NFV Security

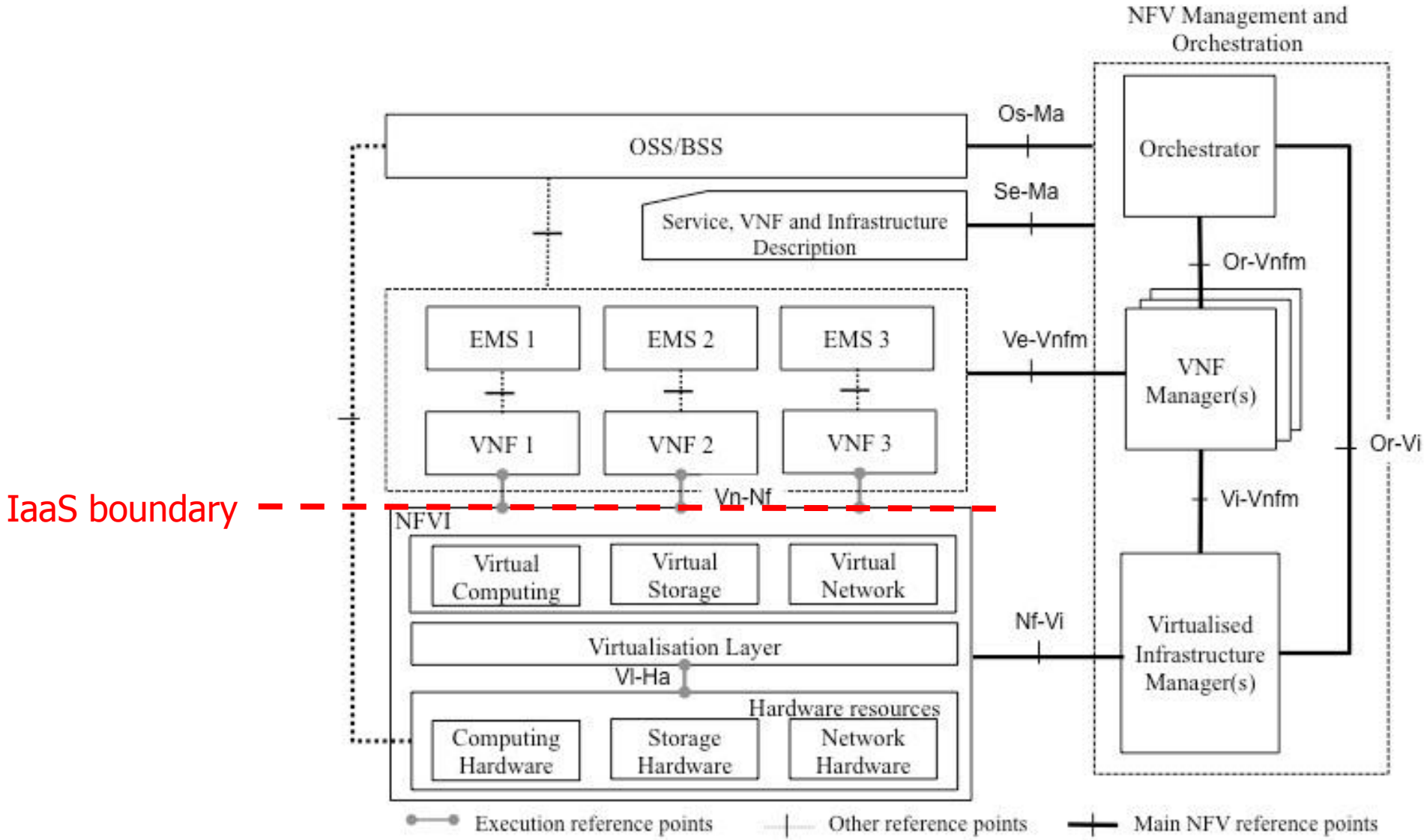
December 8th, 2014

François J.N. Cosquer
IP Platforms CTO Security

Note: *The views expressed in this presentation are those of the author and not necessarily those of Alcatel-Lucent Corporation*

Alcatel·Lucent

NFV = MIGRATION FROM LEGACY TO « CLOUD » ENVIRONMENT



ETSI NFV ISG

RISK: WHAT IS NEW OR DIFFERENT IN NEW ENVIRONMENT? (1/2) INTUITIVELY…

- **Risk potentially impacted by:**
  - Changes of operating environment with additional attack surface layer, combined with the complexity of shared infrastructure
  - Changes in ownership/liability boundaries with potentially mismatched assumptions and expectations between vendors of HW, hypervisors, vNFs and management systems

RISK: WHAT IS NEW OR DIFFERENT? (2/2)
EVIDENCE IS A GOOD COMPLEMENT TO INTUITION…

Using methodology based on a dual approach :

- Top down approach: Survey and identify security issues from industry literature, customers engagements, standard bodies, research institutions

- Bottom up: revisit “usual security suspects” (Confidentiality, Integrity, Availability, etc.) in the scope of the “new” Cloud deployment and operational environment (IaaS as compared to “legacy” platforms)

Objective:

Maintain a list prioritized* of top 5** issues covering in a “holistic” way both breadth and depth

(*) Pragmatic Priority = estimated exposure*implementation mitigation feasibility

(**) 5 should not be read as a fixed number but as a starting point and order of magnitude

TOP SECURITY RISKS

#	RISKS and ISSUES	HIGH LEVEL DEFINITION
SEC-1 INCREMENTAL	**Denial of Service (DoS)** SEC-1.1: DoS or DDoS by flooding of public interface SEC-1.2: DoS by Internal NW resource exhaustion SEC-1.3: DoS by CPU/Memory/Disk resource exhaustion SEC-1.4: DoS by malicious misconfiguration	In the Cloud deployment and IaaS context, Denial of Service needs to be reconsidered with the additional factor of shared resources (Hypervisor, virtual network, compute & storage, etc.)
SEC-2 NEW	**Isolation failure** SEC-2.1: Isolation failure: VM escape SEC-2.2: Isolation failure: VM Hopping SEC-2.3: Isolation failure: prejudicial data access (in transit, in memory, at rest)	In the Cloud deployment and IaaS context, isolation failure becomes a challenge given the additional software layers (Hypervisor / VM) and shared infrastructure.
SEC-3 INCREMENTAL	**Security Logs & incident management failure** SEC-3.1: Lack of Logs SEC-3.2: Complexity of defining logs logical boundary	In the Cloud deployment and « IaaS model » where infrastructure is operated independantly from the applications, security event management and attack identification become more challenging.
SEC-4 NEW	**Legal and regulatory compliancy failure** SEC-4.1: Regulation Geo-deployment SEC-4.2: Compliance in heterogeneous environments	In the Cloud deployment model, the geo- localization of data might need to be enforced; The encryption of specific data might be mandatory. This issue is driven mostly by privacy requirements and legislation.
SEC-5 NEW	**Topology validation & enforcement** SEC-5.1: VM layer misconfiguration SEC-5.2: Topology validation	In the Cloud deployment, the virtual networking configuration layer can be prone to additional errors and make control assurance more challenging.

OPPORTUNITIES

- **NFV changes will provide opportunities to improve security**
  - Leverage the flexibility of virtualized operating environment e.g. the ability to spin up dedicated virtualized firewalls per vNF, automation of firewall placement, configuration and traffic steering, etc.
  - Benefit from advanced virtualization layer capabilities such as hypervisor introspection to monitor and detect anomalous VMs behavior,
  - Automation capabilities such as self-healing

- **SDN** is a key technology enabler for this highly dynamic and complex data center networking environment
  - Fast and easy service turn-up within the data center & between data centers

STANDARDS FOR NFV SEC: «PERSONAL» PERSPECTIVE & PERCEPTION 1/2

- **Perceived Constraints**

  - MATURITY/STABILITY: NFV field is “non mature”, “fast” change pace, “not fully defined” market, “strong” Open Source influence

  - SDO PACE: Standards dev are “slow” pace; Standards need to be relevant for interop and accelerate adoption

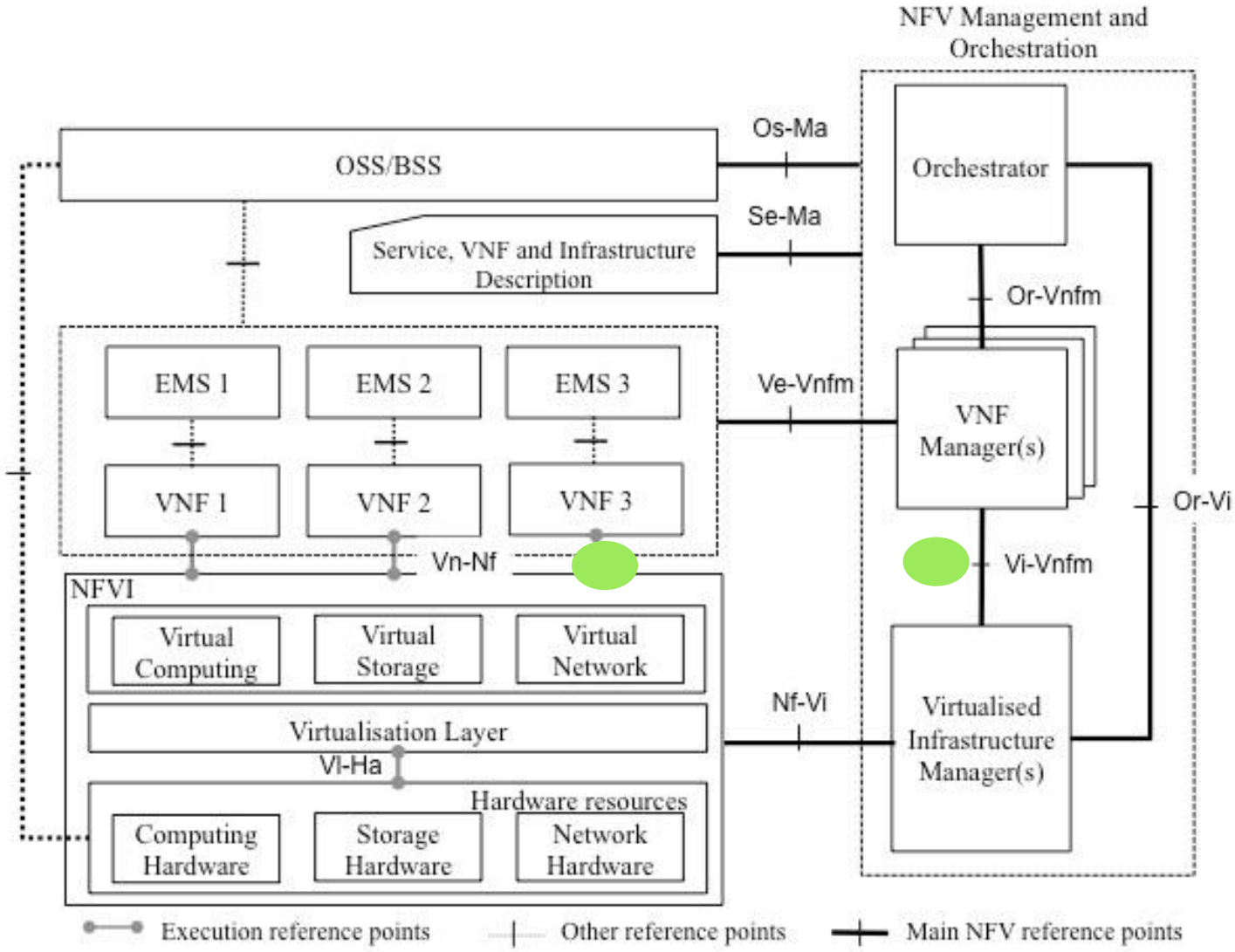
  - CROWDED SPACE: Many bodies and forum active as noted in your previous meetings, effort dilution risk

  - SUCCESSFUL SECURITY STD : lower level such as interface, protocol not architecture (which become basis for best practices and regulations)

  - IT CLOUD: virtualization of IT is more mature field; still perception of lack of standards . Emergence of “de facto” standards linked with strong players. IT and Telco NFV requirements are quite different..

  …. What are the driving forces : FAST INNOVATION vs INTEROP ? Where is security ?

STANDARDS FOR NFV SEC: «PERSONAL» PERSPECTIVE & PERCEPTION 2/2



In that context, NFV security could benefit from very specific effort that helps build technology independent interaction between components

Eg.