NFF Security in Telecom: Yesterday, Today, and Tomorrow

Igor Faynberg
September 2, 2014
Traditional Network Function Deployment

Assumptions:
- Network functions may be directly accessible to subscribers.
- Are managed by internal business units.
- Are physically separated.

Threats:
- Denial of service
- Exploit or violation due to:
  - Administrative error
  - Vulnerabilities of network functions (including hardware, firmware, and software)
- Rogue Insider
Threats to a VNF

VNF = VM + NF

H = Hypervisor-mitigated threats

VNF Threats = Generic VM Threats \cup NF-specific Threats / H
**Assumptions:**
- No external access to Provider’s network
- Network functions managed by internal business units

**SDNC:** SDN Controller
**PCRF:** Policy and Charging Rules Function

**Threats:**
- Exploit or violation due to
  - Administrative error
  - Native vulnerabilities of VNFs
  - Vulnerabilities of virtualization software
  - Vulnerabilities of image files
  - Vulnerabilities of hardware or firmware
- Rogue insider
Assumptions:
Network functions
• are managed by internal business units
• may be accessible to subscribers

Threats:
• All previous threats (amplified) +
• Denial of service

SDNC: SDN Controller
CDN: Content Delivery Network
Assumptions:
Network functions
• may be managed by a third party
• may be directly accessible to subscribers

SDNC: SDN Controller
CDN: Content Delivery Network

Threats:
• All previous threats (amplified) +
• (Involuntary) key escrow
Assumptions
Network functions
• are managed by different parties
• may be accessible to subscribers

Threats:
• All previous threats (amplified) +
• Bad tenant or neighbor
## Threat Mitigation

<table>
<thead>
<tr>
<th></th>
<th>auto-mation</th>
<th>intro-inspection</th>
<th>security analytics</th>
<th>virtual security appliance</th>
<th>strong authN</th>
<th>fine-grained authZ</th>
<th>security zoning</th>
<th>encryption</th>
<th>HSM</th>
<th>secure boot</th>
<th>3rd-party certification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Denial of service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit or violation due to administrative errors</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit or violation due to native vulnerabilities of VNFs</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit or violation due to vulnerabilities of virtualization software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit or violation due to vulnerabilities of VNF images</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Key escrow</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Bad tenant or neighbor</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Rogue insider</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit or violation due to vulnerabilities of hardware and firmware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- Preventive + reactive; software-centric
- Preventive; software-centric
- Preventive
Building-up Comprehensive Security (1/2)

Evolved Packet Core components

Provider Applications

Security as a service
Additional enabler for dynamic security zoning
Additional authentication factors

Network Zoning
Virtual Firewall
DMZ 1
DMZ 2
Virtual Load Balancer
Trusted but Vulnerable Zone
Trusted Zone
DoS mitigation

Virtualized Network Zones

Node hardening
Hypervisor introspection
Network security controls
Vulnerability management

Platform

Network Protection (Firewalls)

Data Center

Evolved Packet Core components
Building up Comprehensive Security (2/2)

**Platform security**
- Physical cloud nodes
- Management System (lifecycle, orchestration, API access, etc.)
- Connectivity
- Federated clouds

**Security through virtualized network functions**
- Load balancing
- Security zoning (e.g., firewall)
- Deep packet inspection
- Domain name service

**Security as a service**
- Identity and access management
- Secure storage (key management and cryptographic operations)
- Security posture assessment and remediation

**On-boarded Application protection**
- Native security
- Cloud-assisted security leveraging virtual security appliances and platform capabilities (e.g., logging, analytics, auto-load-balancing, and auto-healing)
Conclusion

- NFV presents unique opportunities for addressing security problems
- We outline a recursive approach, which
  - Is anchored to platform security
  - Exploits new capabilities
    - Automation and analytics
    - Hypervisor-enabled introspection
- 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