NFV Security – Opportunities and Challenges
(Slides for Discussion in IEEE SRPSDVE Study Group)

Presenter: Ashutosh Dutta, Ph.D.
AT&T Chief Security Organization
IEEE Liaison for ETSI/NFV
Vice Chair – Security Study Group

Email: ashutosh.dutta@att.com
October 29, 2014
Overview of ETSI NFV

• Six Working Groups/Expert Groups
  • Infrastructure WG (INF)
  • Software Architecture (SWA)
  • Management and Orchestration (MANO)
  • Reliability WG
  • Performance Expert Group
  • Security Expert Group
• Proof-of-Concept WG (~25 POC Proposals)
Current Work Items in ETSI/NFV Security Expert Group

- NFV Security Problem Statement – Published
- NFVSEC Security and Trust Guidance Document – Last Call
- Security Monitoring for NFV Deployment – New WI
- Requirements in Certificate Management – New WI
- NFV Certificate Deployment – New WI
- LI Requirements for NFV – New WI
- Gap Analysis for Open Stack Security – New WI
- NFV Attestation – New WI
- Security POCs - ongoing
Security Opportunities and Challenges in a Virtual Environment (ETSI/NFV Problem Statement)

- Hypervisor Vulnerability
- API security
- Orchestration Vulnerability
- Virtual monitoring
  - Limited visibility to Mobility/EPC interfaces (e.g. S6a, S11, S8)
- Virtualized firewalls
- OS level security
  - Secure boot
  - Secure crash
- User/tenant authentication, authentication and accounting
- Topology validation and enforcement
- Performance isolation
- Authenticated Time Service
- Private Keys within Cloud Images
- Detection of attacks on resources in virtualization infrastructure
**ETSI NFV Use Cases**

- **Use Case 1:** Network Functions Virtualization Infrastructure as a Service
- **Use Case 2:** Virtual Network Function as a Service (VNFaaS)
- **Use Case 3:** Virtual Network Platform as a Service (VNPaaS)
- **Use Case 4:** VNF Forwarding Graphs
- **Use Case 5:** Virtualization of Mobile Core Network and IMS
- **Use Case 6:** Virtualization of Mobile Base Station
- **Use Case 7:** Virtualization of the Home Environment
- **Use Case 8:** Virtualization of CDNs (vCDN)
- **Use Case 9:** Fixed Access Network Functions Virtualization
Overview of NFV Use cases

- Virtualization of Mobile CORE and IMS
- Virtualization of Base Stations
- Virtualization of CDN
- Virtualization of Fixed Access
- Virtualization of Home and Enterprise Networks
The Mobility Network of the Future
A Cloud-Based Architecture

Faster and Simplified
Faster Provisioning / Time-to-Market
Effortless Customer Experience
Less Vulnerable

Lower Cost
Reduced Cost of Hardware, Operations, etc.
Higher Utilization
Security as a Service

Scalable
Create new products and services quicker than before
High Bandwidth/Low Latency Applications
Service Chaining – Security services on demand

Secure
Strong Authentication
Firewalls, Proxies, Deep Packet Inspection, etc.
Security Function Virtualization

Dynamic
Network on Demand, Increased Reliability, Flexible
Analytics “Big Data”
Resiliency to DDOS attack

Accessible
Always Connected World
COU, BYOD, Next-Gen App
Flexible
## Security Opportunities from Virtualization

### Benefits of Network Virtualization

<table>
<thead>
<tr>
<th>Benefit</th>
<th>Security Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Simplify the network and remove complexity by separation of control and data</td>
<td>Makes network components less vulnerable to attacks</td>
</tr>
<tr>
<td>Scalability and Network Function Redundancy</td>
<td>Fortifies DDOS mitigation scheme</td>
</tr>
<tr>
<td>Ability to Deploy Multivendor Solutions</td>
<td>Security Function Virtualization</td>
</tr>
<tr>
<td></td>
<td>Security as a Service at Scale</td>
</tr>
</tbody>
</table>
### Security Opportunities from Virtualization

<table>
<thead>
<tr>
<th>Benefits of Network Virtualization</th>
<th>Security Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automation and Relatively Central Management</td>
<td>• Consistent policy configurations and easier regulatory compliance</td>
</tr>
<tr>
<td>Easier integration with operations systems support</td>
<td>• Automated Quarantining</td>
</tr>
<tr>
<td>Flexible Network Configuration</td>
<td>• Facilitates comprehensive security</td>
</tr>
<tr>
<td></td>
<td>• Security Autonomics</td>
</tr>
<tr>
<td></td>
<td>• Easier Patch Management</td>
</tr>
<tr>
<td></td>
<td>• Better Incident Response</td>
</tr>
<tr>
<td></td>
<td>• Traffic Management</td>
</tr>
</tbody>
</table>
Virtualized Mobility Network
The Vision for a Software Defined Network
Network Function Virtualization
Security Challenges and Opportunities

- Existing Threats
- New Virtualization Threats
- Security Opportunities

**Orchestration**
- vMME
- vHSS
- vPCRF
- vS-GW
- vP-GW
- vPCEF

**Hypervisor**
- Common Hardware

**DDoS Mitigation Scheme**
- DDoS Signaling Storm by Mobile Devices
- Attacks from User Plane by Mobile Devices

**Exploit Orchestration Vulnerability**
- DDoS/Attacks from the Internet
- Exploit Hypervisor Vulnerability
- Amplification Attacks Enhanced by Elasticity Function

Mobile Devices (Smartphones, M2M, IoT)

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
Mobility Security in the Cloud
What are Security Opportunities?

- Security Function Virtualization
- Security Services at Scale
- DDoS Mitigation Scheme
- Better Incident Response
Virtualized Mobility Network

Security as a Service at Scale - Opportunity

Security Function Virtualization helps to service chain different types of security services.

Ability to deploy multi-vendor VNFs (e.g., vEPC) makes the network scalable and reliable.

Ability to deploy multi-vendor security services makes it scalable and reliable.

Orchestration

Hypervisor

Common Off The Shelf (COTS) Hardware

Real Time Services

Internet

Cloud Services

Partner Networks
Security Opportunities from Virtualization
DDoS Attack Resiliency on Signaling and Data Plane

Malicious Signaling Storm Traffic

Malware infected Traffic on data plane

Orchestrator instantiates new VM to scale-out vMMME function to sustain the higher traffic load

Orchestrator instantiates new VM to scale-out vPGW function to sustain the higher traffic load
Security Opportunities from Virtualization
SDN Controller Dynamic Service Chaining

Malware on Mobile Devices sends malformed IP packets

SDN Controller dynamically modifies the firewall rules for the related firewalls to thwart the attack

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
Mobility Security in the Cloud
What are the New Attack Vectors?

- Orchestration Vulnerability
- Hypervisor Vulnerability
- Elasticity Amplification
Security Challenges from Virtualization
DNS Amplification Attacks Enhanced by Elasticity Function

Orchestrator instantiates new VM to scale-out vDNS function to accommodate more queries... becomes multiple recursive DNS sever responding to victim

Malicious DNS queries (spoofed source IP address set to the address of the victim)

Victim receives the DNS query response (large/amplified packets)
Security Challenges from Virtualization
Hypervisor and VM

- Increased Admin Privileges
- Host Code Execution
- Resource Exhaustion
- Opportunity

Virtualized Mobility Functions:
- vEPC
- vP-GW
- vPCRF
- vIMS
- vHSS
- vSBC

Orchestration
Hypervisor
Common Off The Shelf (COTS) Hardware

Hypervisor –assisted Introspection provides VM Isolation
Security Pillars
Areas of focus for Security Virtualization

- Security Function Virtualization
- Proof of Concepts
- Security Analytics
- SDN Controller Security
- Policy
- NFV/VNF
- Identity & Access Management
- Orchestration Security
- Regulatory & Compliance
- Hypervisor Security
- API Security
- Data Protection & Privacy
- Trusted Software
- Trusted Software
Threat Scenarios from ETSI NFV Contribution

DC 1

VM1

VM APPs

VM APPs

Web Portal

vSwitch

VMM

Host OS

NIC

MAN/Backbone Network

Boundary network node

EMS/NMS

Internet

ISP

Remote maintenance

Hacker

Social engineering attack

APT attack

Application vulnerabilities

Hacker

Network penetration

Network sniffer

ARP, DoS attack

eavesdropping

misoperation

Improper security policy configuration

malicious behaviour
Threat 1: Attack from VMs in the same domain
- VM would be manipulated by attackers and potentially extend the attack to other VMs
- Buffer overflow, DOS, ARP, Hypervisor, vswitch

Threat 2: Attack to host, hypervisor and VMs from applications in host machine
- Poor design of hypervisors, improper configuration
- Attackers inject malicious software to virtual memory and control VM
- Malformed packet attacks to hypervisors

Threat 3: Attack from host applications communicating with VMs
- Host applications being attacked can initiate monitoring, tampering or DOS attack to communications going through host vSwitch
- Improper network isolation, Improper configuration to application privileges of host machine
- Lack of restriction to services or application
Threat 4: Attack to VMs from remote management path
- Outside attackers could initiate communication by eavesdropping, tampering, DOS attack, and Man-in-the-Middle attack
- Gain illegal access of the system and access OS without authorization, tamper and obtain sensitive and important information of a system
- Poor design and development of the application may lead to many known attacks (e.g., buffer overflow attacks)

Threat 5: Attack to external communication with 3rd party applications
- The API interface accessed by 3rd party applications in the untrusted domains is easily subject to malicious attack. Such attack includes illegal access to API, DOS attack to API platform
- Logical bugs in APIs, API authentication/authorization mechanism problems and security policy configuration problems.

Threat 6: Attack from external network via network edge node
- Virtualized Firewalls, Residential gateways

Threat 7: Attack from host machines or VMs of external network domain
- VNF migration, VNF scaling (Scale in- Scale out)
Hypervisor Vulnerability (Example)

Use Case: Hypervisor gets compromised somehow by the attacker. Attacker uses hypervisor privilege to install kernel root kit in VNF’s OS and thereby controls and modifies the VNF.

Mitigation Techniques:

• Hypervisor Introspection schemes can use the Hypervisor’s higher privilege to secure the guest VMs.
  • A Hypervisor-based introspection scheme can detect guest OS rootkit that got installed by the attacker.
• Adoption of Hypervisor hardening mechanisms can protect hypervisor’s code and data from unauthorized modification and can guard against bugs and misconfigurations in the hardened hypervisors.
• Use Software vulnerability management procedure to make sure the hypervisor is secured from attack
• **Use Case:** An attacker uses legitimate access to the orchestrator and manipulates its configuration in order to run a modified VNF or alter the behavior of the VNF through changing its configuration through the orchestrator. This will compromise the VNF separation as the administrator of one VNF can get admin privilege of another VNF and the separation between the VNFs cannot be maintained.

• **Potential Mitigation Techniques:**
  
  • Deploy some of the inherent best current practices for orchestration security by way of detection mechanism when the separation is violated, provide secure logging for access, automated system or configuration auditing.
  
  • Deploy security monitoring system that will detect the compromised VNF separation, any kind of anomaly in the system or provide alert mechanism when some critical configuration data in the orchestrator is altered.
  
  • Access Control, File system protection, system integrity protection
  
  • Hardening of separation policy through proper configuration management
<table>
<thead>
<tr>
<th>Category</th>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1</td>
<td>Loss of Availability</td>
<td>Attackers flood an interface resulting in DoS condition (e.g. multiple authentication failure on s6a, DNS lookup)</td>
</tr>
<tr>
<td>T2</td>
<td>Crashing a network element</td>
<td>Attackers crash a network element by sending malformed packets</td>
</tr>
<tr>
<td>T3</td>
<td>Loss of Confidentiality</td>
<td>Attackers eavesdrop on sensitive data on control and bearer plane</td>
</tr>
<tr>
<td>T4</td>
<td>Data leakage</td>
<td>Unauthorized access to sensitive data on the server (HSS profile, etc.)</td>
</tr>
<tr>
<td>T5</td>
<td>Loss of Integrity</td>
<td>Attackers modify information during transit (DNS redirection, etc.)</td>
</tr>
<tr>
<td>T6</td>
<td>Data modification</td>
<td>Attackers modify data on network element (change the NE configurations)</td>
</tr>
<tr>
<td>T7</td>
<td>Loss of Control</td>
<td>Attackers control the network via protocol or implementation flaw</td>
</tr>
<tr>
<td>T8</td>
<td>Compromise of network element</td>
<td>Attackers compromise of network element via management interface</td>
</tr>
<tr>
<td>T9</td>
<td>Malicious Insider</td>
<td>Insiders make data modification on network elements, make unauthorized changes to NE configuration, etc.</td>
</tr>
<tr>
<td>T10</td>
<td>Theft of Service</td>
<td>Attackers exploits a flaw to use services without being charged</td>
</tr>
</tbody>
</table>

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
Data Plane Overload by DDoS
Malware-Based Attack

Subscriber with Malware

DOS by Malware

eNodeB

MME

HSS

PCRF

S1-MME

S1-U

S11

S6a

Gx

S5

SGi

P-GW

Other Mobile Operators

Internet or Other PDNs

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
Signaling Plane Overload via DDoS
UE authentication Failure Attack
Classification of NFV Security

• OS
• Network
• Protocol
• Mobility (Specific to Mobility Network)
• Cloud+
• NFV Specific
• Threat Scenarios
## Basic NFV Security Features

<table>
<thead>
<tr>
<th>Security Goals</th>
<th>Security Tasks</th>
<th>Security classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>ID Management</td>
<td>Enhanced password policy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Repeated attempt lock out</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use external AAA</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Use 2-factor authentication</td>
<td></td>
</tr>
<tr>
<td>Hardening</td>
<td>Removes unnecessary services and lockdown configurations</td>
<td>OS</td>
</tr>
<tr>
<td></td>
<td>Patch procedure, patch strategy, and patch life-cycle mgmt</td>
<td></td>
</tr>
<tr>
<td>Advanced Threat</td>
<td>Anti-virus and Anti-malware</td>
<td>OS</td>
</tr>
<tr>
<td>Firewall</td>
<td>Virtual firewall appliance</td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Hypervisor introspection</td>
<td></td>
</tr>
<tr>
<td>IDS/IPS</td>
<td>Virtual monitoring</td>
<td>Network</td>
</tr>
<tr>
<td></td>
<td>Virtual security appliance</td>
<td></td>
</tr>
</tbody>
</table>

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
## Security Feature Enhancements on NFV
### Basic – Mobility Security

<table>
<thead>
<tr>
<th>Security Goals</th>
<th>Security Tasks</th>
<th>Security classification</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobility Standards and Protocol Security</strong></td>
<td>AKA -authentication process</td>
<td>Mobility</td>
</tr>
<tr>
<td></td>
<td>NAS signaling ciphering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>NAS signaling integrity protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RRC signaling ciphering</td>
<td></td>
</tr>
<tr>
<td></td>
<td>RRC signaling integrity protection</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Temporary ID assignment by EPC e.g. GUTI and TMSI</td>
<td></td>
</tr>
<tr>
<td><strong>Enhanced 911</strong></td>
<td>Authentication and encryption over SLg interface to Intrado/TCS</td>
<td>Mobility</td>
</tr>
<tr>
<td><strong>CALEA</strong></td>
<td>Authentication and encryption for connectivity to LEA over HI2 (signaling) and HI3 (content) interfaces</td>
<td>Mobility</td>
</tr>
<tr>
<td><strong>Transport Security</strong></td>
<td>IPSec for backhaul e.g., third party network or cloud platform issues</td>
<td>Mobility</td>
</tr>
<tr>
<td><strong>User Plane Ciphering</strong></td>
<td>User Plane Ciphering</td>
<td>Mobility</td>
</tr>
</tbody>
</table>
## Security Feature Enhancements on NFV

### Cloud Enhancement

<table>
<thead>
<tr>
<th>Security Goals</th>
<th>Security Tasks</th>
<th>Security classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Limit Exposure and Protecting Highly Exposed Area</td>
<td>Establish zone architecture</td>
<td>Cloud+</td>
</tr>
<tr>
<td></td>
<td>On Internet connection: DDoS/inbound FW protection</td>
<td></td>
</tr>
<tr>
<td>Enhanced Cloud Security and Compensating Control</td>
<td>Create per-VM encryption capability</td>
<td>Cloud+</td>
</tr>
<tr>
<td>Enhanced Cloud Security on Control Plane Access</td>
<td>XML firewall on North-facing API access portal</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Control administrator’s console access through RBAC</td>
<td>Cloud+</td>
</tr>
<tr>
<td></td>
<td>Administrator access under two-factor authentication</td>
<td></td>
</tr>
</tbody>
</table>
### Security Feature Enhancements on NFV

#### NFV Security

<table>
<thead>
<tr>
<th>Security Goals</th>
<th>Security Tasks</th>
<th>Security classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application-aware Security Gateway</td>
<td>In-line NFV-aware DPI virtual IDPS appliance for detection and ramification</td>
<td>NFV</td>
</tr>
</tbody>
</table>
| Enhanced OS/App loading security      | ▪ abnormal process detection  
▪ trusted boot  
▪ trusted application execution     |                         |
| Service Chaining                      | Authenticated NFV when added/inserted into the processing chain                | NFV                     |
|                                       | Action of dropping the NFV from the processing chain is authenticated and assured |                        |
|                                       | Session-state remains assured, authenticated and recoverable when a NFV module is dropped from the processing chain |                        |
|                                       | Asset inventory and accounting of the modules for platform integrity  
Multitenant or carrier of carriers (e.g., MVNO) accounting |                        |

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
## Security Feature Enhancements on NFV

### NFV Security

<table>
<thead>
<tr>
<th>Security Goals</th>
<th>Security Tasks</th>
<th>Security classification</th>
</tr>
</thead>
</table>
| Application-aware Security Monitoring               | NFV Threat Detection based on consolidated SIEM  
Correlate application, OS and network detected security events/logs            | NFV                     |
| On-demand Security Ramification Measures in the Cloud| Flexible topology modification for on-demand virtual DPI appliance in-line insertion to conduct emergency FW/IDPS filtering | NFV                     |
| Enhanced Application Security                       | Customized and run-time key management using PKI augmented with HSM           | NFV                     |
| Enhanced Application Security                       | Enhanced verification methodologies for protocol and/or state-machine violations | NFV                     |
| Enhanced Application Security and Integrity         | Detection mechanism for overloading a production function (Enhance L7+ DDoS)   | NFV                     |
| Enhanced Application Security and Integrity         | Inter-site resiliency design – High Availability, and also to cover BC & DR (Business Continuity and Disaster Recovery) | NFV                     |

© 2014 AT&T Intellectual Property. All rights reserved. AT&T and the AT&T logo are trademarks of AT&T Intellectual Property.
Security Feature Enhancements on NFV

### NFV Security

<table>
<thead>
<tr>
<th>Security Goals</th>
<th>Security Tasks</th>
<th>Security classification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enhanced Application Security and Service Reputation</td>
<td>Internet connection - outbound AUP (Accepted Use Policy) violation detection</td>
<td>NFV</td>
</tr>
<tr>
<td>Enhanced Application Security and Service Revenue</td>
<td>Theft of Service (APN abuse) i.e., user bypass the validation in HSS/PCRF/PCEF to use services without being charged</td>
<td>NFV</td>
</tr>
</tbody>
</table>
Summary

- Transformation of Mobility to Cloud
- Emerging services are evolving rapidly
- Opportunities in this new virtualized environment
- Need to develop Threat Taxonomy, Threat Models and Mitigation Techniques for new Security Challenges
- Comprehensive security architecture is essential
Summary

- ETSI/NFV Investigates Security Deployment Issues
- Transformation of Mobility to Cloud
- Emerging services are evolving rapidly
- Opportunities in this new virtualized environment
- Need to develop Threat Taxonomy, Threat Models and Mitigation Techniques for new Security Challenges
- Comprehensive security architecture is essential