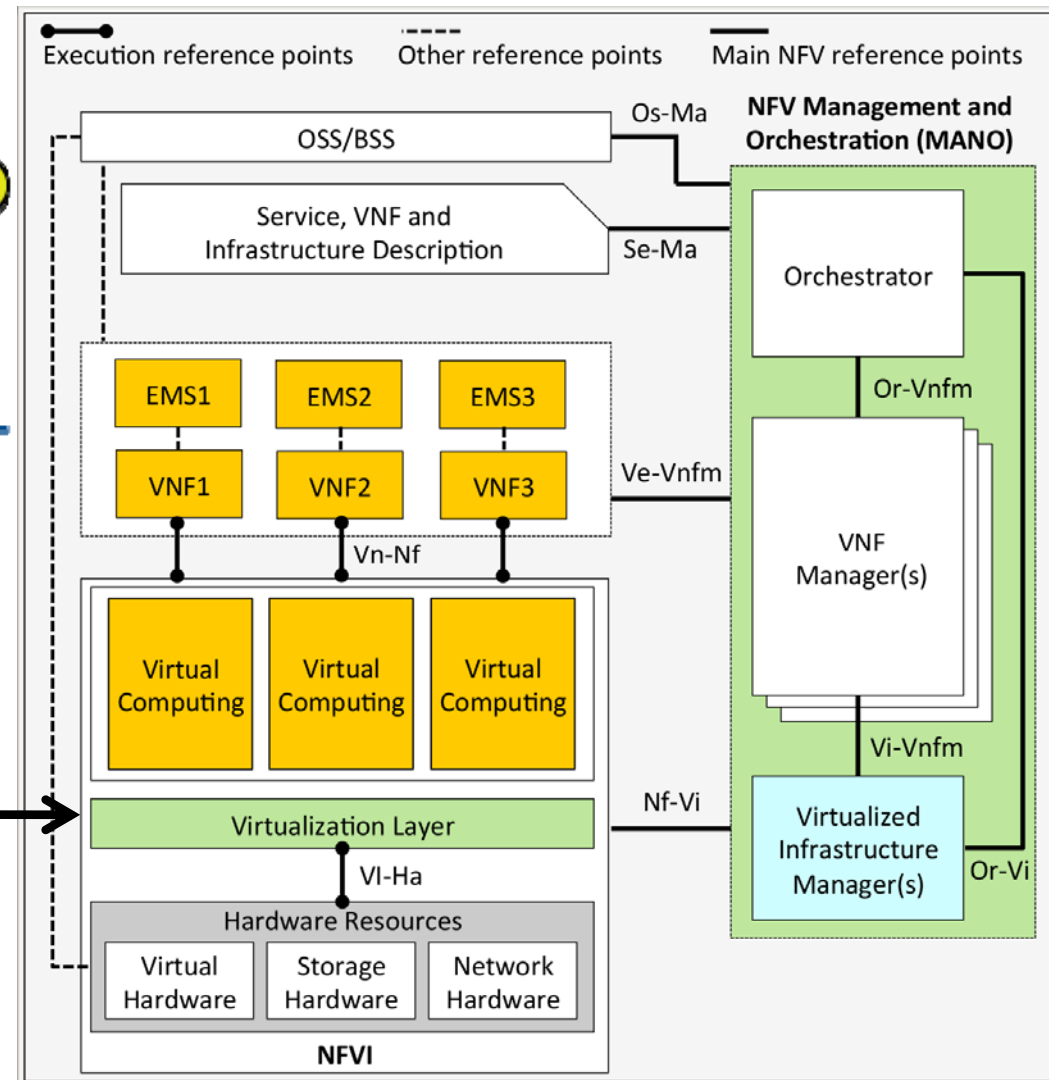


SDN as a building block of NFV

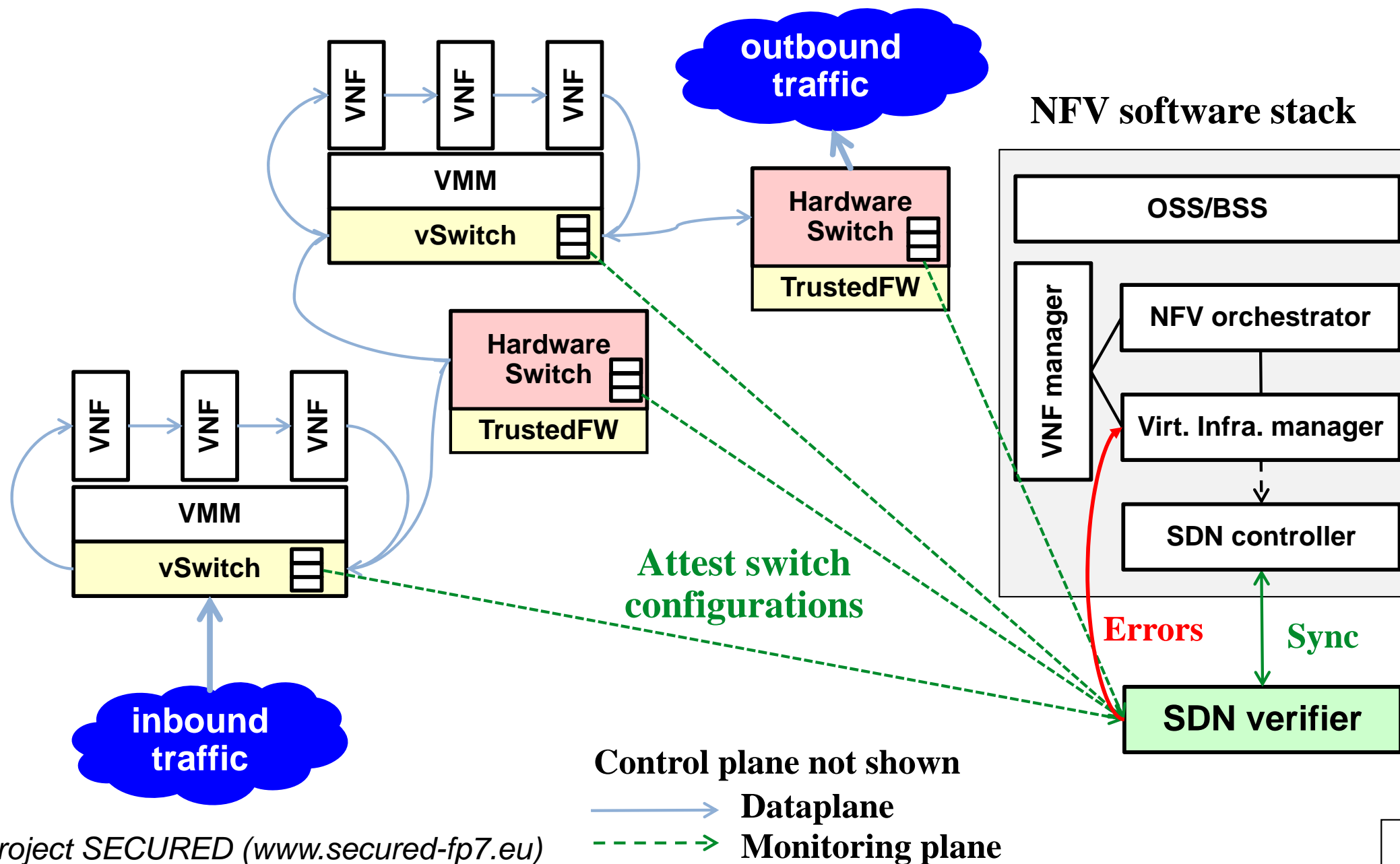
ETSI VNF chaining and NFV Architecture



Powered by SDN



SDN compliance monitoring for NFV



THANK YOU !



Project SECURED (www.secured-fp7.eu)



Disclaimer

EU disclaimer

SECURED (project no. 611458) is co-funded by the European Union (EU) via the European Commission (EC), under the Information and Communication Technologies (ICT) theme of the 7th Framework Programme for R&D (FP7).

This document does not represent the opinion of the EC and the EC is not responsible for any use that might be made of its content.

SECURED disclaimer

The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.