INTRODUCTION TO NFV SEC WG & NFV SECURITY CHALLENGES

Alex Leadbeater, BT Group PLC (UK)

Vice Chairman ETSI NFV SEC WG

BT

NFV & ZERO TOUCH WORLD CONGRESS

NFV Security State of the Art

- NFV potentially offers considerable security improvements over legacy networks when deployed carefully.
  - Virtualisation of specific functions or groups of functions.
  - Enterprise Edge
- Full network single Hypervisor / admin domain virtualisation likely to be insecure and vulnerable.
- Security issues are fixable with enhancement or changes to existing software architectures and platform hardware.
- **So, how do we address these?**

The NFV SEC Working Group Mission

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 Regulatory Requirement 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)*

Some Observations

- NFV presents unique opportunities for addressing legacy security weakness but also introduces new challenges.
- 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
- 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

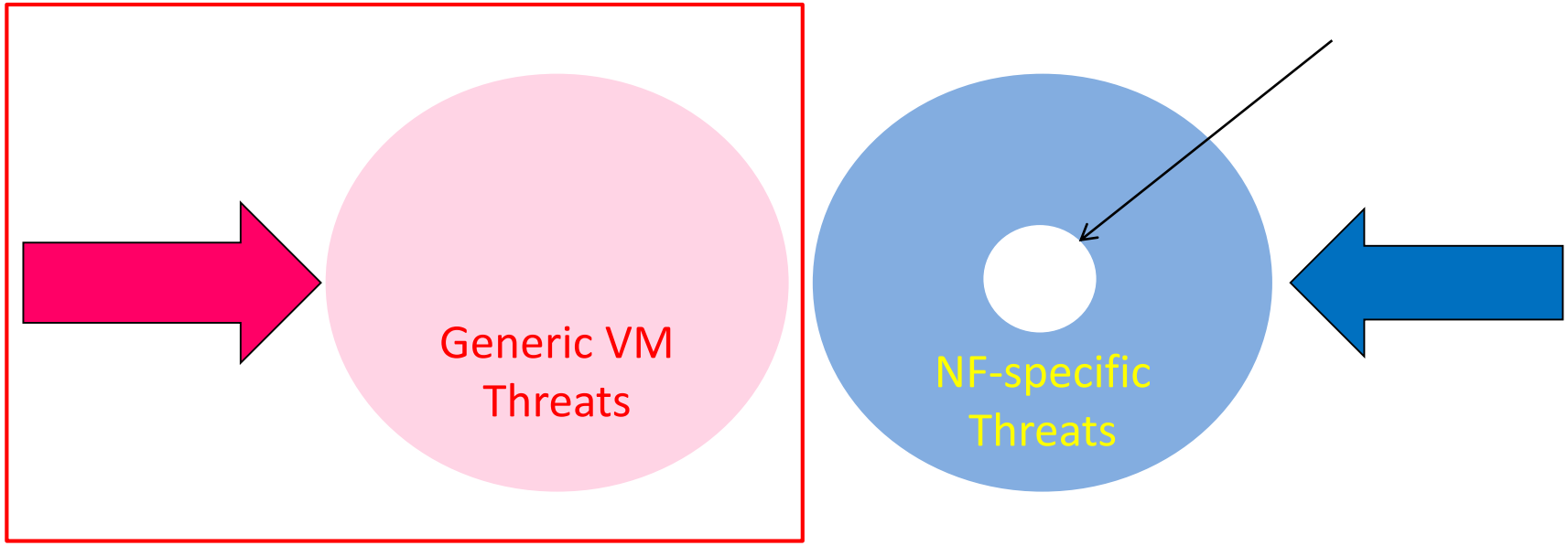
A unique problem: Multiple trust domains [More Later].

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 and Clean Up
- 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 (Sensitive Functions & CNI)

An Abstract View: Threats to a VNF



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

- Threats musts be addressed across virtualisation layers together and not in isolation.

Hypervisor Introspection: Virtual machines have no secrets

And so:

1) The hypervisor must be trusted

2) There is a need for specialized hardware

3) Sensitive functionality must be segregated from general admin view. (AuC, HSS etc)

Some NFV & Industry Gaps

- Problem statement is 2+ years old.
  - Progress on some items better than others.
- Full Multi Trust Domain Hypervisor and Administration OS isolation.
- Host HSM / TPM hardware slicing per VM.
- HSM / TPM mobility
- Platform Hardening for CNI and Sensitive Functions
  - Disabling of unnecessary hardware features in hosts (eg PCIX DMA)
  - Full boot attestation from hardware to VM with direct APIs.
- Precise Time (dedicating cores works but is wasteful).
- Hardware Mediated Execution Environments (HMEEs).

Major Thrusts in our Current Work

- System architecture for execution of sensitive NFV components — NFV SEC 012
  - Considered the minimum baseline for telecoms grade NFV Security.
  - 85% of 3GPP functions are sensitive.
- Security Monitoring and Management — NFV SEC 013
  - Distributed & adaptive security monitoring
  - One of the key security enhancements NFV brings over legacy.
- Remote Attestation Architecture — NFV SEC 018
  - Definition of NFV attestation scope, stakeholders, interfaces and protocols
- Security of MANO interfaces — NFV SEC 014
  - Threats, Mitigations & Requirements
- Security Policy Management — NFV SEC 017
  - Policy Management behind Security Monitoring & Management SEC 013
- API Access Token Specification — NFV SEC 022
  - Access Tokens between VNFs, VNFM, NFVO and VIM

Major Thrusts in our Current Work – Closing the Gaps

- System Architecture Spec for NFV Security Enhancements — NFV SEC 019
  - Building on NFV 012 Baseline.
  - Support for full sensitive function isolation & multi trust domains
  - Critical National Infrastructure (CNI)
- Precise Time, Location & Timestamps — NFV SEC 016
  - The art of the possible
  - New and existing industry capabilities.
- Secure Identity Management — NFV SEC 020
  - End to End / Top to Bottom Identity management
  - Enables Anti-Fraud, Cyber Defense, Network Forensics, System wide Fault Management.
- Regulatory Support — NFV SEC 011

Key Technology Gap Challenges: CNI PoC

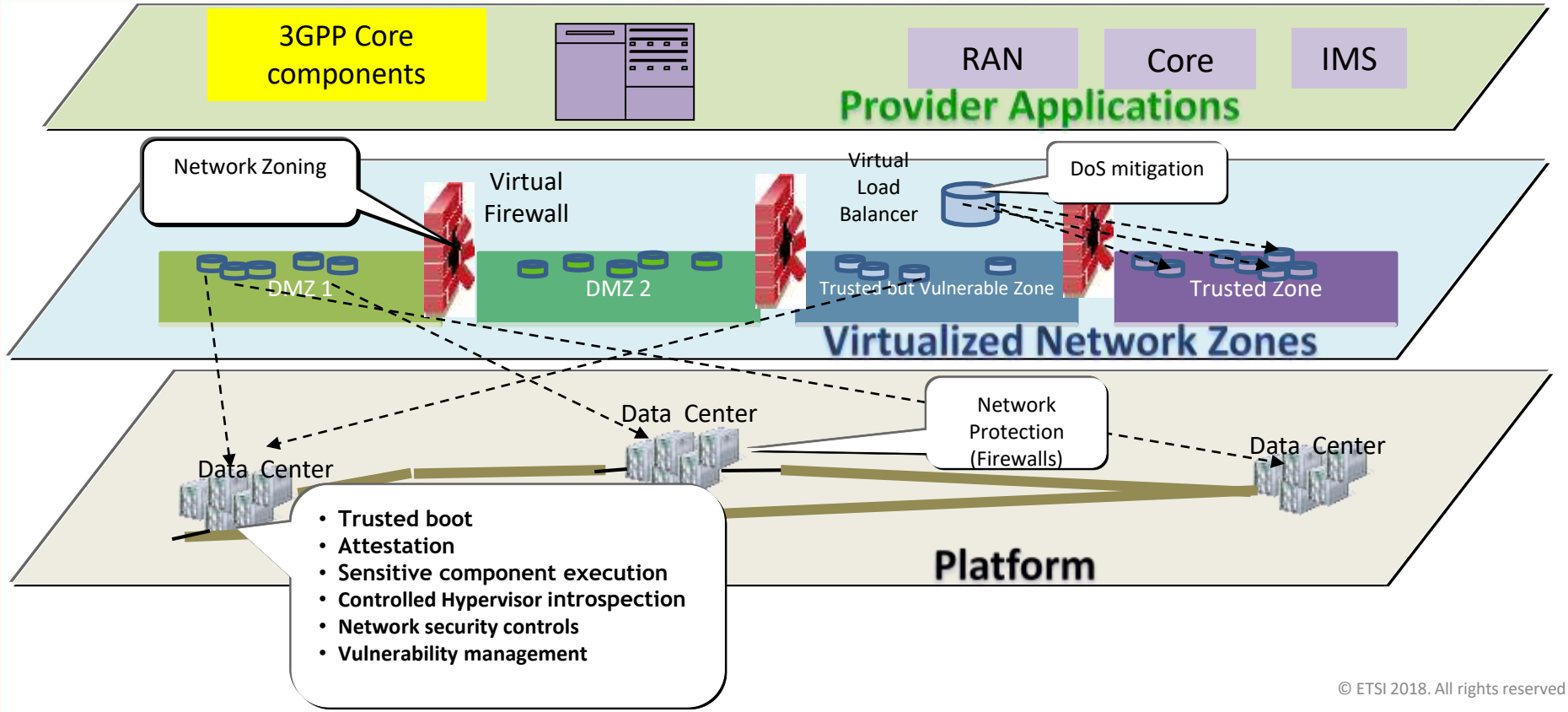
- Administrative isolation
  - For a *given* VNFI, there must exist *at least* two admin layers:
    - A *separate admin layer* must exist for each functional security domain in which that VNFI has a role;
    - Some VNFIs may require four (or more) admin layers.
  - A breach in one admin layer MUST NOT affect any other admin layer.
- Secured execution
  - Must deliver confidentiality and integrity of instructions and data within an area of process space based on a hardware root-of-trust.

Key Technology Gap Challenges: CNI PoC

- Develop a hardware-mediated enclave that delivers
  - confidentiality and integrity

  of instructions and data within a process space, based on a hardware root-of-trust.
- This will protect against
  - Eavesdropping, Replay and masquerade attacks
  - Alteration attacks & Insider threats
- Necessary capabilities:
  - Load validated executable code into enclave;
  - Attest integrity/authenticity of code prior to execution;
  - Load data into enclave, run code, ensure no other process on the host (including Hypervisor) can inspect, alter, replay, etc;
  - Securely transfer data to/from authorized functions outside of enclave;
  - Securely destruct enclave data when no longer required, ensuring that *no data can be recovered*.

Comprehensive Security: A Vision



Summary

- Security is always a moving target.
- NFV brings both benefits and challenges to overall network security compared to legacy networks.
- Secure restricted deployments entirely feasible.
- Wider deployments would currently require additional threat mitigations.
- Remaining security gaps need to be addressed if full power of NFV is to be realised.
- https://portal.etsi.org/tb.aspx?tbid=799&SubTB=799

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:
  - Published Docs: https://docbox.etsi.org/ISG/NFV/Open/Publications_pdf
  - Working Drafts http://docbox.etsi.org/ISG/NFV/Open/Drafts/
  - Issue tracker http://nfvwiki.etsi.org/index.php?title=NFV_Issue_Tracker
  - Detailed Release 3 specification progress can be found at: https://nfvwiki.etsi.org/index.php?title=Feature_Tracking