Welcome to the World of Standards

ETSI

World Class Standards

NFV SEC TUTORIAL

Igor Faynberg, CableLabs

Chairman, NFV Security WG

SDN OpenFlow WORLD CONGRESS

The NFV SEC Working Group Mission

The NFV SEC Working Group comprises Computing, Networking and Cloud security experts representing **Network Operators, Equipment Vendors**, and **Law Enforcement Agencies** who advise the NFV ISG on all matters of the relevant security technologies while developing a wide range of industry specifications that:

- **Identify both** the NFV-specific security problems as well as the technological advantages of the NFV environment that can be harnessed to **improve** the security of the network operators' services;
- **Provide specific guidance** on various aspects of the NFV security in a systematic, holistic manner—building trust from secure hardware modules to software and covering identity management, authentication, authorization, and secure attestation, as well as the means of global monitoring of the whole NFV environment and decisive operational security actions in response to security breaches;
- **Address in minute detail** the security of current Open Source-based platforms (such as *OpenStack*) ;
- **Contribute to solving the problem** of implementing Lawful Interception in the NFV environment; and…
- **Work in close collaboration** with other ETSI NFV WGs, PoCs, as well as external organizations (in particular, *ETSI TC Cyber, ETSI TC LI, Trusted Computing Group*, *3GP*P SA 3,5G *SELFNET* Consortium, and contributing members of *OpenStack)*

The ETSI NFV Security Working Group (https://portal.etsi.org/tb.aspx?tbid=799&SubTB=799)

- Was created as an ***expert group*** in 2012 (Phase 1) with the objective to establish the NFV *security problem statement* and advise all working groups rather than progress specific work items - but this has changed!
- **Started by Bob Briscoe (BT)**
  - Just **three** experts at the onset of the NFV;
  - Only e-mail exchanges
- **In Phase 2 has grown to…**
  - Full working group (Chairman: **Igor Faynberg**, **CableLabs**; Vice Chairman: **Mike Bursell, Intel**)
  - Steady **30+** active participants from **various** companies (**200** on the mailing list,) and government agencies
  - Regular weekly 2-hour meetings, and a steady stream of contributions
  - A reference point for joint work with ETSI TC Cyber, ETSI TC LI, Trusted Computing Group, 3GPP, and *5G Selfnet Consortium*

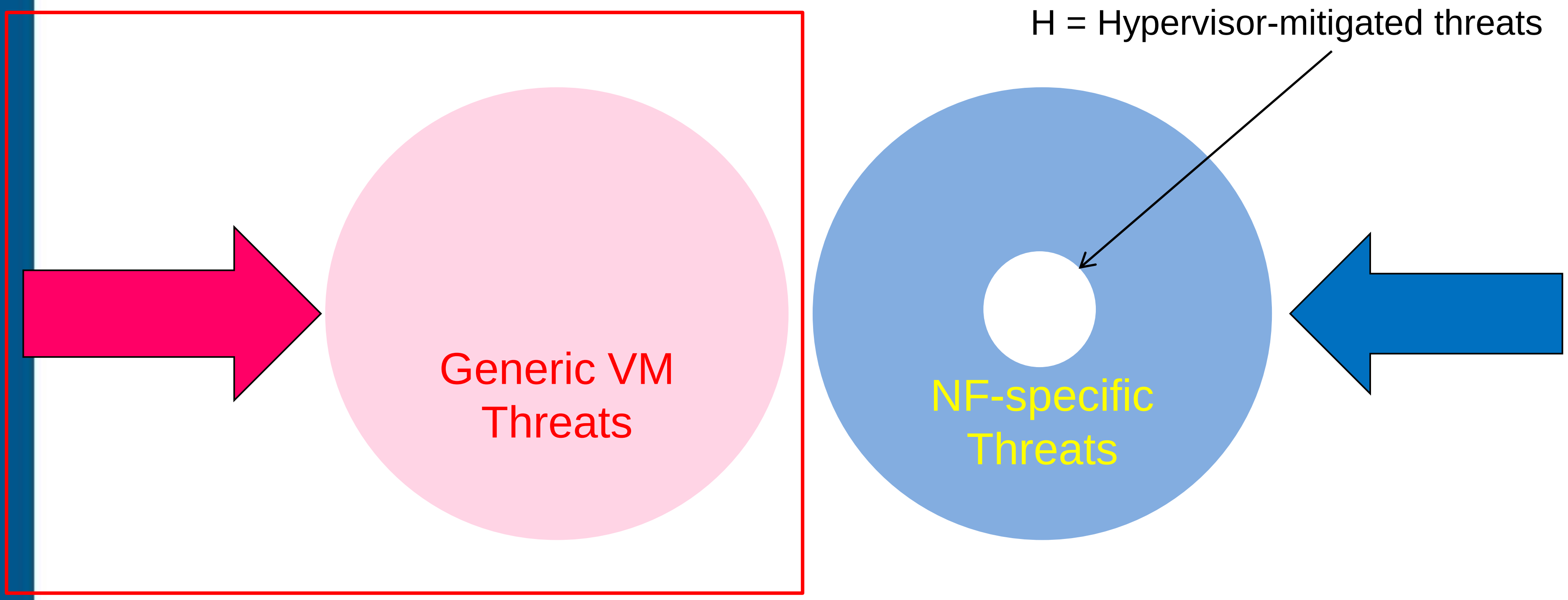
Some Observations

- NFV presents unique opportunities for addressing security problems
- The SEC approach
  - Is anchored to platform security (reinforced through trusted boot and remote attestation)
  - Exploits new capabilities:
    - Automation
    - Remote attestation
    - Hypervisor or agent-enabled introspection
    - Holistic security monitoring
  - Provides global response to security events according to the network operators' policies
- NFV can
  - Facilitate agile provision of secure services by the carrier
  - Provide better protection of the carrier cloud

A unique problem: Multiple trust domains (use case: *Lawful Interception*)

An Abstract View: Threats to a VNF

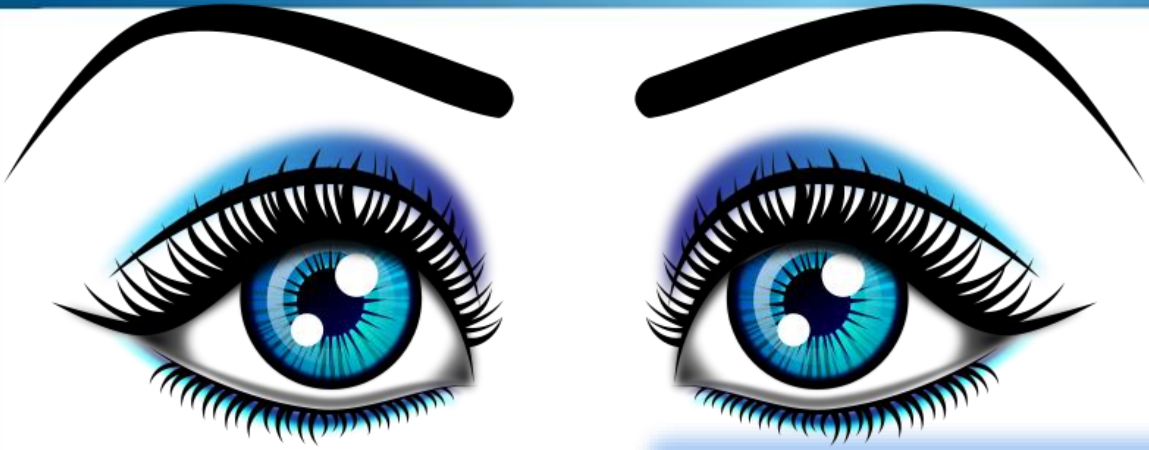
VNF = VMs + NF



VNF Threats = Generic VM Threats ∪ NF-specific Threats / H

Hypervisor Introspection:

Virtual machines have no secrets



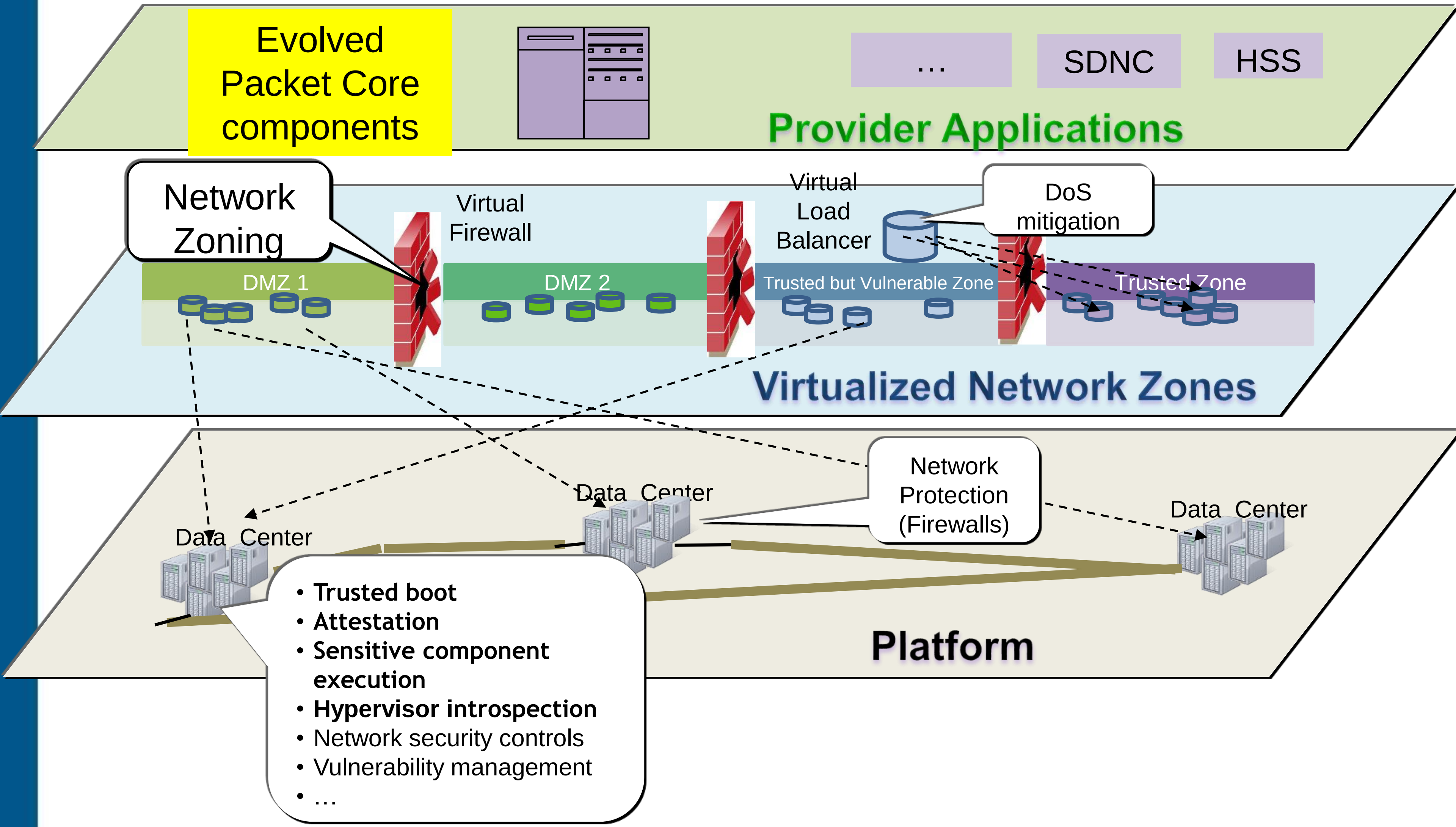
And so:

1) The hypervisor must be trusted

2) There is a need for specialized hardware

3) There is a problem with Lawful Interception

Comprehensive Security



- **Trusted boot**
- **Attestation**
- **Sensitive component execution**
- **Hypervisor introspection**
- Network security controls
- Vulnerability management
- …

Problems identified in the NFV Security Problem Statement

- Topology Validation and Enforcement
- Availability of Management Support Infrastructure
- Secured Boot
- Secure Crash

- Performance Isolation
- User/Tenant Authentication, Authorization, and Accounting
- Authenticated Time Service
- Private Keys within Cloned Images
- Back-doors via Virtualized Test and Monitoring Functions
- Multi-Administrator Isolation
- Security monitoring across multiple administrative domains (i.e., lawful interception)

http://www.etsi.org/deliver/etsi_gs/NFV-SEC/001_099/001/01.01.01_60/gs_NFV-SEC001v010101p.pdf

Major Thrusts in our Current Work

- Lawful Interception
- Architecture for the Execution of Sensitive Components (both the TPM and HSM approaches)
- Remote Attestation (with the review of the latest research on run-time attestation)
- Security of MANO interfaces

The full list of our current work items is available at

https://portal.etsi.org/tb.aspx?tbid=799&SubTB=799

ETSI

World Class Standards

More information:

NFV Technology Page (information)
http://www.etsi.org/nfv

NFV Portal (working area)
http://portal.etsi.org/nfv

NFV Proofs of Concept (information)
http://www.etsi.org/nfv-poc

NFV Plugtest (information & registration)
http://www.etsi.org/nfvplugtest

Open Area:

Drafts http://docbox.etsi.org/ISG/NFV/Open/Drafts/

Issue tracker http://nfvwiki.etsi.org/index.php?title=NFV_Issue_Tracker