Security aspects of Network Functions Virtualization

Prabhu T

NEC India Pvt Ltd

15-12-2015 WWSMC 2015

Outline

- Virtualization and its history
- Role of Cloud Computing
- Introduction to NFV
- Challenges in NFV
- NFV reference architectural framework
- NFV security aspects

Virtualization and its history

- Virtualization technology emulates physical resources such as computing and networking resources, operating systems, storage devices as virtual versions that allow to run multiple virtual versions (applications) on a single physical host machine.

- Virtualization technology was first developed by Jim Rymarczyk as time sharing mainframe systems (shared use of computer resources among a group of users) in 1960s for multitasking purpose by IBM [1].

- It leads to develop Full virtualization, para-virtualization, hardware assisted virtualization, etc. [2].

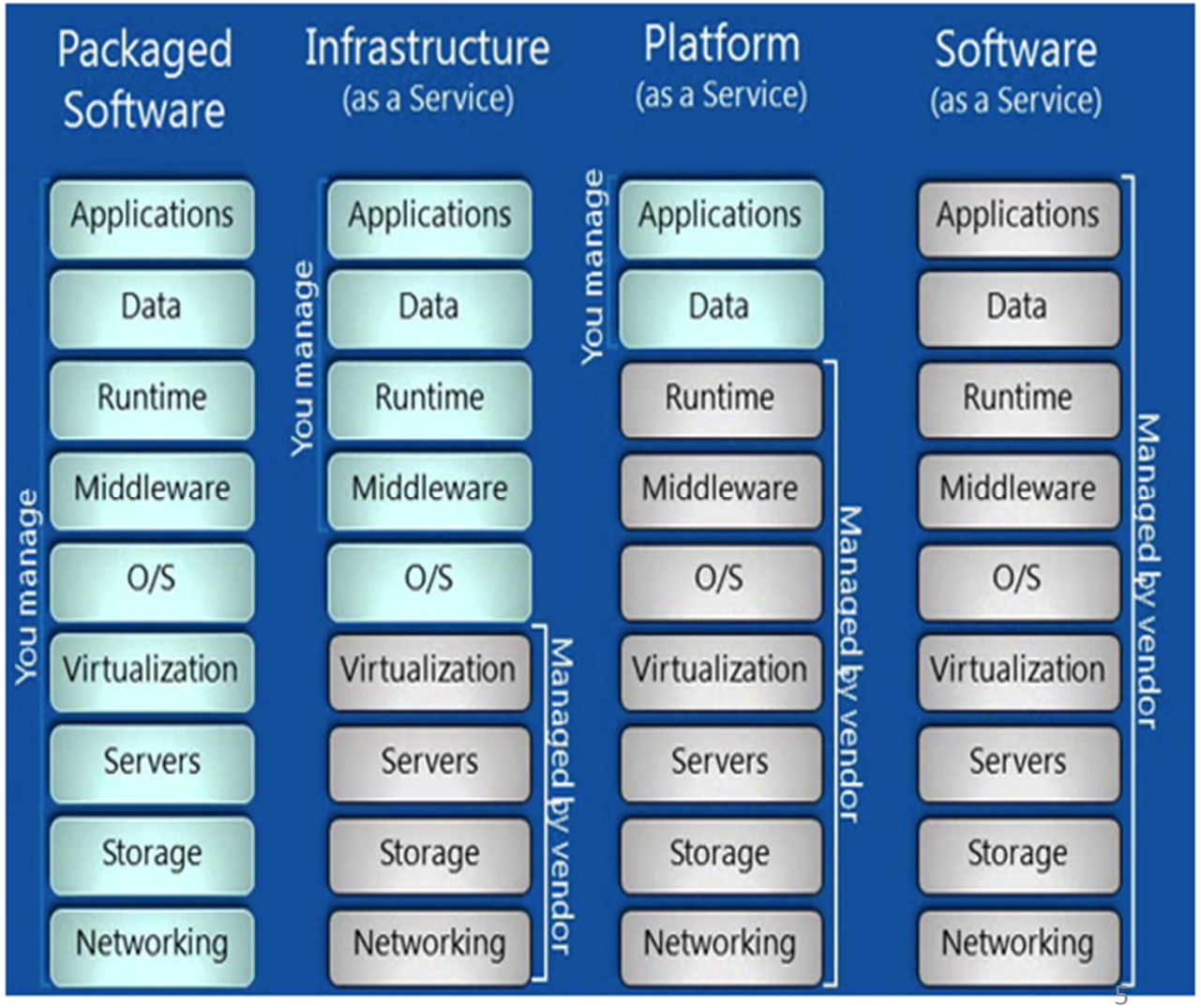
Role of cloud computing (1/2)

- Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction [3].

- Cloud essential characteristics:
  - On demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service

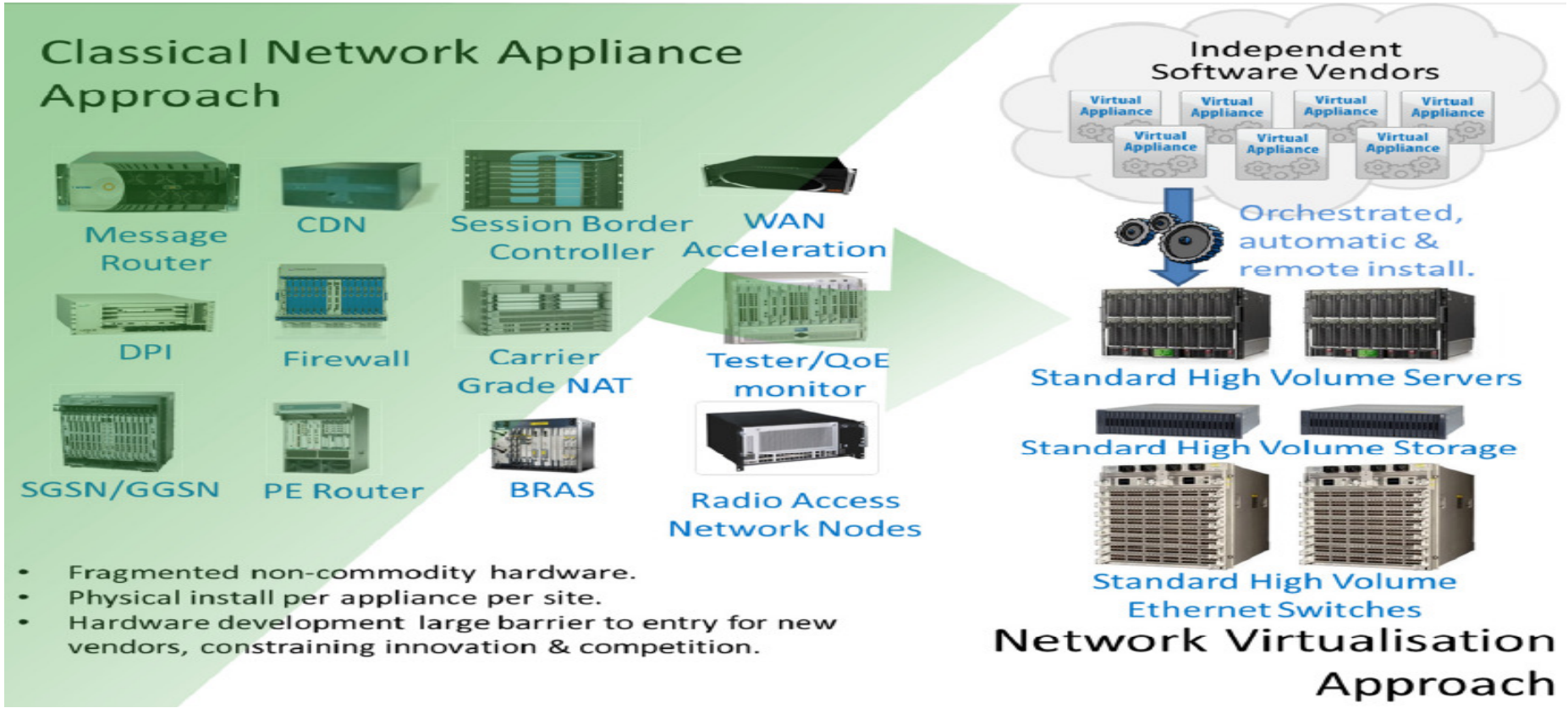
Role of cloud computing (2/2)

- Service models
  - SaaS
  - PaaS
  - IaaS



Introduction to NFV

- NFV aims to run current hardware based network elements or functional blocks as software modules on top of the COTS server by virtualizing the network elements and its functions.

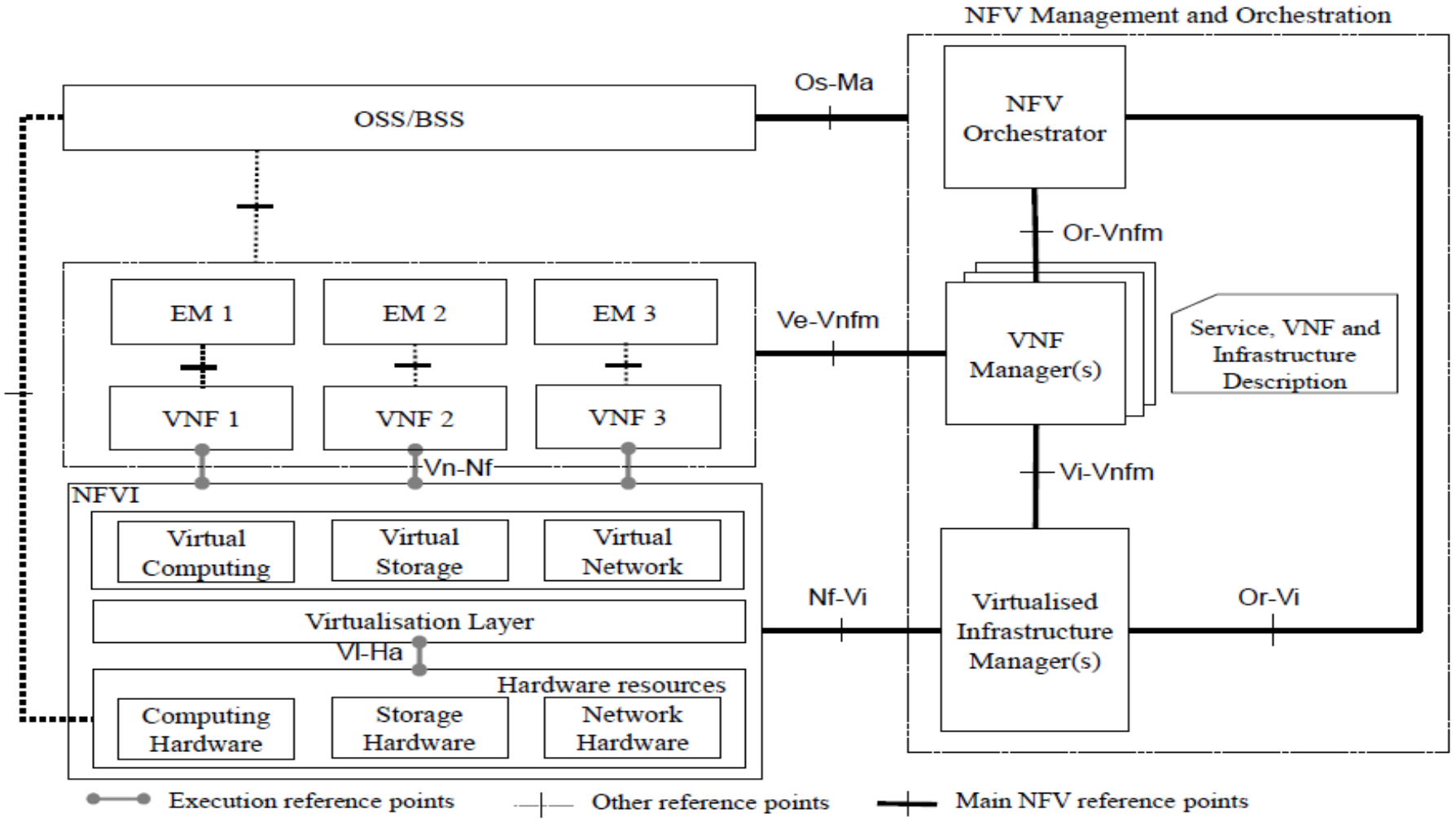


Vision for NFV [4]

Challenges in NFV

- High performance and portability using virtualized network
- Interoperability between different vendors VNFs, hardware, hypervisors, etc.
- Interoperation and co-operation of VNFs with PNFs
- Managing resources and orchestrating multiple VNFs from different locations
- Ensuring security and configuration of dynamic nature of VNFs and other NFV assets
- Automation and scaling
- Resiliency, fault and failure management
- Integration of multiple VNFs of different vendors without lock-in

NFV architectural framework



NFV reference architectural framework [5]

NFV security aspects

- Security aspects of NFV infrastructure
  - Hardware, virtualization layer, host OS and service model aspects
- Security aspects of VNFs network
  - Inter and intra VNF communication
  - Life cycle management of VNF
- Security aspects of NFV MANO
  - Resource and service management aspects
  - Life cycle management of network services
  - Network controller aspects
- Lawful interception
  - Identity issues and geographical regulation issues

Potential areas of concern

The following are highlighted in ETSI NFV SEC document [6]

- Topology Validation and Enforcement
- Availability of Management Support Infrastructure
- User/Tenant Authentication, Authorization, and Accounting
- Secure Crash
- Secured Boot
- Performance Isolation
- Authenticated Time Service
- Private Keys within Cloned Images
- Back-doors via Virtualized Test and Monitoring Functions
- Multi-Administrator Isolation
- Security monitoring and auditing

Other potential concerns

- DoS/DDoS attacks on virtualization layer, resource and service management nodes, network controllers and other sensitive NFV components
- Secure lifecycle management of VNFs and NSs
- Fast and secure live migration of VNFs
- Secure communication over the new NFV reference points and interfaces
- Secure storage and access control

References

[1] History of virtualization, http://www.networkworld.com/article/2254433/virtualization/with-long-history-of-virtualization-behind-it--ibm-looks-to-the-future.html

[2] Vmware: “Understanding Full virtualization, para virtualization, and Hardware assist,” white paper, 2007

[3] NIST 800-145: “The NIST Definition of Cloud Computing,”, 2007

[4] ETSI: “NFV - An Introduction, Benefits, Enablers, Challenges & Call for Action,” 2012

[5] ETSI GS NFV 002: “NFV Architectural Framework,” 2014

[6] ETSI GS NFV SEC 001: “NFV Security; Problem Statement,” 2014