Bootstrapping Trust in SDN Infrastructure

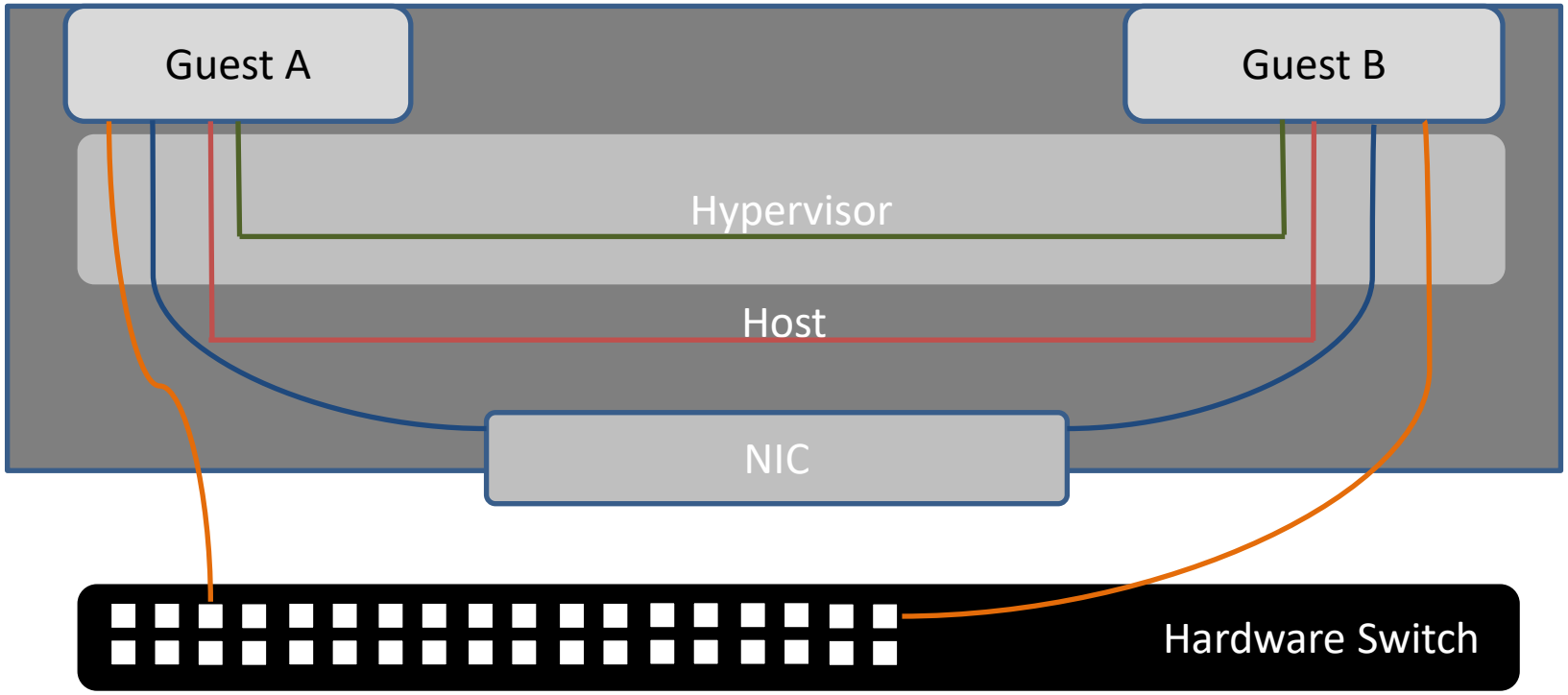
Nicolae Paladi

RISE SICS

June 16, 2017

This work was carried out under the 5G-ENSURE project (www.5gensure.eu), which is funded by the European Union's Horizon 2020 research and innovation programme under the grant agreement number 671562. Responsibility for the information and views set out in this document lies entirely with the authors.

Hardware vs virtualization



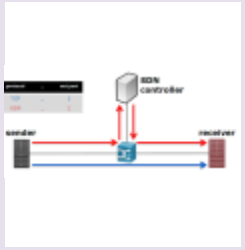
- Hairpin switching does not scale enough to keep up with increase in numbers of virtual endpoints.
- Software (aka virtual) switches have been widely adopted in virtualized deployments

Software allows new capabilities (for attacks!)

- Software implementations (most often) reside on commodity operating systems
  - Larger attack surface;
  - Collocation with other (potentially malicious) applications;
  - Component isolation depends on the configuration of the software stack
  - Abundant opportunities to make mistakes!

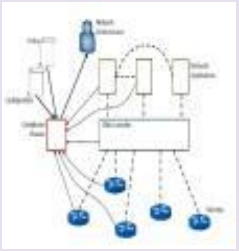
5G-ENSURE Security Enablers in Task 3.5

Fingerprinting SDN networks



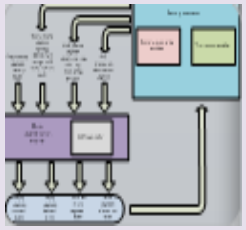
Preventing information leakage about switch configurations in SDN networks

Component interactions



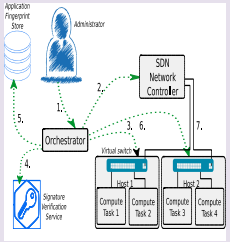
Checking policy compliance of interactions between network components

Micro-segmentation



Managing segments in a 5G network in which strict security policies can be enforced

Bootstrapping trust

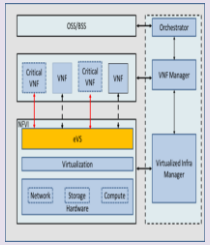


Verifying integrity of software network components prior to enrollment into infrastructure

Access control

Controlling access of network applications to network resources

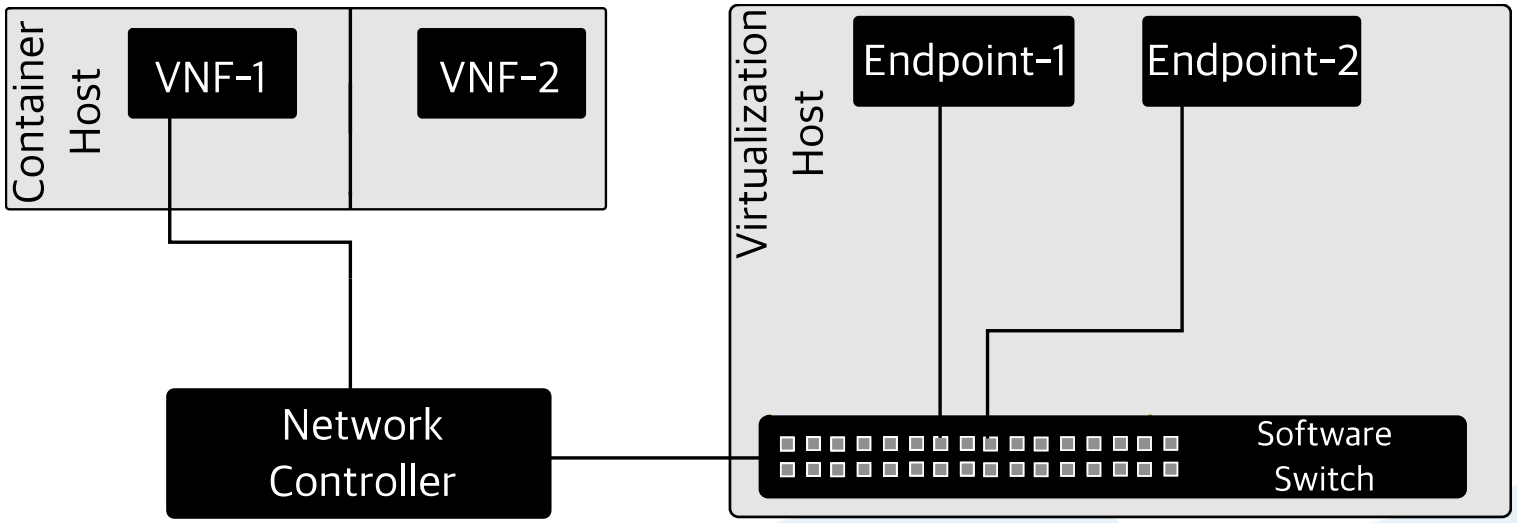
Flow control for critical VNF



Protecting critical VNFs at runtime from malicious threats through in-network detection and mitigation

Motivation

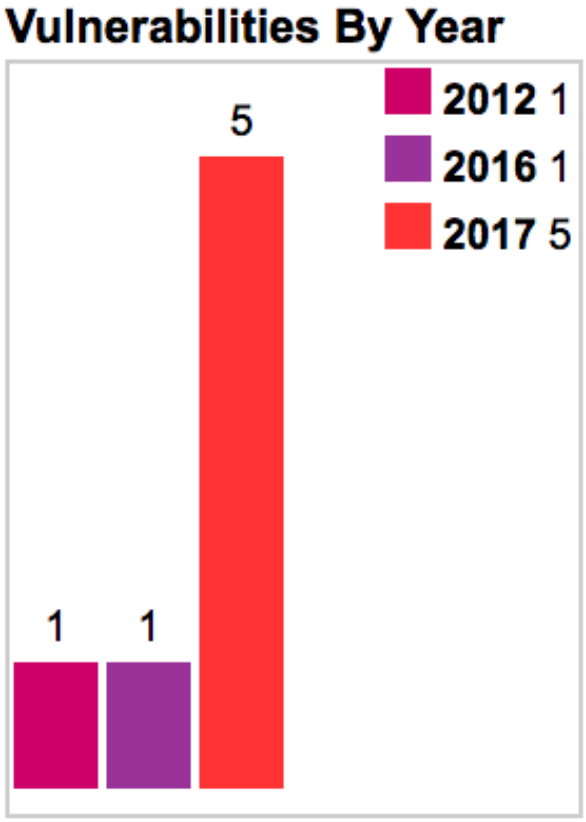
- Software implementations of network components rely on commodity platforms (for better or worse…)

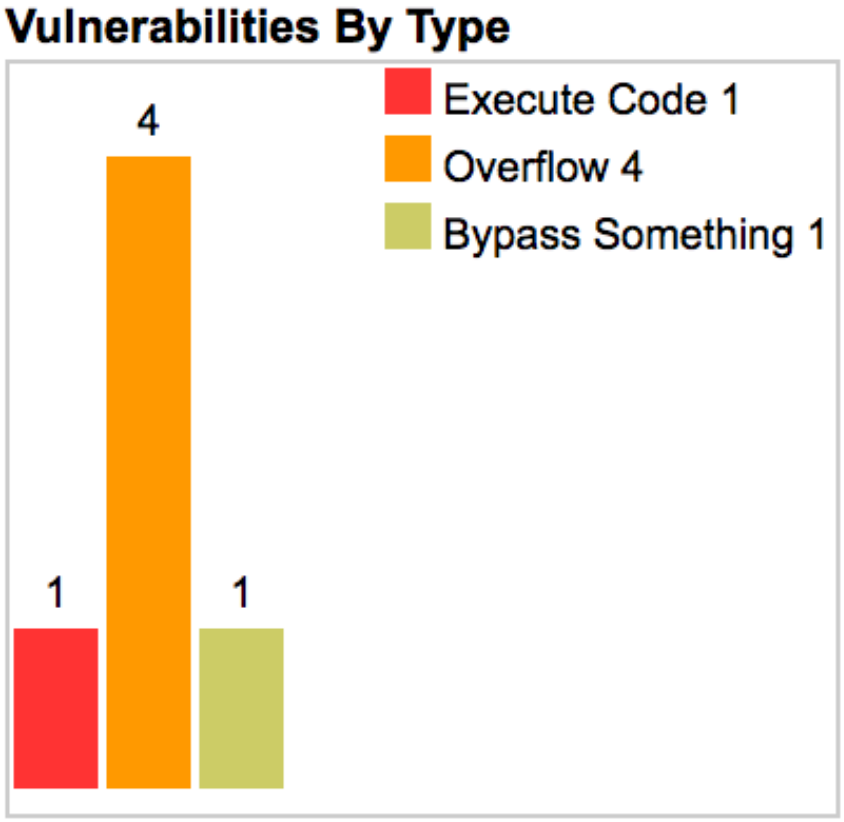


- Platforms must be diligently configured and regularly patched to avoid vulnerabilities.

Attack vectors

- Vulnerabilities in Open vSwitch





Attack vectors

- Docker vulnerabilities
- Vulnerabilities in Docker images

the security ledger

Friday, June 9, 2017

INTERNET OF THINGS ~ THREATS ~ THOUGHT LEADERSHIP ~ PODCASTS VIDEO WHITEPAPERS

Unpatched Vulnerabilities Common on Docker Hub Images

May 29, 2015 10:41 by Paul

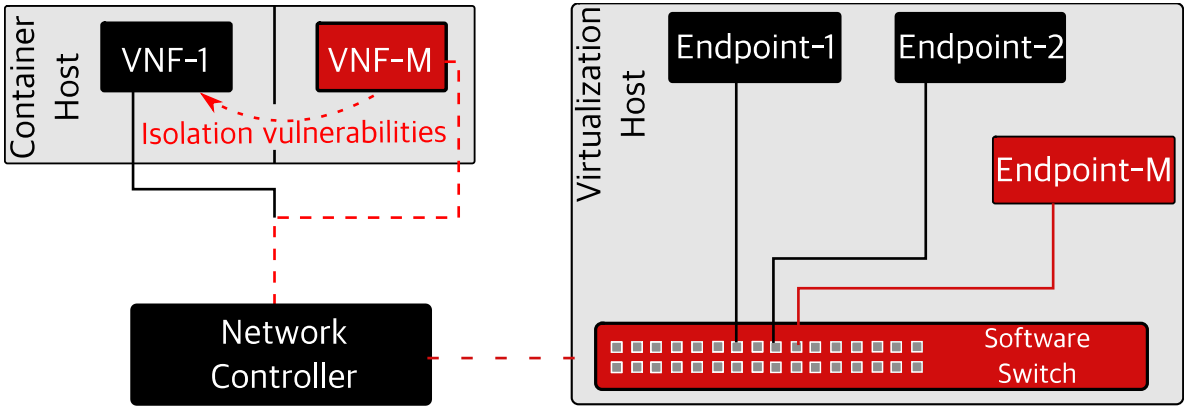
docker

A survey of Docker repositories found that critical vulnerabilities are common in both official and general repositories.

In-brief: A survey out from the firm Banyan finds that official and general repositories on Docker Hub are rife with serious and exploitable software vulnerabilities, including Heartbleed, Shellshock and Poodle.

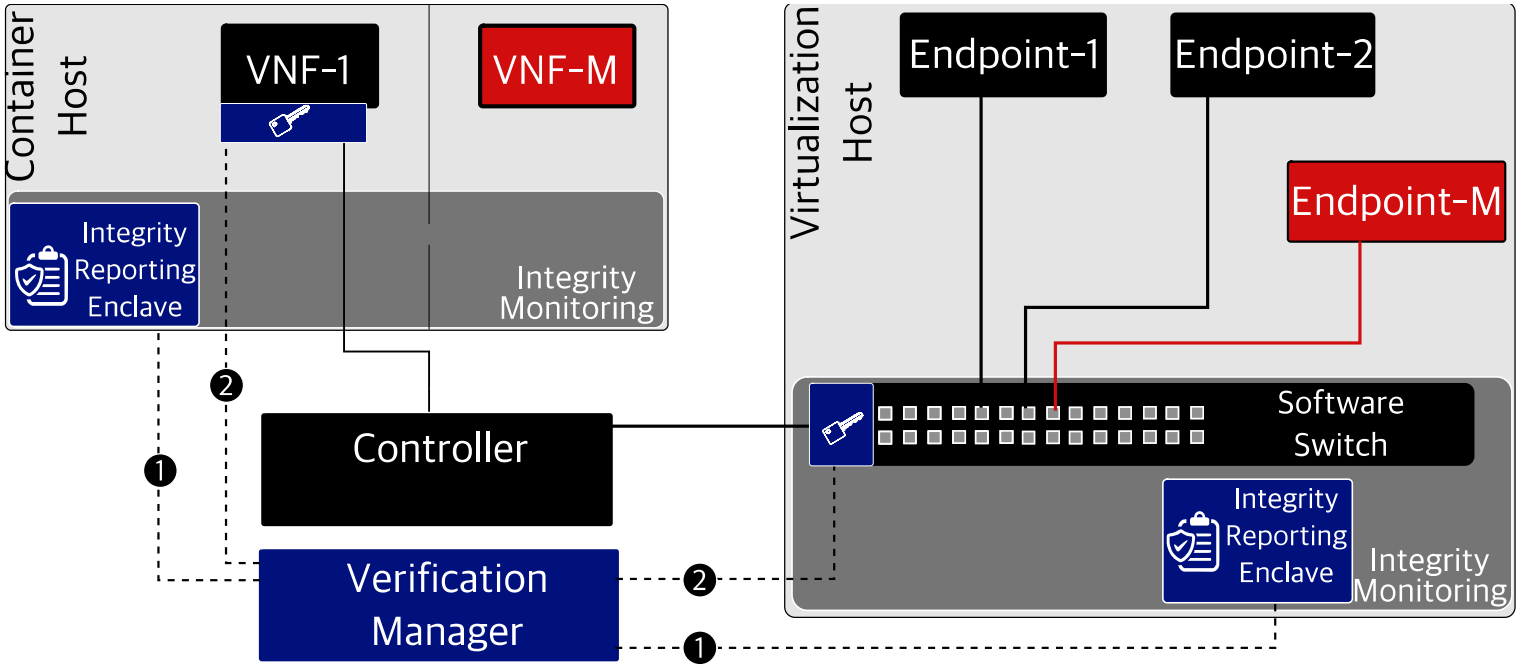
Threat scenario

- Underlying software stack can contain multiple exploitable vulnerabilities



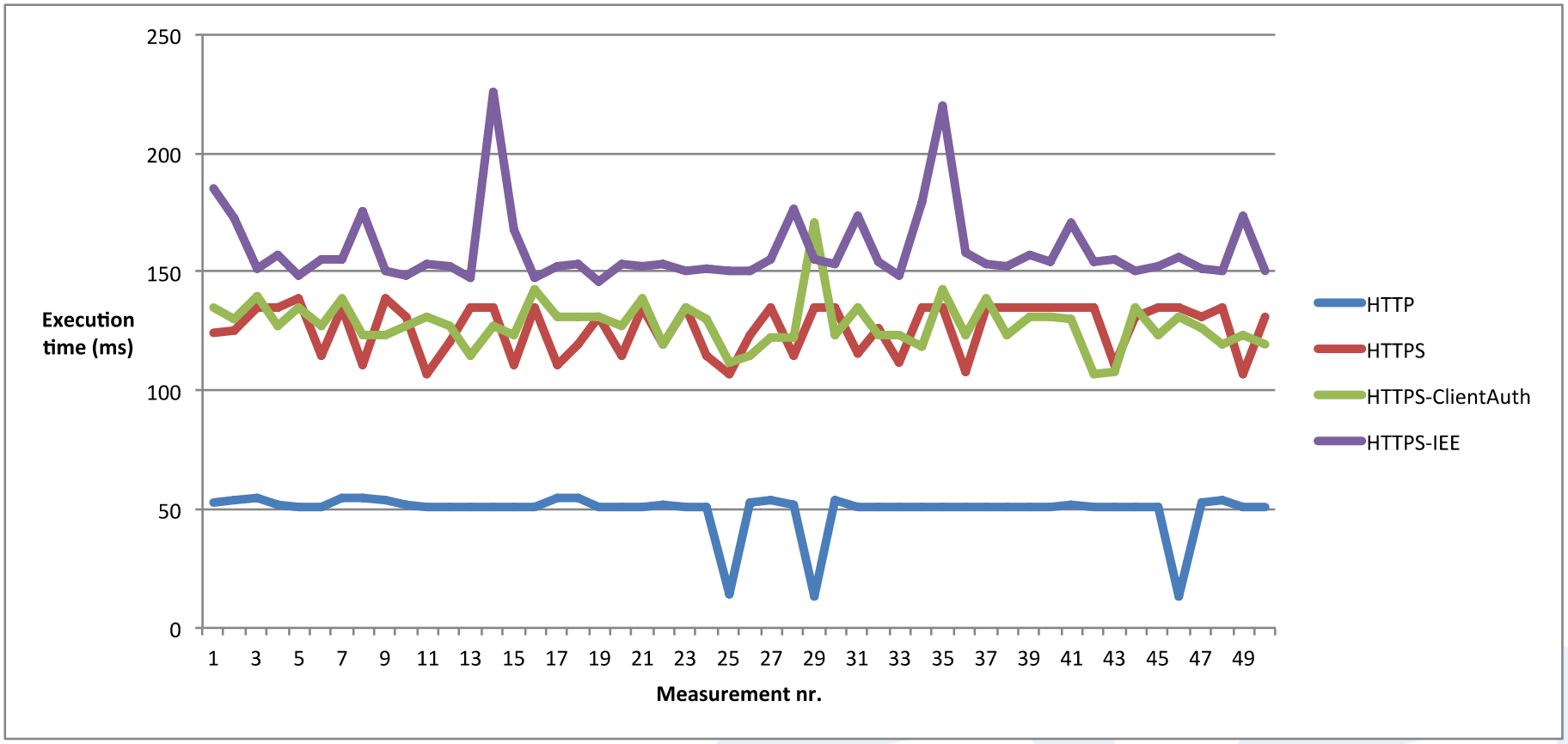
- Isolation breaches may allow to extract/modified security-sensitive data (e.g. authentication credentials, configuration, flow tables etc.)

Countermeasure



- Isolated execution enclaves implemented with Intel SGX
- Keys never leave enclaves
- TLS context never leaves enclaves
- Encryption/decryption in enclaves
- Implementation with Docker (for VNFs) and Open vSwitch

Results



- On par with both plain HTTPS and HTTPS with client authentication
- Minor performance penalty due to context switch

Video Demo

Dedicated File

References

- www.5gensure.eu
- Paladi, Nicolae, Christian Gehrmann. "TruSDN: Bootstrapping Trust in Cloud Network Infrastructure", *SecureComm'16* (in press).
- Rizzo, Luigi, and Giuseppe Lettieri. "Vale, a switched ethernet for virtual machines." *Proceedings of the 8th international conference on Emerging networking experiments and technologies*. ACM, 2012.
- B. Pfaff, J. Pettit, T. Koponen, E. Jackson, A. Zhou, J. Rajahalme, J. Gross, A. Wang, J. Stringer, P. Shelar, K. Amidon, and M. Casado, "The Design and Implementation of Open vSwitch", NSDI '15.
- Thimmaraju, Kashyap, et al. "Reigns to the Cloud: Compromising Cloud Systems via the Data Plane." *arXiv preprint arXiv:1610.08717* (2016).
- M.-W. Shih, M. Kumar, T. Kim, and A. Gavrilovska, "S-NFV: Securing NFV States by Using SGX", SDN-NFV Security '16.
- S. Kim, J. Han, J. Ha, T. Kim, and D. Han, "Enhancing security and privacy of tor's ecosystem by using trusted execution environments", NSDI '17
- "Intel 82599 10 GbE contoller datasheet," http:// download.intel.com/design/network/datashts/82599_ datasheet.pdf, April 2010