A QUICK INTRODUCTION TO THE NFV SEC WG

Igor Faynberg, Cable Labs

Chairman ETSI NFV SEC WG

The NFV SEC Working Group Misson

The NFV SEC Working Group comprises computer-. network-, and Cloud security experts—representing network operators, equipment vendors, and law enforcement agencies—who advice 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 manger—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 the the present 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 Phase 1 in 2012 with the objective to establish the NFV *security problem statement* and advise all working groups rather than have its individual work items (but that has changed!)
- Started by **Bob Briscoe (BT)**
  - with three experts at the onset of the NFV;
  - no communications beyond e-mail exchange
- In Phase 2 has grown to
  - a full working group (Vice Chairman: **Alex Leadbeater, BT)**
  - Steady 30+ active participants from various companies (200 on the list,) and government agencies—regular weekly two-hour-long 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*

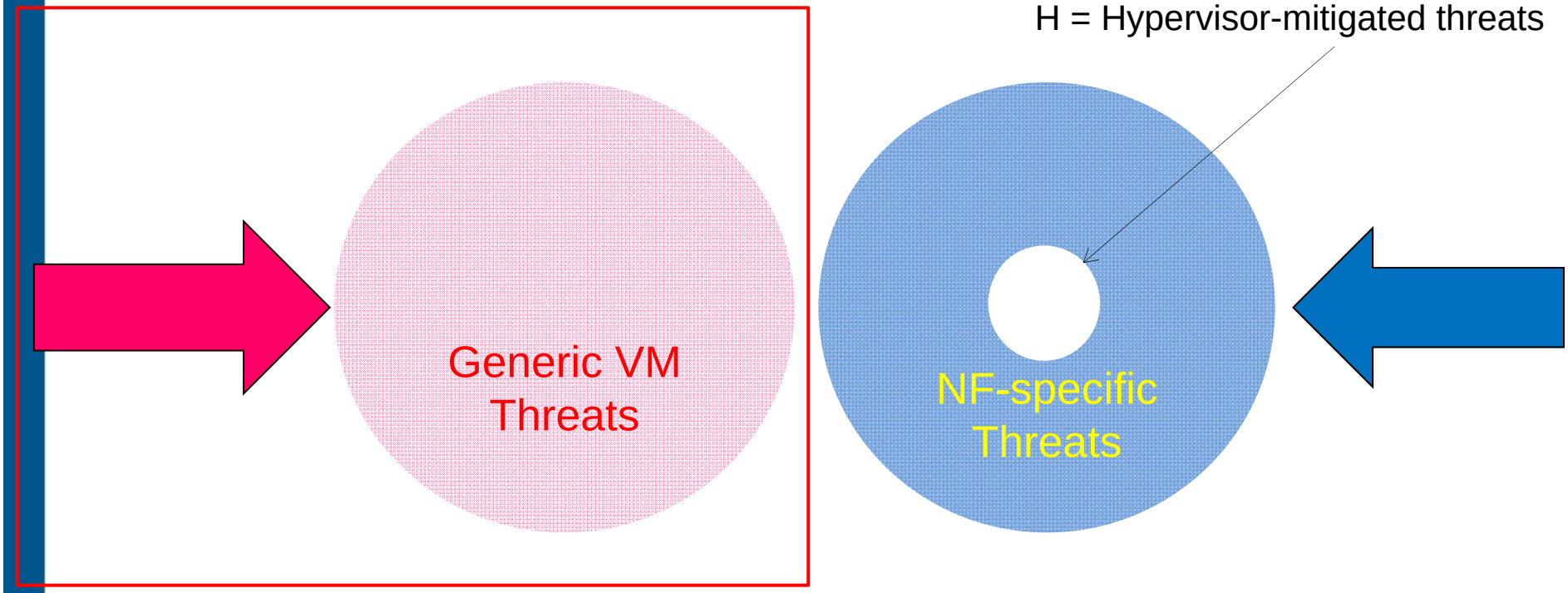
Some Observations

- 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
    - Hypervisor- or agent-enabled introspection
    - Holistic security monitoring
  - Provides global response to security events according to the network operators' policies
- NFV can
  - Improve the security properties of network functions
  - 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

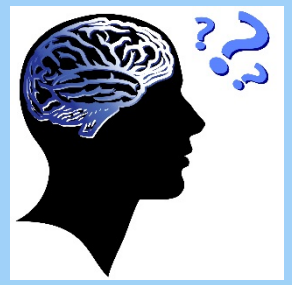
Hypervisor Introspection:
Virtual machines have no secrets

And so:

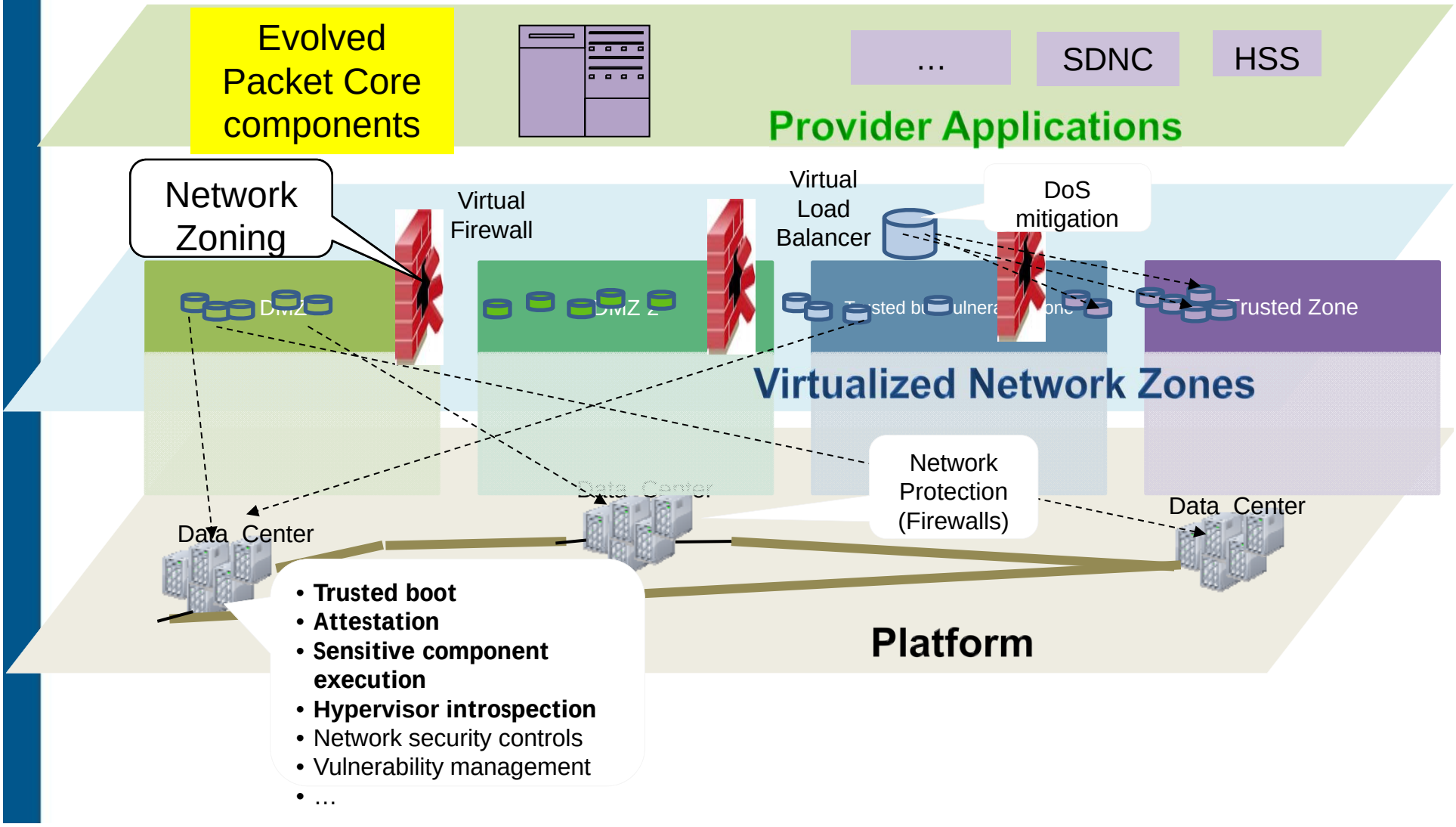
1) The hypervisor must be trusted

2) There is a need for specialized hardware

3) There is a problem with Lawful Interception



Comprehensive Security: a Vision



Problems identified in the NFV Security Problem Statement

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

- 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)

	Topology Validation & Enforcement	Availability of Management Support Infrastructure	Secured Boot	Performance Isolation	User/Tenant AAA	Private Keys within Cloned Images	Back-Doors via Virtualized Test & Monitoring Functions	Multi-Administrator Isolation
Cataloguing security features in management software		*			*	*		*
Report on Lawful Interception Implications				*	*			*
Security and Trust Guidance	*	*	*	*	*	*		*
Report on Certificate Management					*	*		
Report on Attestation Technologies and Practices for Secure Deployments	*		*					*
Report on use cases and technical approaches for multi-layer host administration			*	*				*
Security Report on NFV LI Architecture	*		*	*				*
System architecture specification for execution of sensitive NFV components			*	*			*	*
Security Management and Monitoring specification	*						*	*

Major Thrusts in our Current Work

- Lawful Interception
- Architecture for the Execution of Sensitive Components
- Security Monitoring and Management
- Remote Attestation (with the review of the latest research on run-time attestation)
- Security of MANO interfaces
- Timestamps

Under Construction

- Policy Management
- VNF Package Signing
- Comprehensive Identity Management

The full list of our work items

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