Security Challenges and Opportunities in SDN/NFV Networks

Presenter: Ashutosh Dutta, Ph.D.

Chief Security Organization

AT&T, New Jersey, USA

Email: ashutosh.dutta@att.com

November 11, 2016

Talk Outline

- Drivers for Network Virtualization
- Opportunities and Challenges in Security Virtualization
- Threat Scenarios
- Use Cases
- Industry Standards Activities
- Summary

Emerging Services Trends
Our Connected World is Evolving!

Smart Workplace
Asset Tracking
Internet of Things
WebTV
Video
Smart Meter
Digital Content
Smart City
Mobilize Everything
Robotics
Semantic Web
Security
Big Data
SmartGrid
Augmented Reality
M2M
Digital Learning
Sensor Network
Wearable Computing
Virtualization
BYOD
Voice Recognition
Digital Life
Gesture Computing
Entertainment
Gamification
Gaming
Connected Car
Social Internet
Location Based Services
Mobile Payment
Mobile Advertisement
mHealth
Knowledge Management
Virtual Personal Assistant
User Generate Content
Software Defined Anything

Key Characteristics of 5G

- Massive MIMO
- RAN Transmission – Centimeter and Millimeter Waves
- New Waveforms
- Shared Spectrum Access
- Advanced Inter-Node Coordination
- Simultaneous Transmission Reception
- Multi-RAT Integration & Management ✓

- D2D Communications
- Efficient Small Data Transmission
- Wireless Backhaul / Access ✓ Integration
- Flexible Networks ✓
- Flexible Mobility ✓
- Context Aware Networking
- Information Centric Networking
- Moving Networks

Types of 5G Applications

Enhanced Mobile Broadband

- Mobile Broadband, UHD / Hologram, High-mobility, Virtual Presence

Critical Communications

- Interactive Game / Sports, Industrial Control, Drone / Robot / Vehicle, Emergency

Massive Machine Type Communications

- Subway / Stadium Service, eHealth, Wearables, Inventory Control

Network Operation

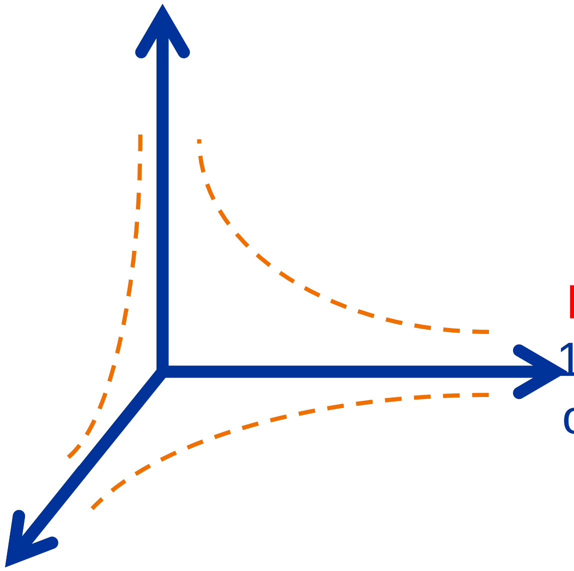
- Network Slicing, Routing, Migration and Interworking, Energy Saving

Enhancement of Vehicle-to-Everything

- Autonomous Driving, safety and non-safety features

Speed: >10 Gb/s ➔ Tb/s

Massive Content



Massive Sensing

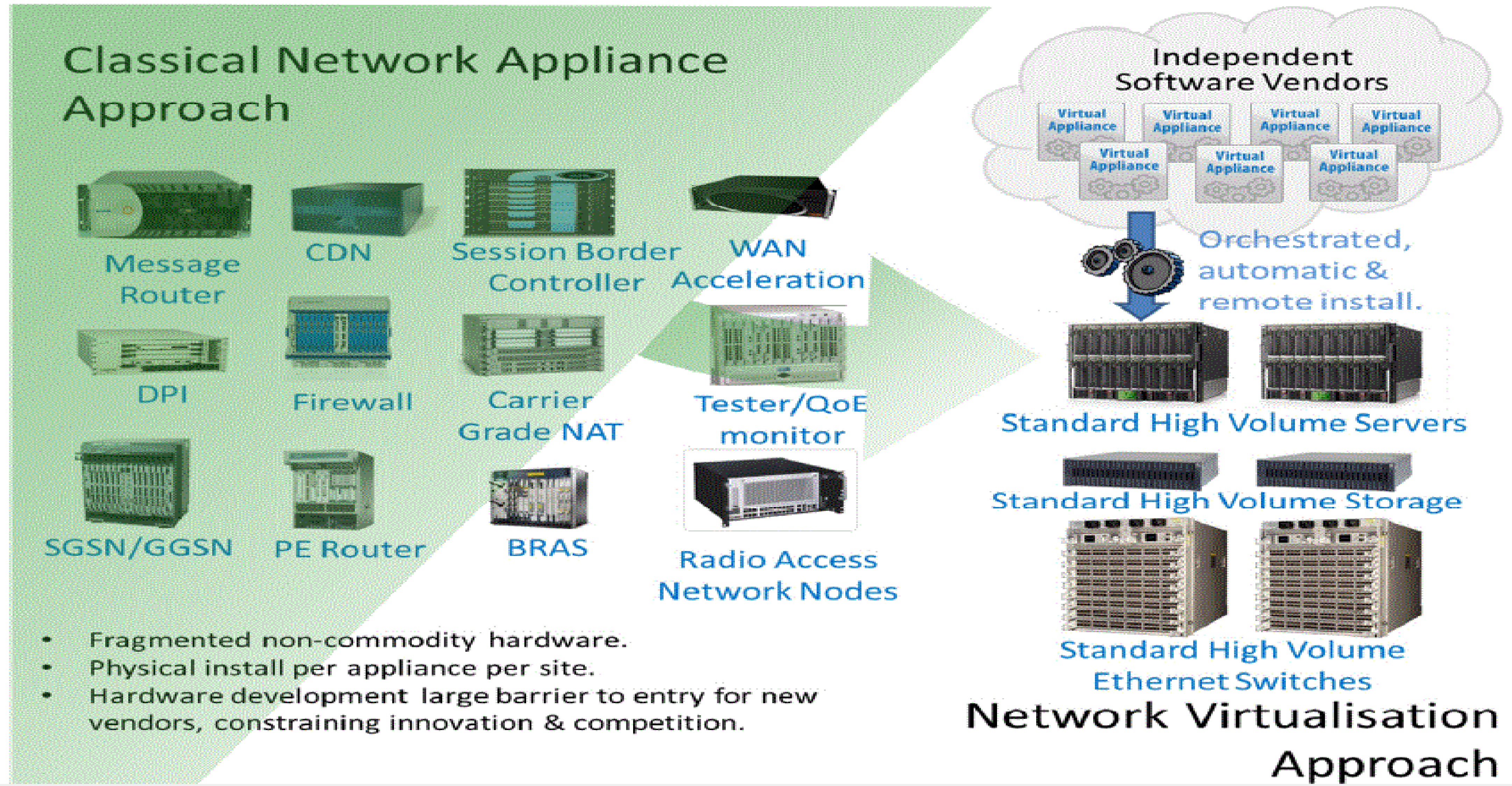
1b/s over 10 years off an AAA battery

Massive Control

Response: 1 ms

Courtesy: Gerhard Fettweis

ETSI/NFV Vision for Network Function Virtualization

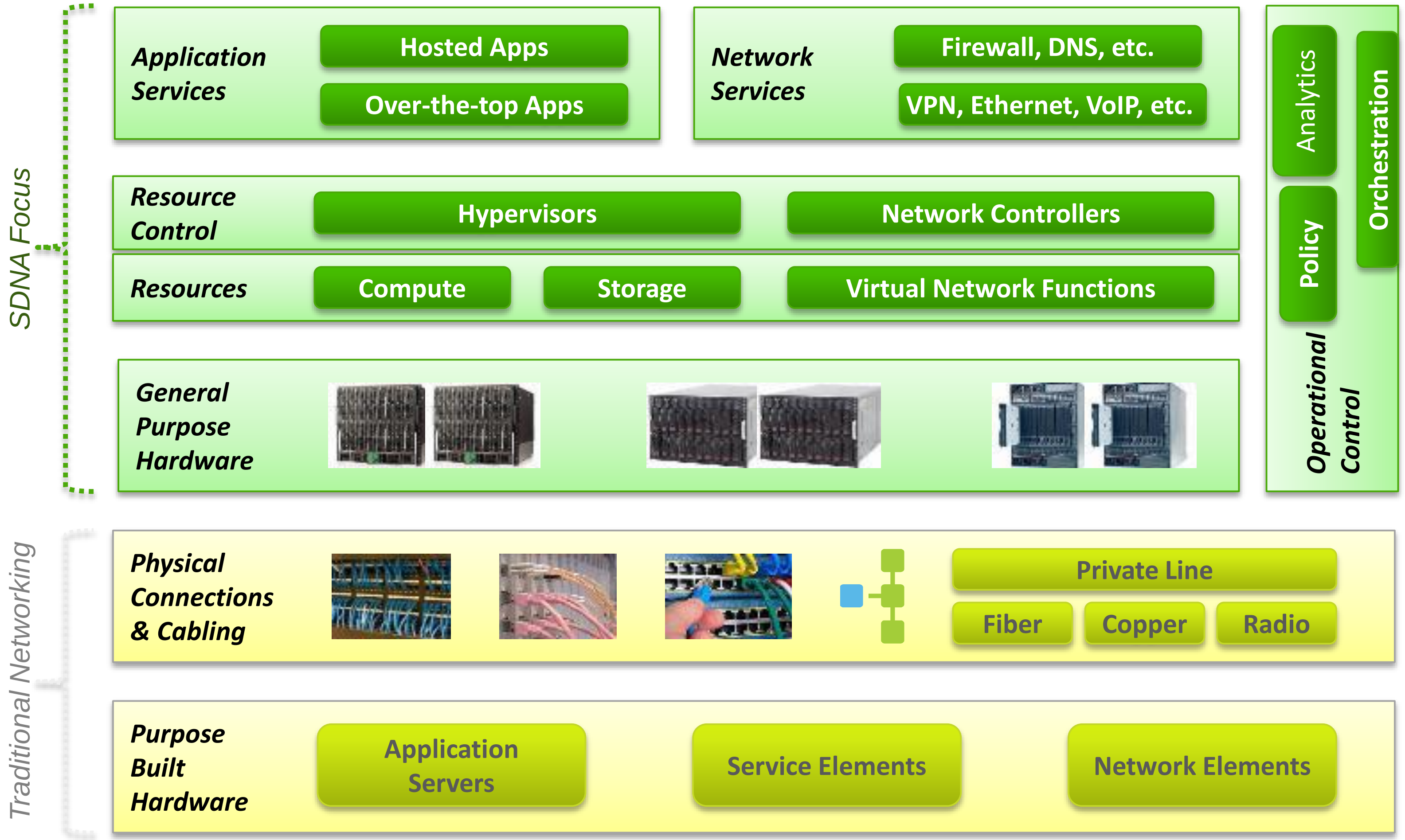


Classical Network Appliance Approach

- Fragmented non-commodity hardware.
- Physical install per appliance per site.
- Hardware development large barrier to entry for new vendors, constraining innovation & competition.

Network Virtualisation Approach

Traditional Network vs. Virtualized Network



SDNA Focus

Application Services: Hosted Apps; Over-the-top Apps

Network Services: Firewall, DNS, etc.; VPN, Ethernet, VoIP, etc.

Resource Control: Hypervisors; Network Controllers

Resources: Compute; Storage; Virtual Network Functions

General Purpose Hardware

Analytics

Policy

Orchestration

Operational Control

Traditional Networking

Physical Connections & Cabling: Private Line; Fiber; Copper; Radio

Purpose Built Hardware: Application Servers; Service Elements; Network Elements

Virtualized Networks

- General purpose cloud-based hardware components
- Software-based virtual network components and services
- Dynamic real-time configuration to support internal or customer activity
- Programmable network management
  - Software Defined Network controls
  - Real-time analytics and policy driven orchestration of service, network and capacity requests

Traditional Networks

- Built using purpose-built hardware coupled with physical connectivity
- Control logic largely coordinated and implemented by layers of OSSs
- Control, Forward and Data Planes are tightly integrated in Network Elements
  - OA&M, inventory views and operational controls managed in OSSs to avoid negative impact to service performance

The Network of the Future

A Cloud-Based Architecture

Faster

- Faster provisioning and time-to-market
- Effortless customer experience

Lower Cost

- Reduced cost of hardware, operations, etc.
- Higher utilization

Scalable

- Create new products, services quicker than before
- Add services on-demand and in near real-time

Secure

- Strong authentication
- Firewalls, proxies, deep packet inspection, etc.

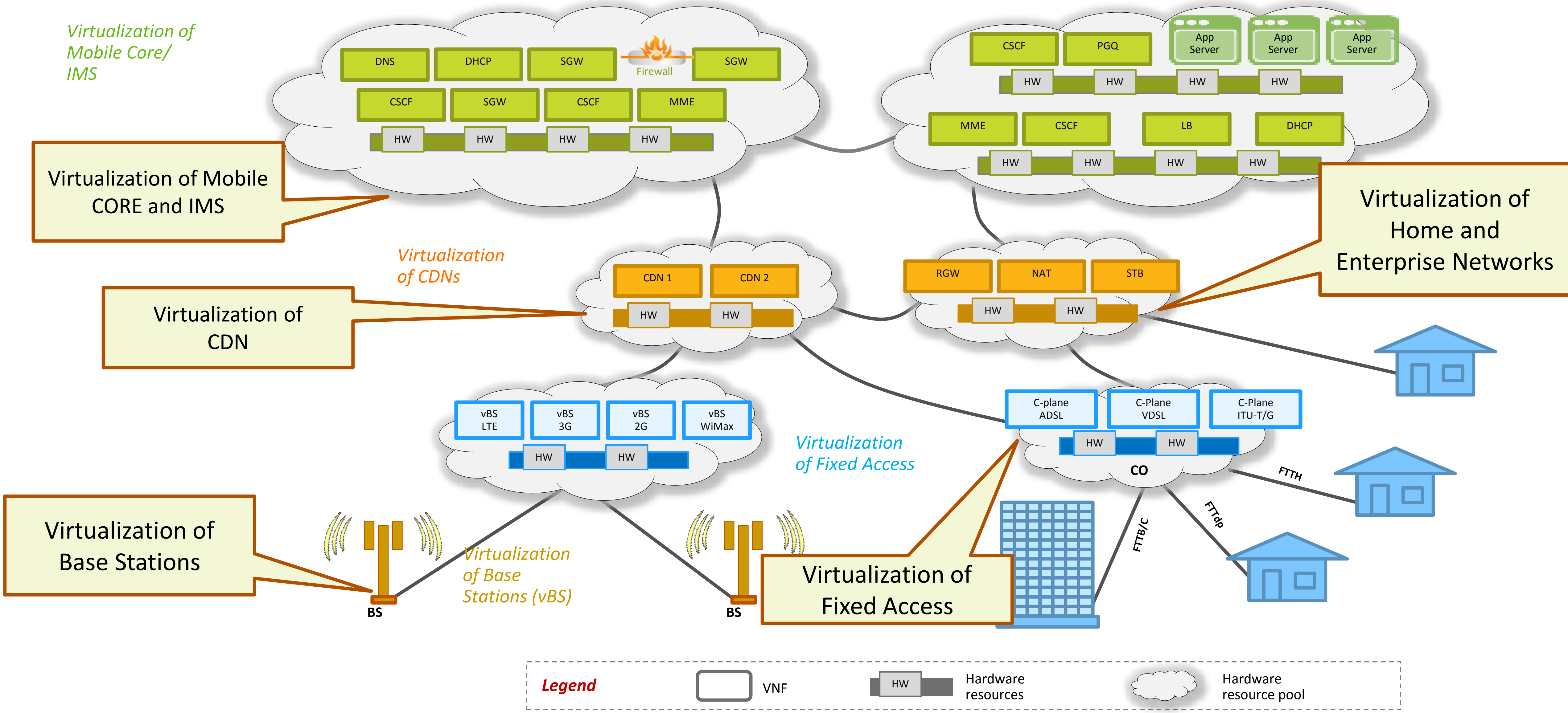
Dynamic

- Network on-demand, increased reliability, flexibility
- Analytics "big data"

Accessible

- Always connected world
- COU, BYOD, next-gen app

Overview of NFV (Network Function Virtualization) Sample Use cases



Virtualization of Mobile CORE and IMS

Virtualization of CDN

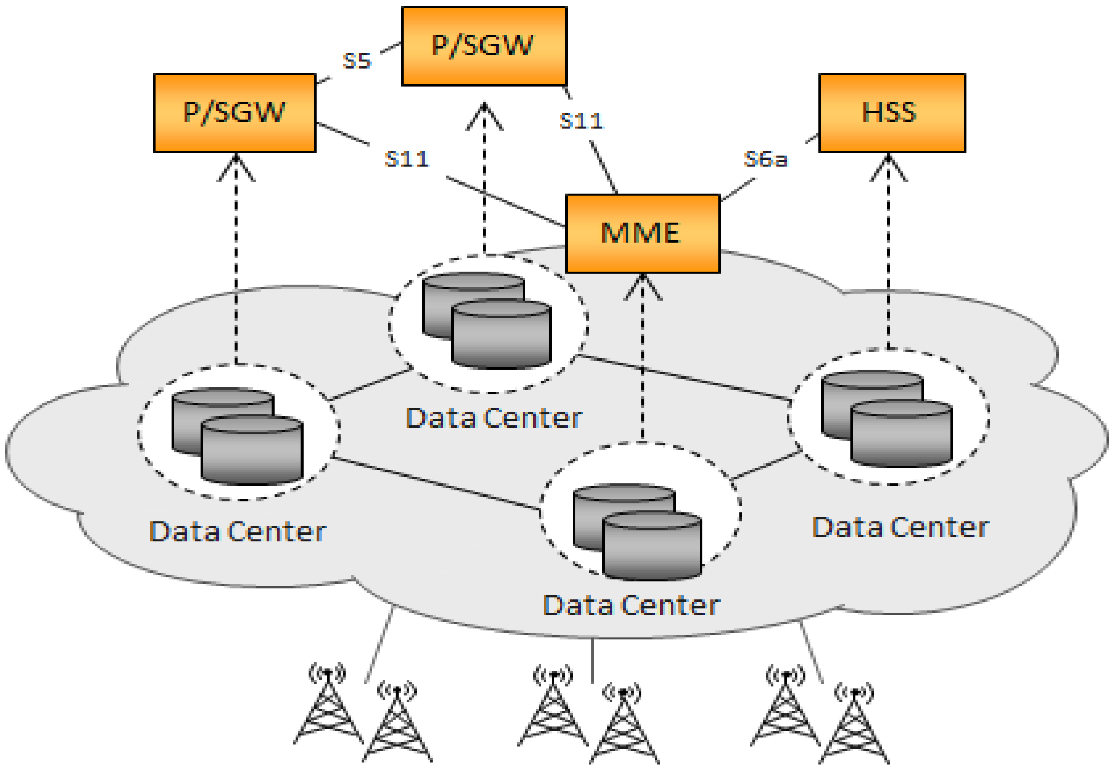
Virtualization of Base Stations

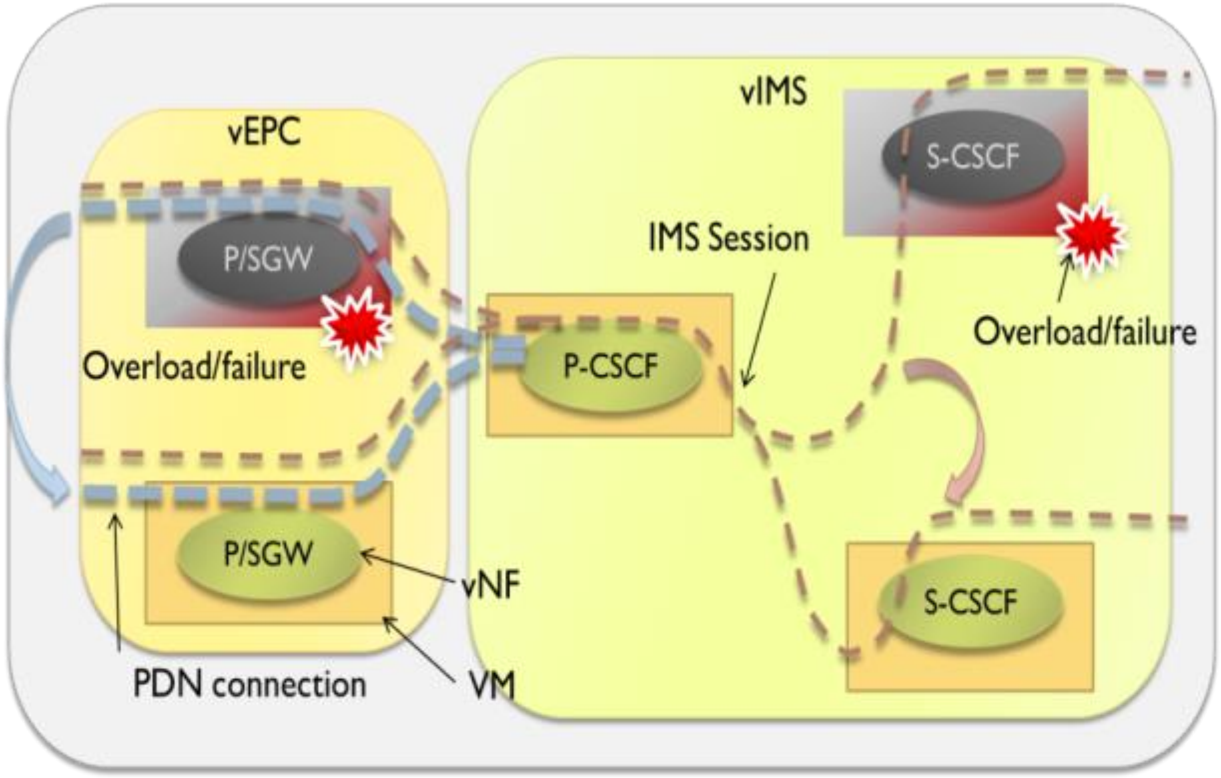
Virtualization of Fixed Access

Virtualization of Home and Enterprise Networks

NFV Use Case: Virtualization of Mobile Core Network (EPC) and IMS

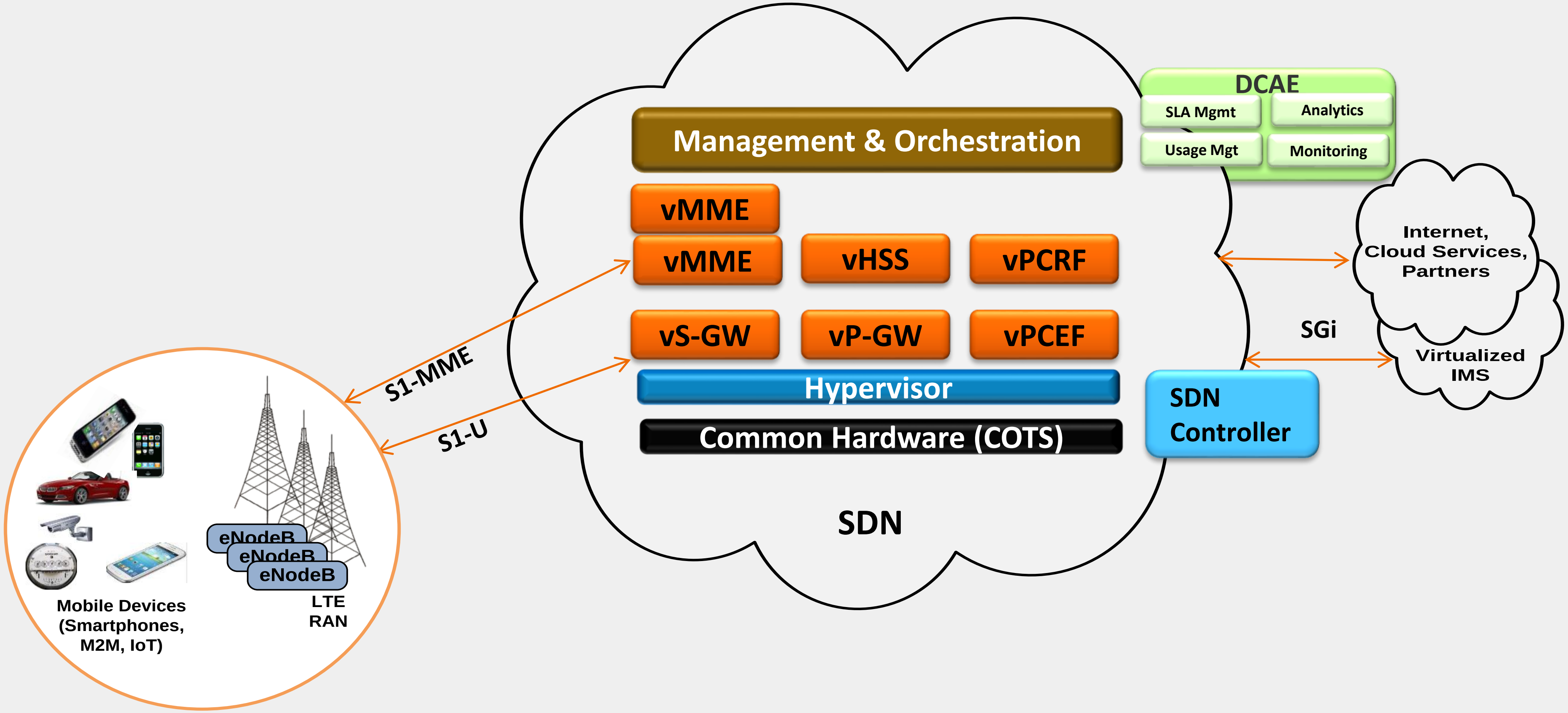
Network Operation





VNF Relocation

SDN/NFV-based Evolved Packet Core

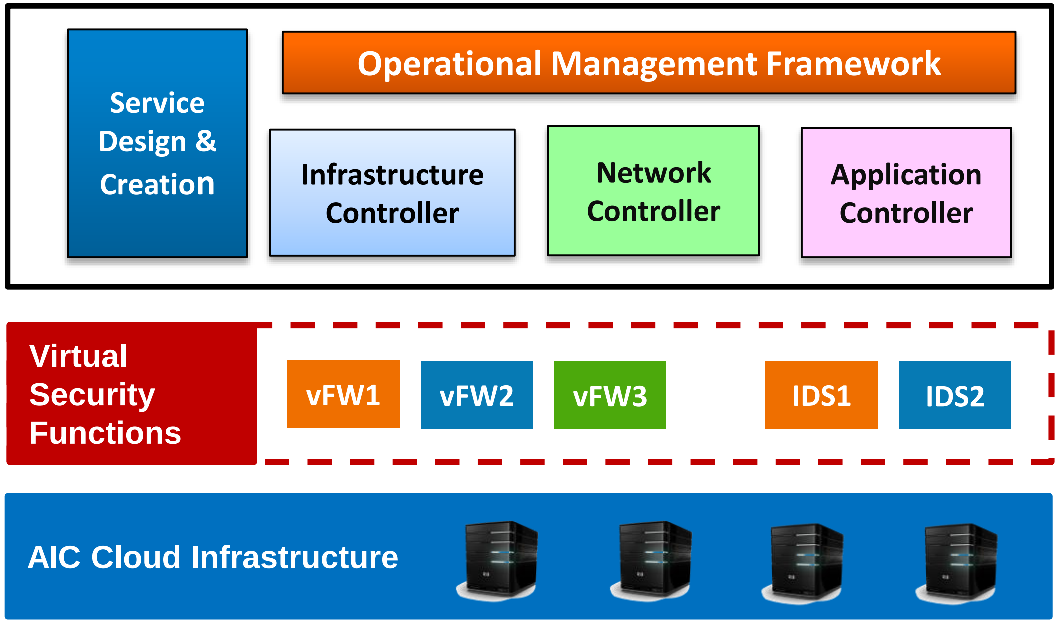


Security Transformation – Virtual Firewall an Example

Non-Virtualized Security

- Wide variety of vendor specific security hardware
- Requires vendor specific FW management platforms
- Requires hands-on customized physical work to install
- Multiple support organizations
- No single operations model or database of record

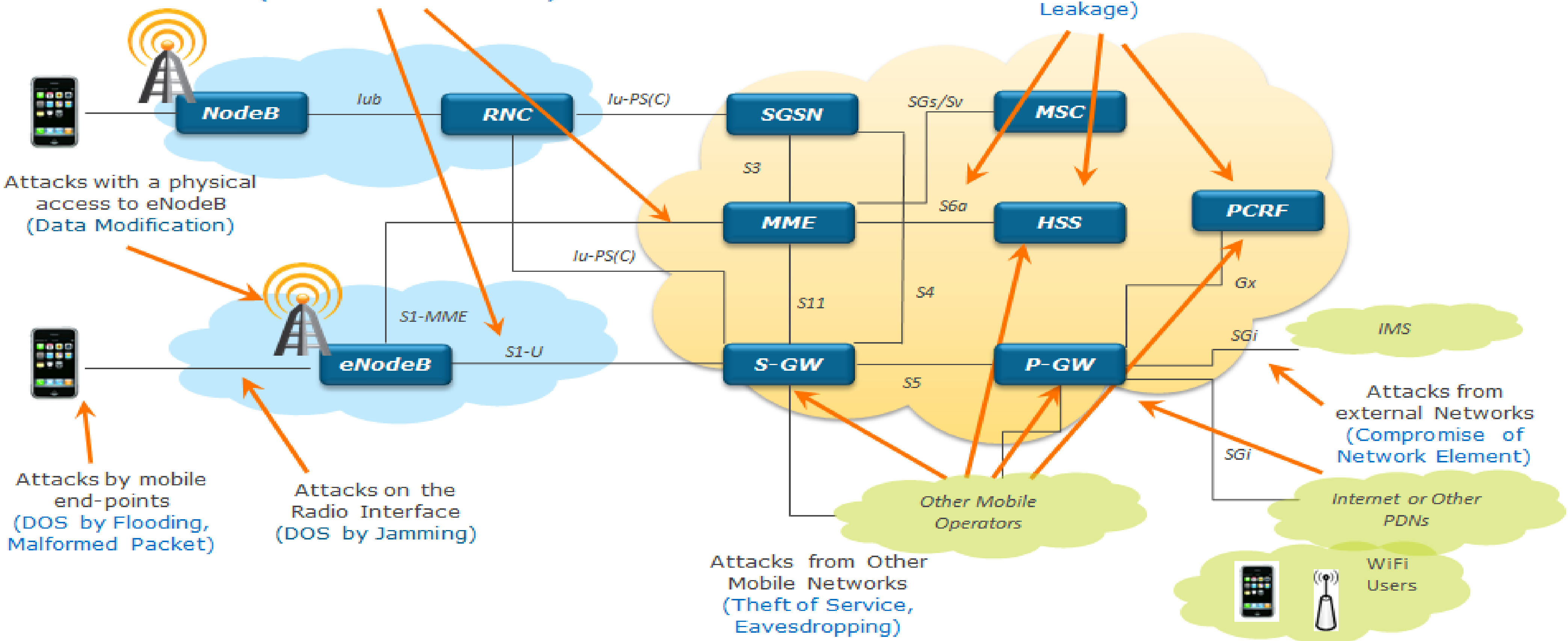
Domain 2.0 Security


Service Design & Creation
Operational Management Framework
Infrastructure Controller
Network Controller
Application Controller
Virtual Security Functions
vFW1
vFW2
vFW3
IDS1
IDS2
AIC Cloud Infrastructure

- Security functions will be cloud-based
- Security dynamically orchestrated in the cloud as needed
- Streamlined supplier integration using D2 catalog
- Centralized common management platform
- Creates a standard operations/support model

General Threat Taxonomy (EPC)

LTE/EPC Security Threats Categories



Attacks with physical access to transport network (Man-in the Middle Attack)

Insider attacks (Data Modification, Data Leakage)

Attacks with a physical access to eNodeB (Data Modification)

Attacks by mobile end-points (DOS by Flooding, Malformed Packet)

Attacks on the Radio Interface (DOS by Jamming)

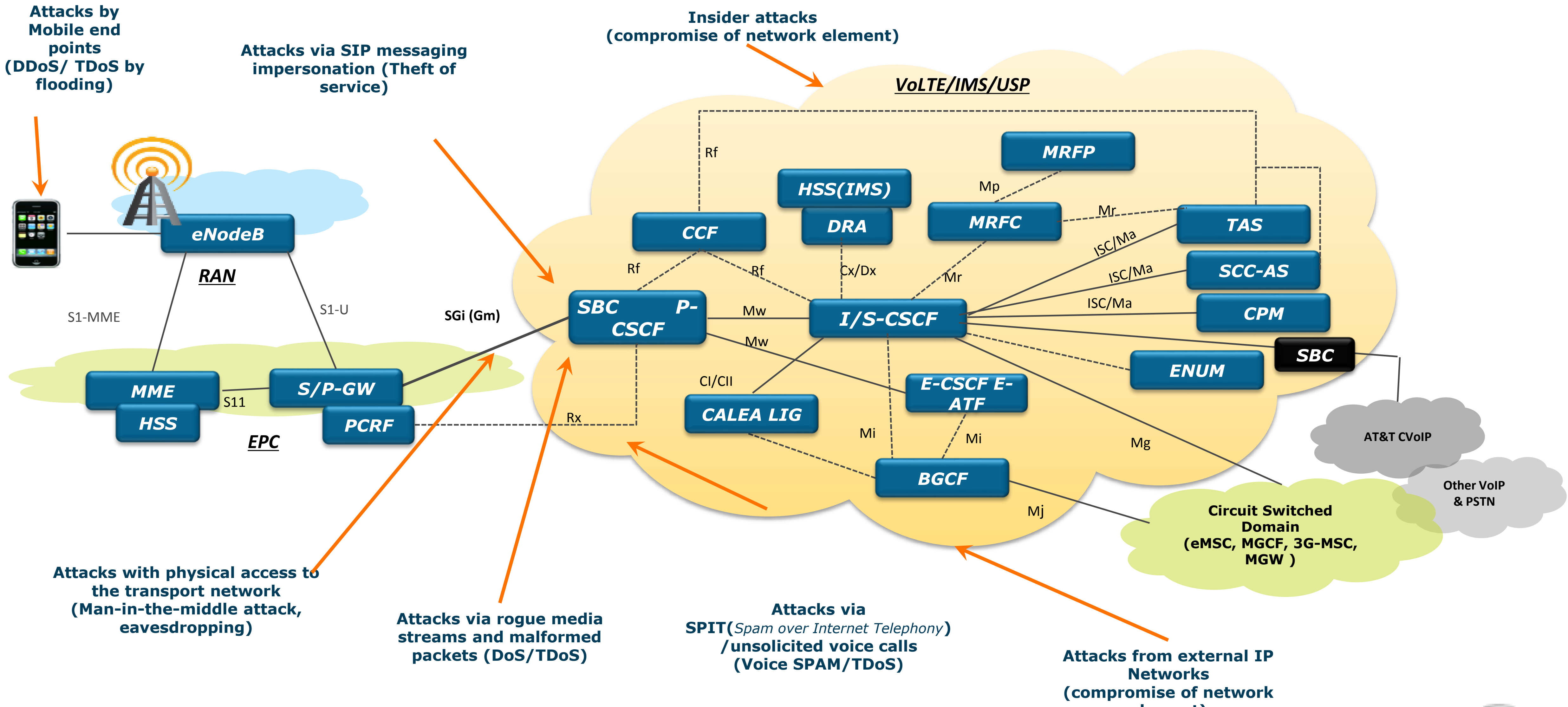
Attacks from Other Mobile Networks (Theft of Service, Eavesdropping)

Attacks from external Networks (Compromise of Network Element)

Mobile Network Security - EPC
Threat Categories

	Category	Threat	Description
T1	Loss of Availability	Flooding an interface	Attackers flood an interface resulting in DoS condition (e.g. multiple authentication failure on s6a, DNS lookup)
T2		Crashing a network element	Attackers crash a network element by sending malformed packets
T3	Loss of Confidentiality	Eavesdropping	Attackers eavesdrop on sensitive data on control and bearer plan
T4		Data leakage	Unauthorized access to sensitive data on the server (HSS profile, etc.)
T5	Loss of Integrity	Traffic modification	Attackers modify information during transit (DNS redirection, etc.)
T6		Data modification	Attackers modify data on network element (change the NE configurations)
T7	Loss of Control	Control the network	Attackers control the network via protocol or implementation flaw
T8		Compromise of network element	Attackers compromise of network element via management interface
T9	Malicious Insider	Insider attacks	Insiders make data modification on network elements, make unauthorized changes to NE configuration, etc.
T10	Theft of Service	Service free of charge	Attackers exploits a flaw to use services without being charged

Attacks Taxonomy – VoLTE/IMS/USP



Attacks by Mobile end points (DDoS/ TDoS by flooding)

Attacks via SIP messaging impersonation (Theft of service)

Insider attacks (compromise of network element)

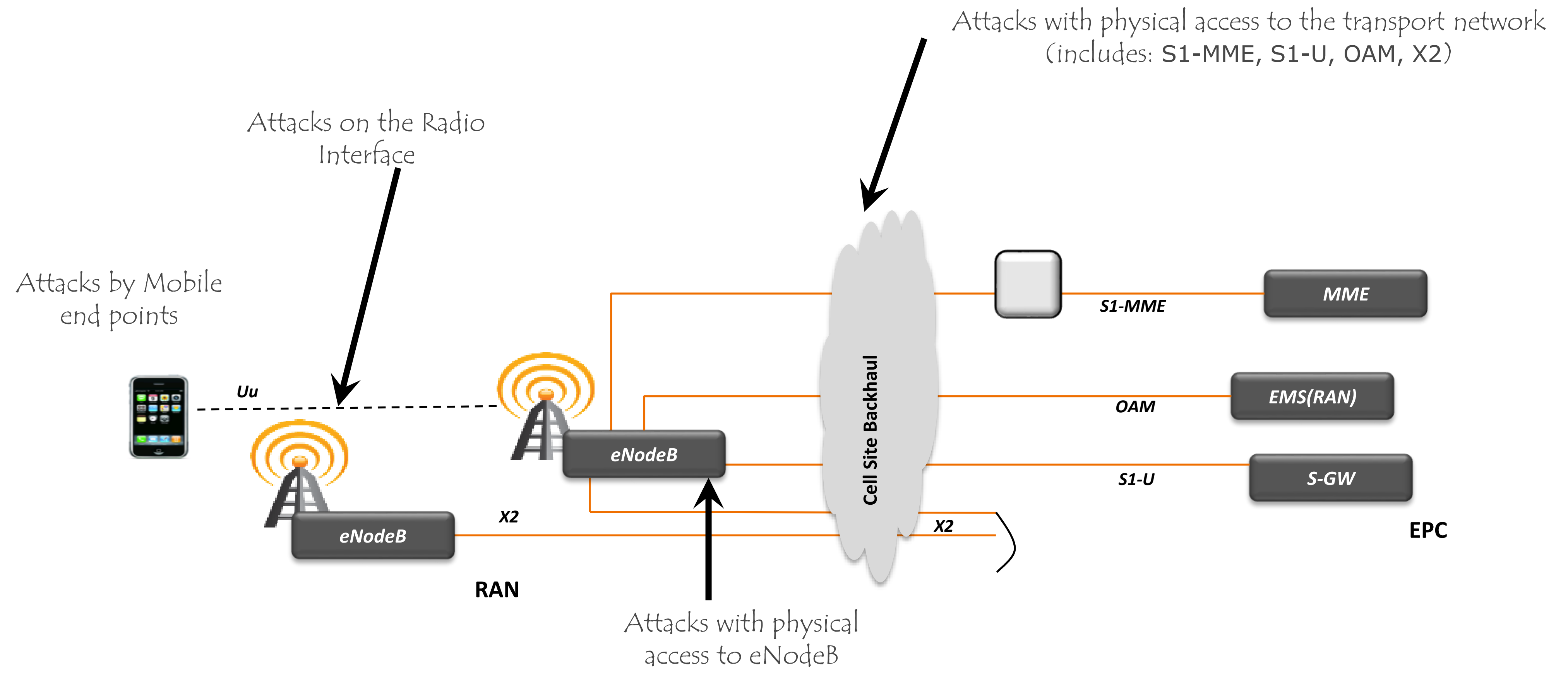
Attacks with physical access to the transport network (Man-in-the-middle attack, eavesdropping)

Attacks via rogue media streams and malformed packets (DoS/TDoS)

Attacks via SPIT(*Spam over Internet Telephony*) /unsolicited voice calls (Voice SPAM/TDoS)

Attacks from external IP Networks (compromise of network element)

Attacks on LTE-RAN


Attacks with physical access to the transport network
(includes: S1-MME, S1-U, OAM, X2)
Attacks on the Radio Interface
Attacks by Mobile end points
Uu
eNodeB
eNodeB
X2
RAN
Cell Site Backhaul
S1-MME
MME
OAM
EMS(RAN)
S1-U
S-GW
X2
EPC
Attacks with physical access to eNodeB

What are the Security Impacts?

Security Benefits of a Cloud-Based Architecture

Network Simplification & Automation	Network is less vulnerable to security threats, consistent policy configuration, automated quarantine
Flexibility & Scalability	Improved incident response, DDoS resiliency, block/reroute of malicious traffic
Multi-vendor Implementation	Eliminate single point of failure, Security Function Virtualization, Security as a service

What are the Security Implications?

Security Challenges of a Cloud-Based Architecture

Common Cloud Infrastructure	▶	Hypervisor vulnerabilities, VM/Guest OS manipulation, Data exfiltration/destruction
Software Enabled Automated Provisioning	▶	Orchestration vulnerabilities, Automated network configuration exploits, Malicious misconfiguration, SDN controller exploits
Flexibility & Elasticity	▶	Amplification of attacks due to elasticity

Security Advantages of SDN/NFV

A Comprehensive View of SDN/NFV Security Advantages

Performance Improvements:

Streamline and Reduce Incident Response Cycle Time

Streamline and Reduce Patching Cycle Time

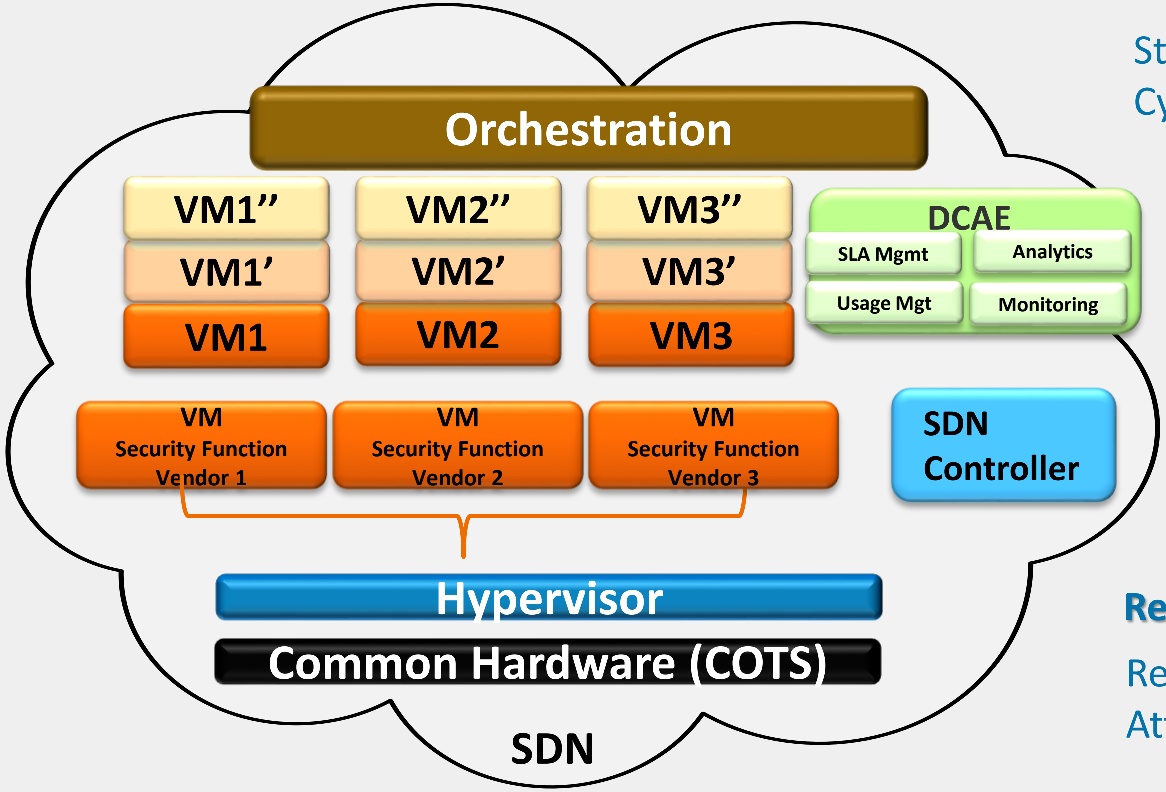
Design Enhancements:

Centralize Control and Management Functions

Security Embedded at Design Time

Security that Exceeds Existing Perimeter

Multivendor Security Service



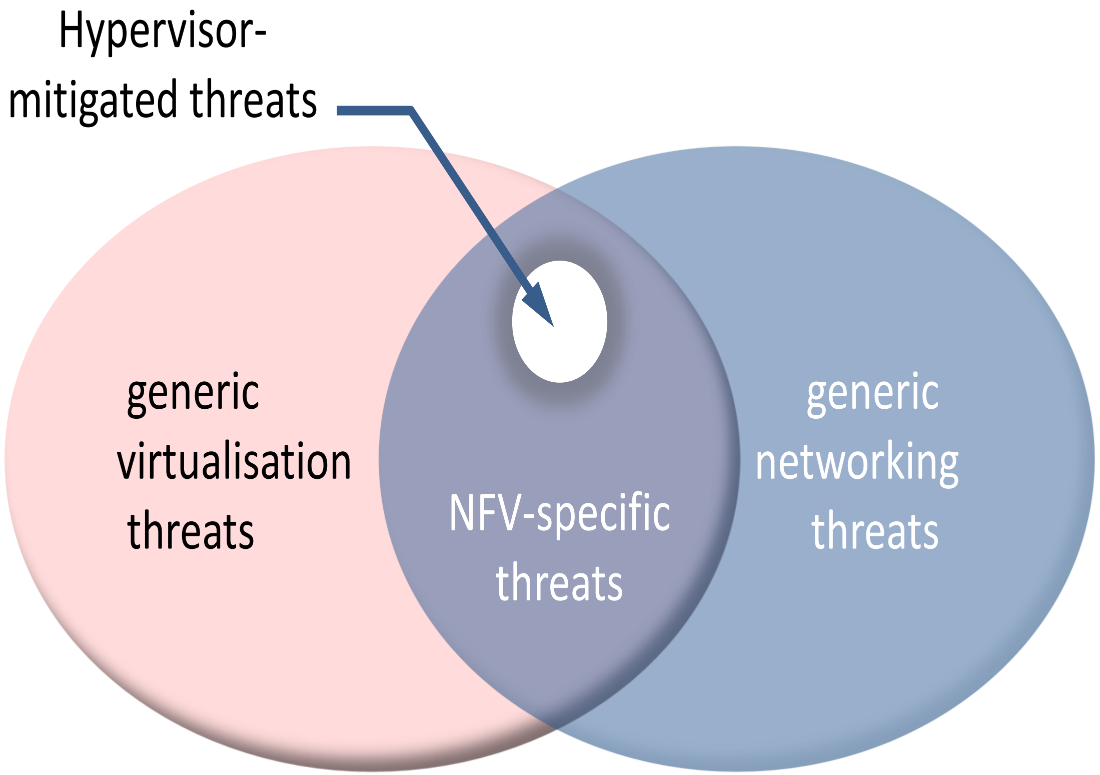
Real-Time capabilities:

Real-Time Scaling to Absorb DDOS Attacks

Real-Time Integration of "Add-on" Security Functions

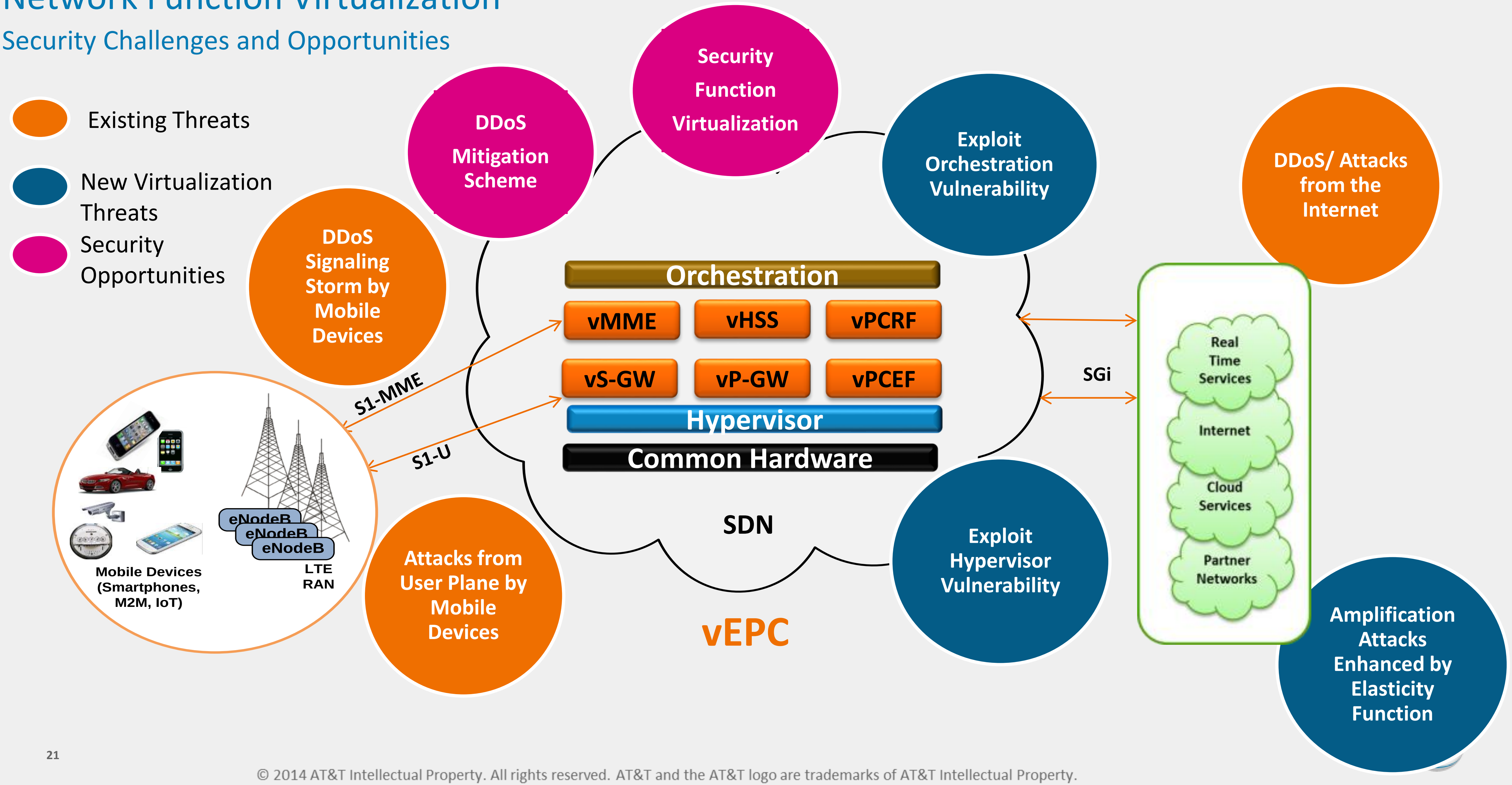
Security Challenges in a Virtual Environment – ETSI Problem Statement Draft

- Hypervisor Vulnerability
- API security
- Orchestration Vulnerability
- Virtual monitoring
  - Limited visibility to Mobility/EPC interfaces (e.g. S6a, S11, S8)
- Virtualized firewalls
- 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
- Security monitoring across multiple administrative domains (i.e., Lawful Interception)


Hypervisor-mitigated threats
generic virtualisation threats
NFV-specific threats
generic networking threats

Network Function Virtualization

Security Challenges and Opportunities


● Existing Threats
● New Virtualization Threats
● Security Opportunities
DDoS Mitigation Scheme
Security Function Virtualization
Exploit Orchestration Vulnerability
DDoS/ Attacks from the Internet
DDoS Signaling Storm by Mobile Devices
Orchestration
vMME
vHSS
vPCRF
vS-GW
vP-GW
vPCEF
Hypervisor
Common Hardware
SDN
vEPC
S1-MME
S1-U
SGi
Real Time Services
Internet
Cloud Services
Partner Networks
eNodeB
eNodeB
eNodeB
LTE RAN
Mobile Devices (Smartphones, M2M, IoT)
Attacks from User Plane by Mobile Devices
Exploit Hypervisor Vulnerability
Amplification Attacks Enhanced by Elasticity Function

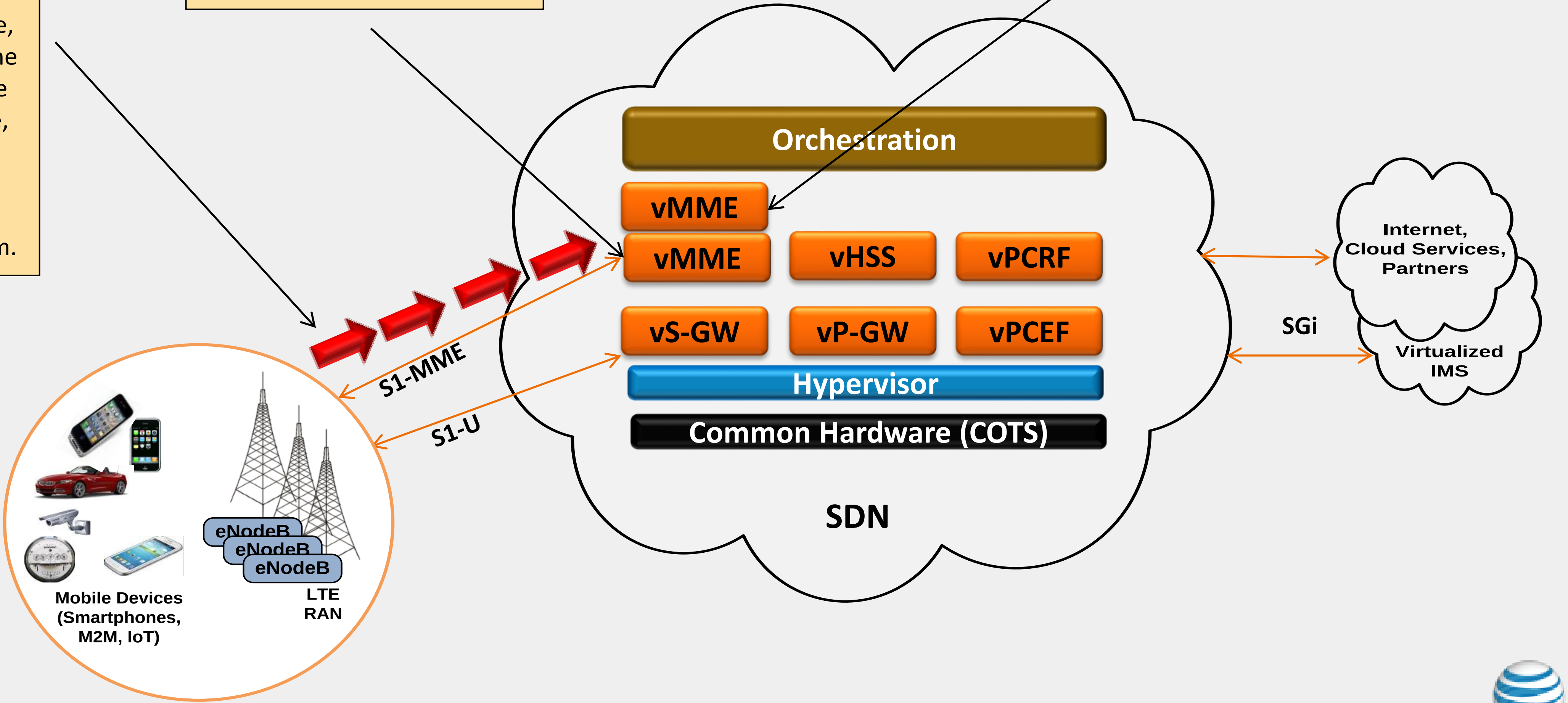
Security Opportunities from Virtualization

DDoS Attack Resiliency

1 Attacker creates a Botnet army by infecting many Mobile devices with a ‘remote-reboot’ malware, attacker then instructs the malware to reboot all the devices at the same time, this will cause excessive malicious Attach Requests, creating a Malicious Signaling Storm.

2 vMME is under DDoS attack

3 Orchestrator instantiates new VM to scale-out vMME function to sustain the higher traffic load while we investigate.



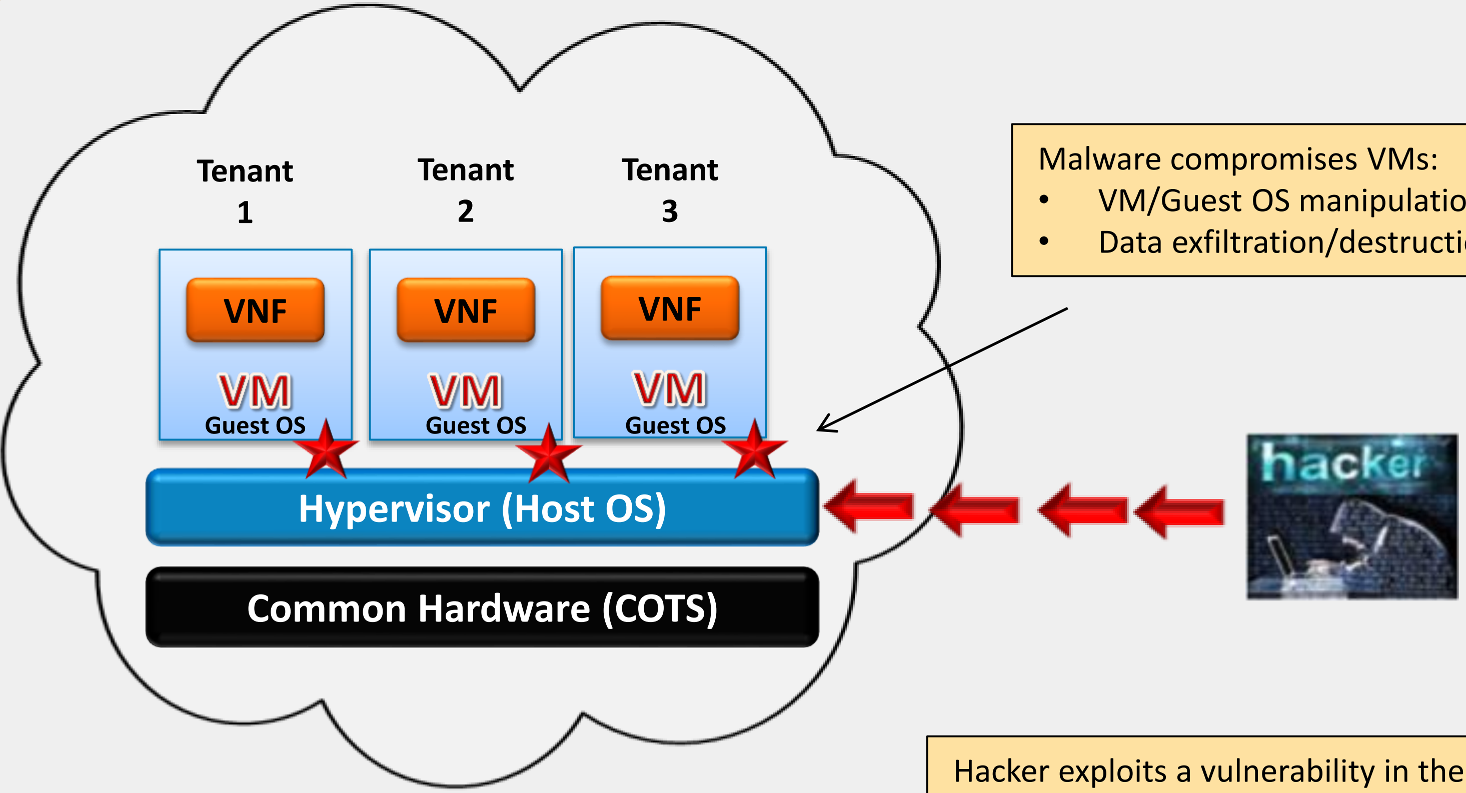
Security Challenges from Virtualization

Hypervisor Vulnerabilities

3

To prevent this type of attack, we must:

- ✓ Conduct security scans and apply security patches
- ✓ Ensure the Hypervisor is hardened and minimized (close vulnerable ports)
- ✓ Ensure the access to the Hypervisor is controlled via User Access Management,



2

Malware compromises VMs:

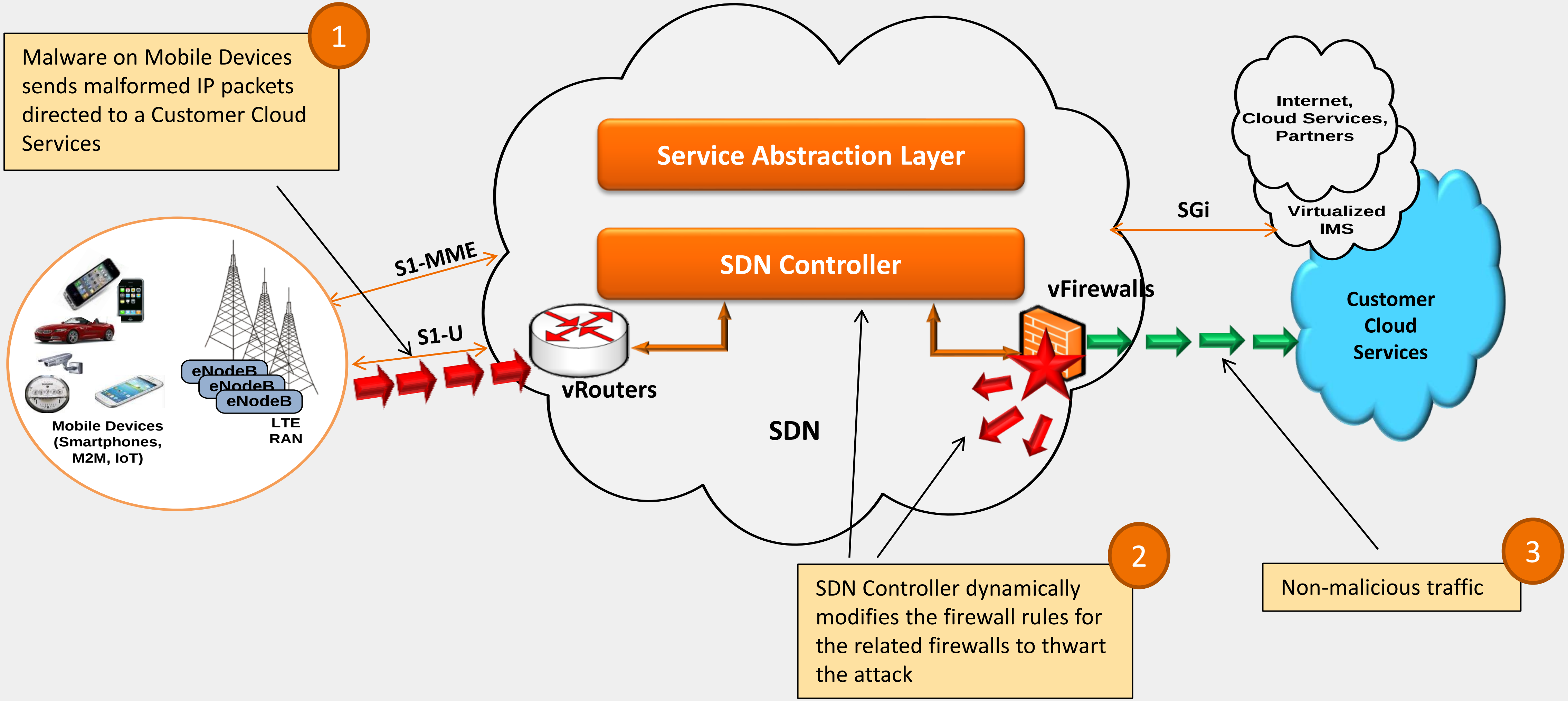
- VM/Guest OS manipulation
- Data exfiltration/destruction

1

Hacker exploits a vulnerability in the Open Source code and infects the Hypervisor with a Malware

Security Opportunities from Virtualization

SDN Controller Dynamic Security Control

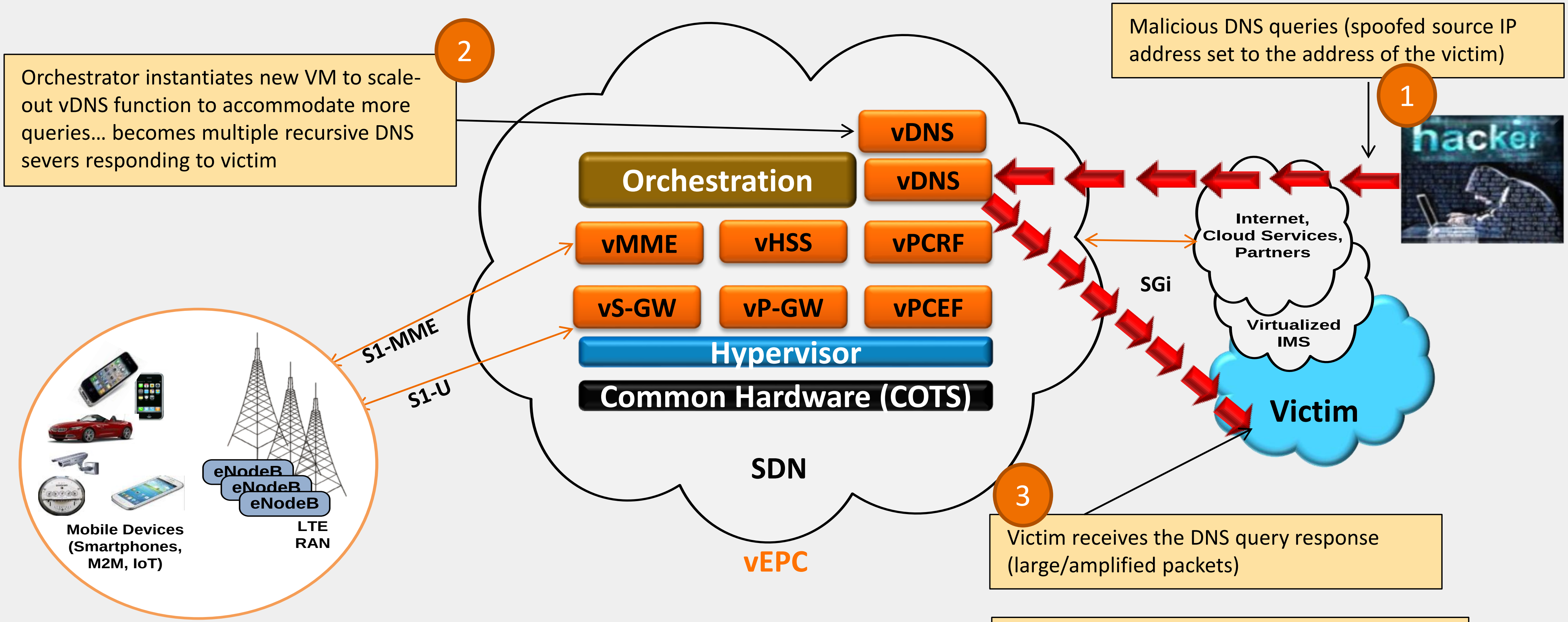


1 Malware on Mobile Devices sends malformed IP packets directed to a Customer Cloud Services

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

3 Non-malicious traffic

DNS Amplification Attacks Enhanced by Elasticity Function



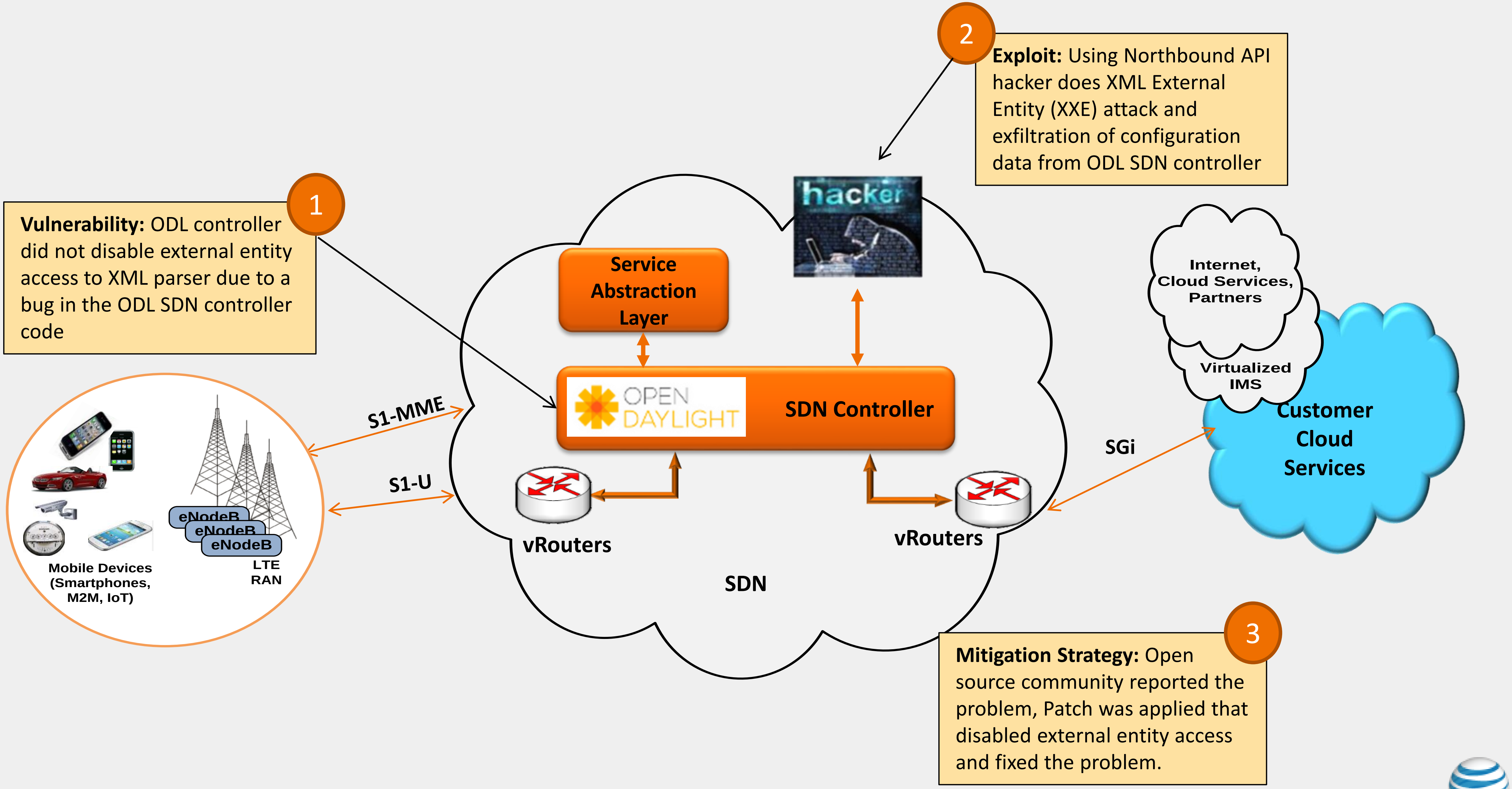
1 Malicious DNS queries (spoofed source IP address set to the address of the victim)

2 Orchestrator instantiates new VM to scale-out vDNS function to accommodate more queries… becomes multiple recursive DNS severs responding to victim

3 Victim receives the DNS query response (large/amplified packets)

NOTE: we must implement vIDS/vIPS & vFirewalls to mitigate these types of attacks

Security Vulnerability in ODL SDN Controller



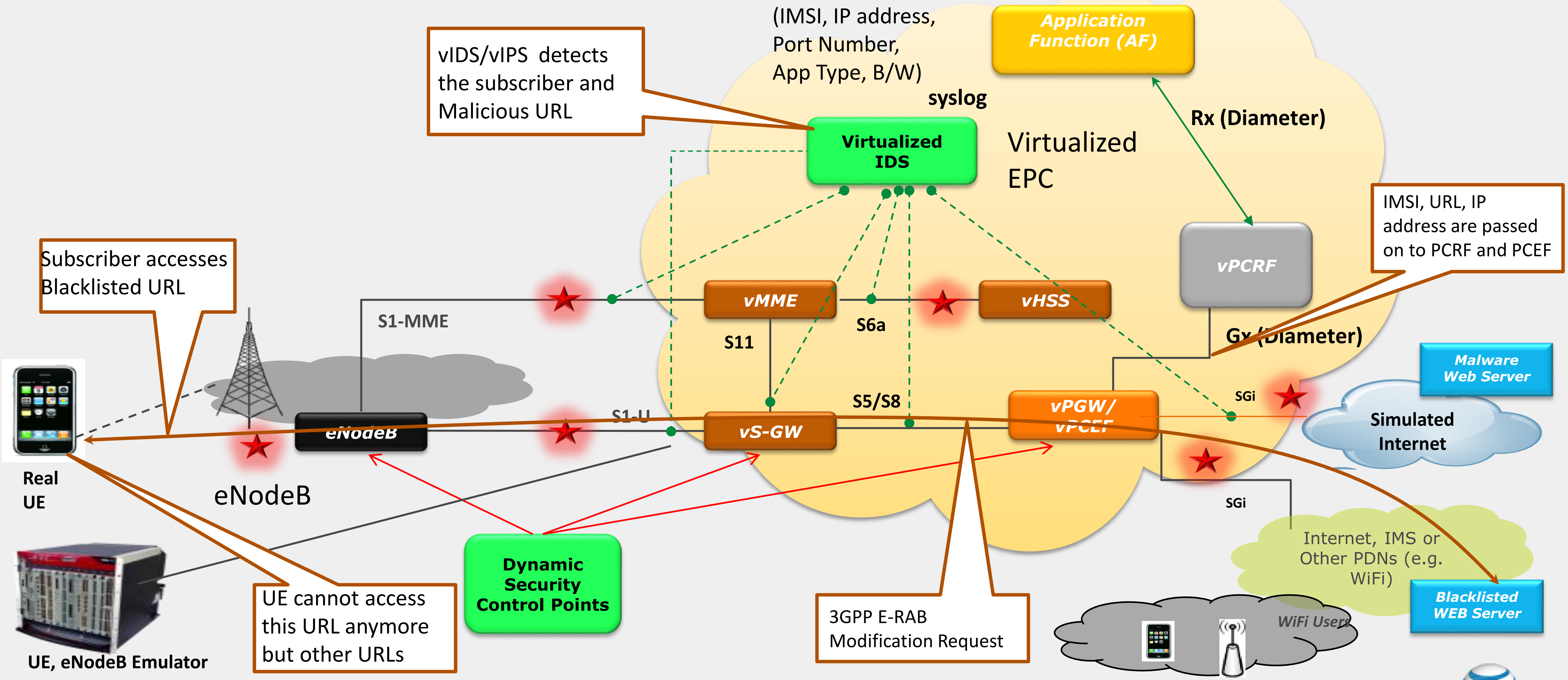
1 **Vulnerability:** ODL controller did not disable external entity access to XML parser due to a bug in the ODL SDN controller code

2 **Exploit:** Using Northbound API hacker does XML External Entity (XXE) attack and exfiltration of configuration data from ODL SDN controller

3 **Mitigation Strategy:** Open source community reported the problem, Patch was applied that disabled external entity access and fixed the problem.

Virtual IDS Prototype for Mobility CORE

1. Malicious URL Detection and Mitigation



vIDS/vIPS detects the subscriber and Malicious URL

Subscriber accesses Blacklisted URL

UE cannot access this URL anymore but other URLs

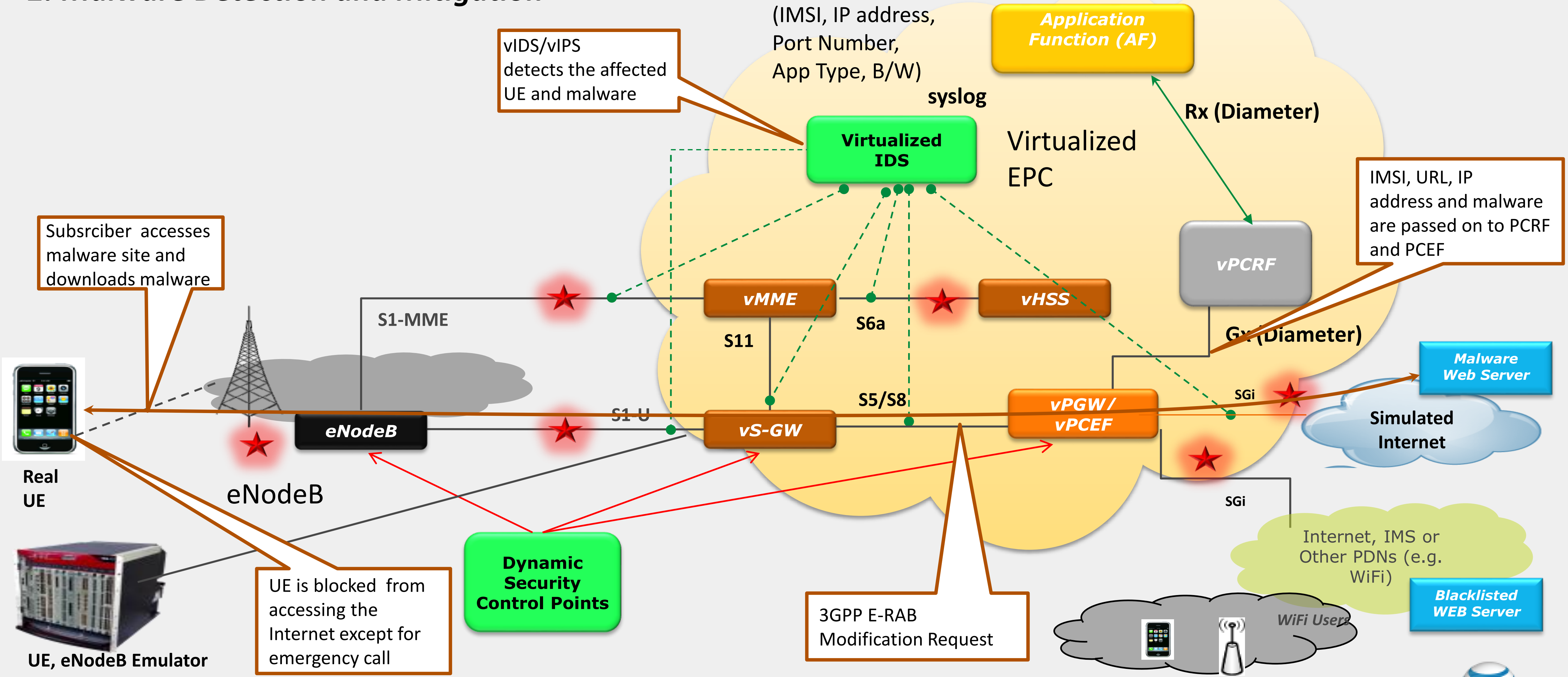
IMSI, URL, IP address are passed on to PCRF and PCEF

3GPP E-RAB Modification Request

(IMSI, IP address, Port Number, App Type, B/W)

Virtual IDS Prototype for Mobility CORE

2. Malware Detection and Mitigation



vIDS/vIPS detects the affected UE and malware

(IMSI, IP address, Port Number, App Type, B/W)

Subsrciber accesses malware site and downloads malware

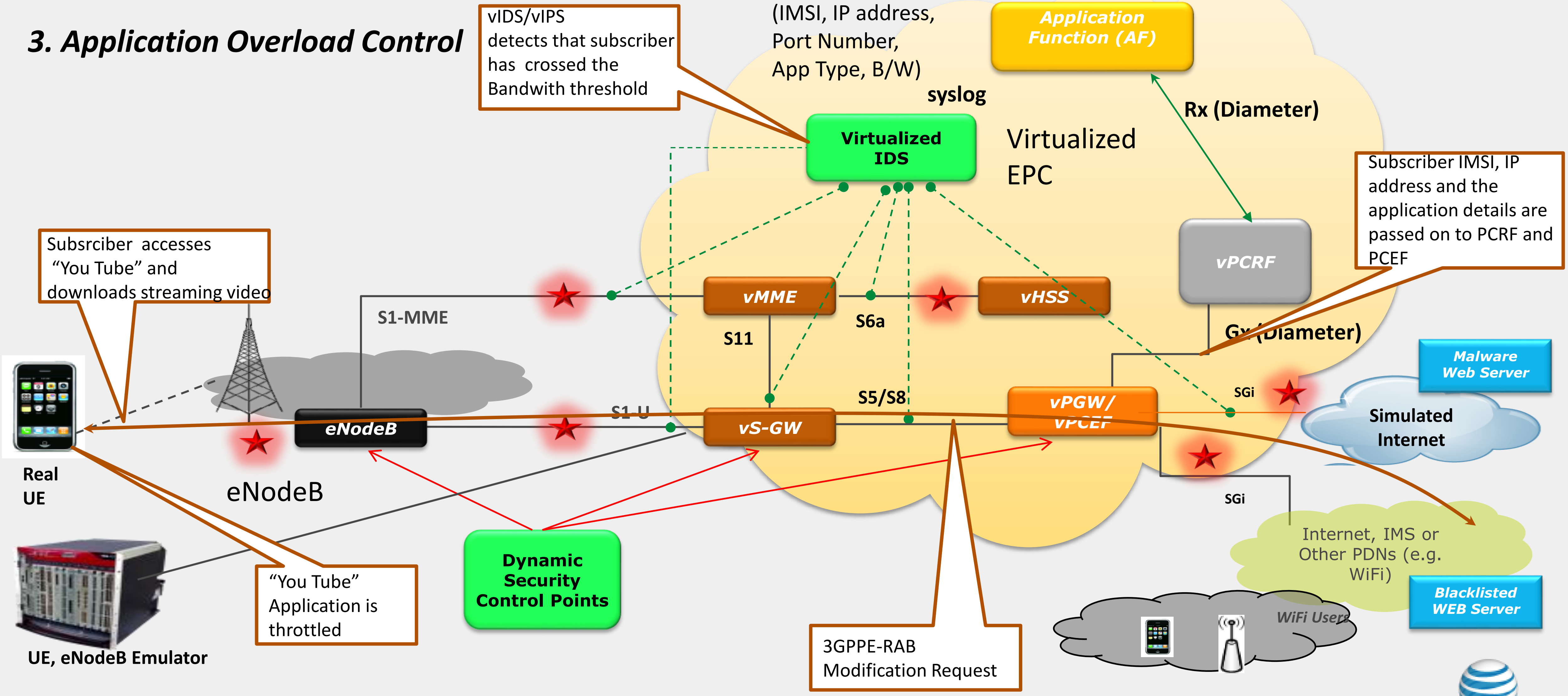
IMSI, URL, IP address and malware are passed on to PCRF and PCEF

UE is blocked from accessing the Internet except for emergency call

3GPP E-RAB Modification Request

Virtual IDS Prototype for Mobility CORE

3. Application Overload Control



vIDS/vIPS detects that subscriber has crossed the Bandwith threshold

(IMSI, IP address, Port Number, App Type, B/W)

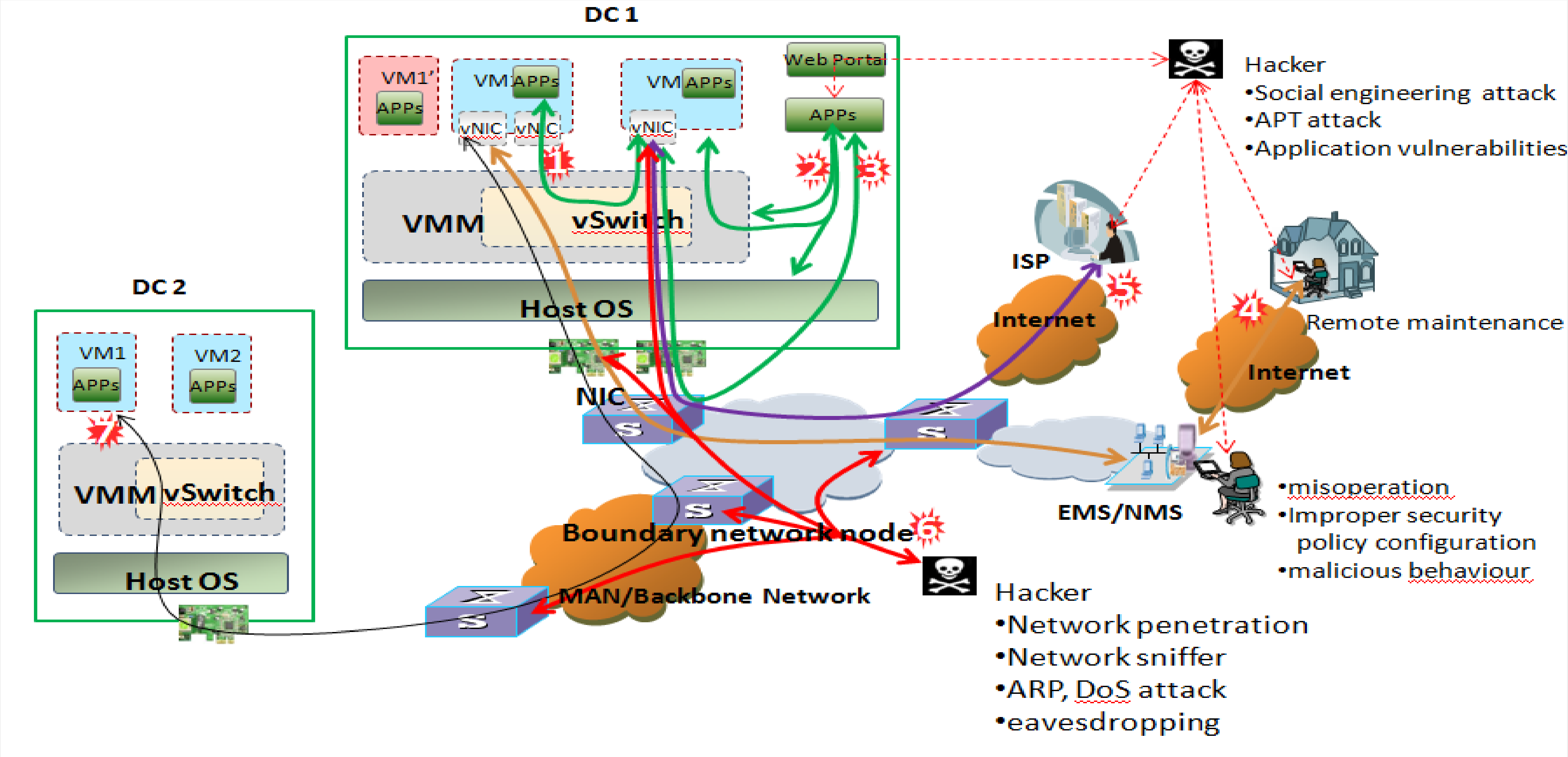
Subsrciber accesses "You Tube" and downloads streaming video

Subscriber IMSI, IP address and the application details are passed on to PCRF and PCEF

"You Tube" Application is throttled

3GPPE-RAB Modification Request

Threat Scenarios in NFV (Ref - ETSI NFV)



Hacker
- Social engineering attack
- APT attack
- Application vulnerabilities

- misoperation
- Improper security policy configuration
- malicious behaviour

Hacker
- Network penetration
- Network sniffer
- ARP, DoS attack
- eavesdropping

Attack Types in NFV (Ref- ETSI/NFV)

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

Attack Types in NFV (Ref-ETSI/NFV)(Contd.)

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

Orchestration Vulnerability (Example)

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.

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

Security Pillars

A Comprehensive View of AT&T Domain 2.0 Security Strategy

Software Security Model

Security Function Virtualization

Industry Engagement

SDN Controller Security

Identity & Access Management

Security Analytics

Orchestration Security

Hypervisor Security

Open Source -- Implementation & Challenges

- AT&T is increasing software & Open Source usage exponentially
- Domain 2 moves from hardware to software-based systems

- Increasingly leveraging Open Source software by AT&T and industry
- Vulnerabilities include recent XML External Entity (XXE) types attack
- Need a stronger developer support program (CII)

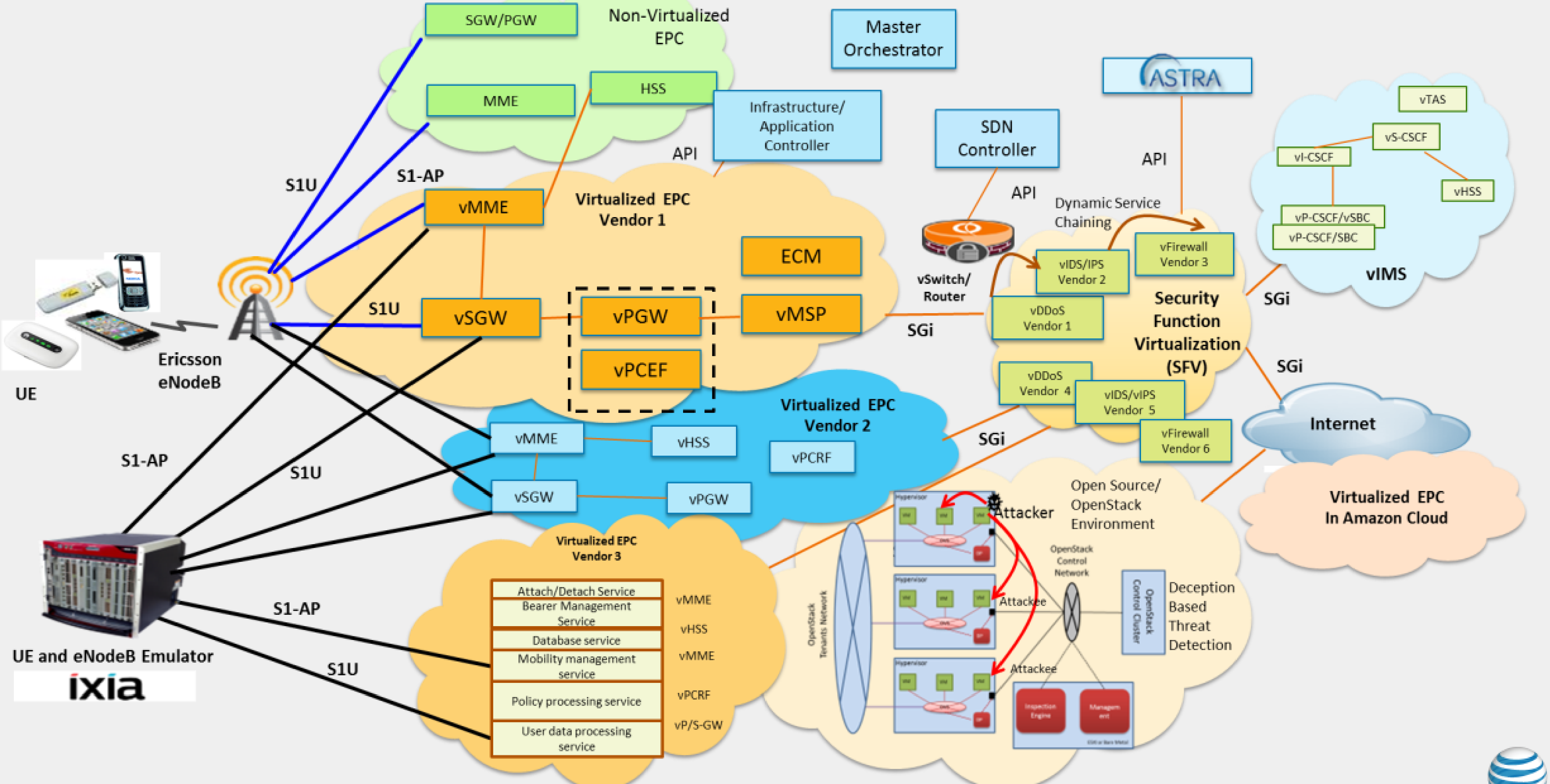
Active participation in Open Source Forums to drive security best practices

Open Source Lab to gain hands-on experience and verify the vulnerabilities and report

Work with the vendor community for

- Automated asset inventory / discovery tools
- Vulnerability correlation tools
- Software design phase security evaluation tools

Domain 2.0 Security/OpenSource Lab – Middletown, NJ



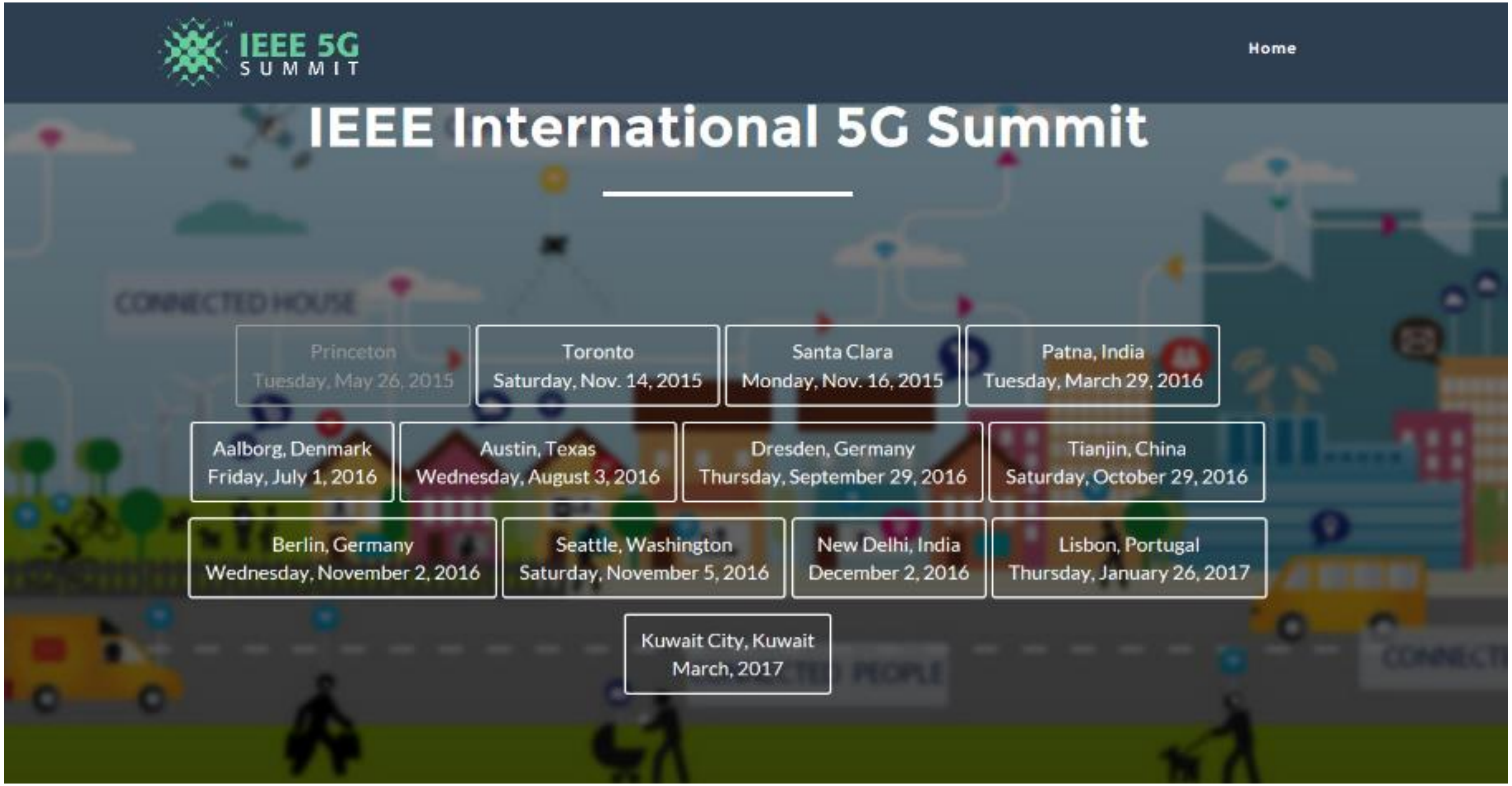
Relevant SDN/NFV Security Standards

Forum	Focus
IETF	Network Virtualization Overlay, Dynamic Service Chaining, Network Service Header
3GPP	Mobility and Security Architecture and Specification
ETSI ISG NFV ✓	NFV Platform/Deployment Standards – Security, Architecture/Interfaces, Reliability, Evolution, Performance
ONF	OpenFlow SDN Controller Standards
OPNFV	NFV Open Platform/eCOMP/OPNFV Community TestLabs
Openstack	Cloud Orchestrator Open Source
OpenDaylight	Brownfield SDN Controller Open Source
ONOS	OpenFlow SDN Controller Open Source
DPDK/ODP	CPU/NIC HW API – Data Plane Development Kit
KVM	Hypervisor
OVS	Open Source vSwitch
Linux	Operating System, Container Security
ATIS/NIST/FCC/CSA	Regulatory Aspects of SDN/NFV

ETSI/NFV Security Expert Group work Items

Work Items	Scope
NFV Security Problem Statement Document	Identifies and proposes solutions to any new vulnerabilities that result from the introduction of NFV
Security and Trust Guidance	Describes the security and trust guidance that is unique to NFV development, architecture and operation
Cataloguing Security Features in Management Software	Catalogue security features in management software relevant to NFV - OpenStack as the first case study.
Lawful Interception Implications	Identify the security and architecture pre-conditions for the provision of LI in an NVF based network
Certificate Management	Looks at various certificate deployment scenarios and describe certificate specific use cases
Report on Security Aspects and Regulatory Concerns	Addresses the security aspects and regulatory concerns of NFV related documents and applications
Report on Attestation Technologies and Practices for Secure Deployments	Identifies gaps in existing attestation technologies and practice
Security Monitoring – Report on Use Cases and Requirements	Investigate the security monitoring requirements and deployment use cases in an NFV environment
Use cases for multi-layer host administration	Addresses provision of multi-layer administration issues within a single host.

Galaxy of 5G Summit Series



IEEE International 5G Summit

Princeton
Tuesday, May 26, 2015

Toronto
Saturday, Nov. 14, 2015

Santa Clara
Monday, Nov. 16, 2015

Patna, India
Tuesday, March 29, 2016

Aalborg, Denmark
Friday, July 1, 2016

Austin, Texas
Wednesday, August 3, 2016

Dresden, Germany
Thursday, September 29, 2016

Tianjin, China
Saturday, October 29, 2016

Berlin, Germany
Wednesday, November 2, 2016

Seattle, Washington
Saturday, November 5, 2016

New Delhi, India
December 2, 2016

Lisbon, Portugal
Thursday, January 26, 2017

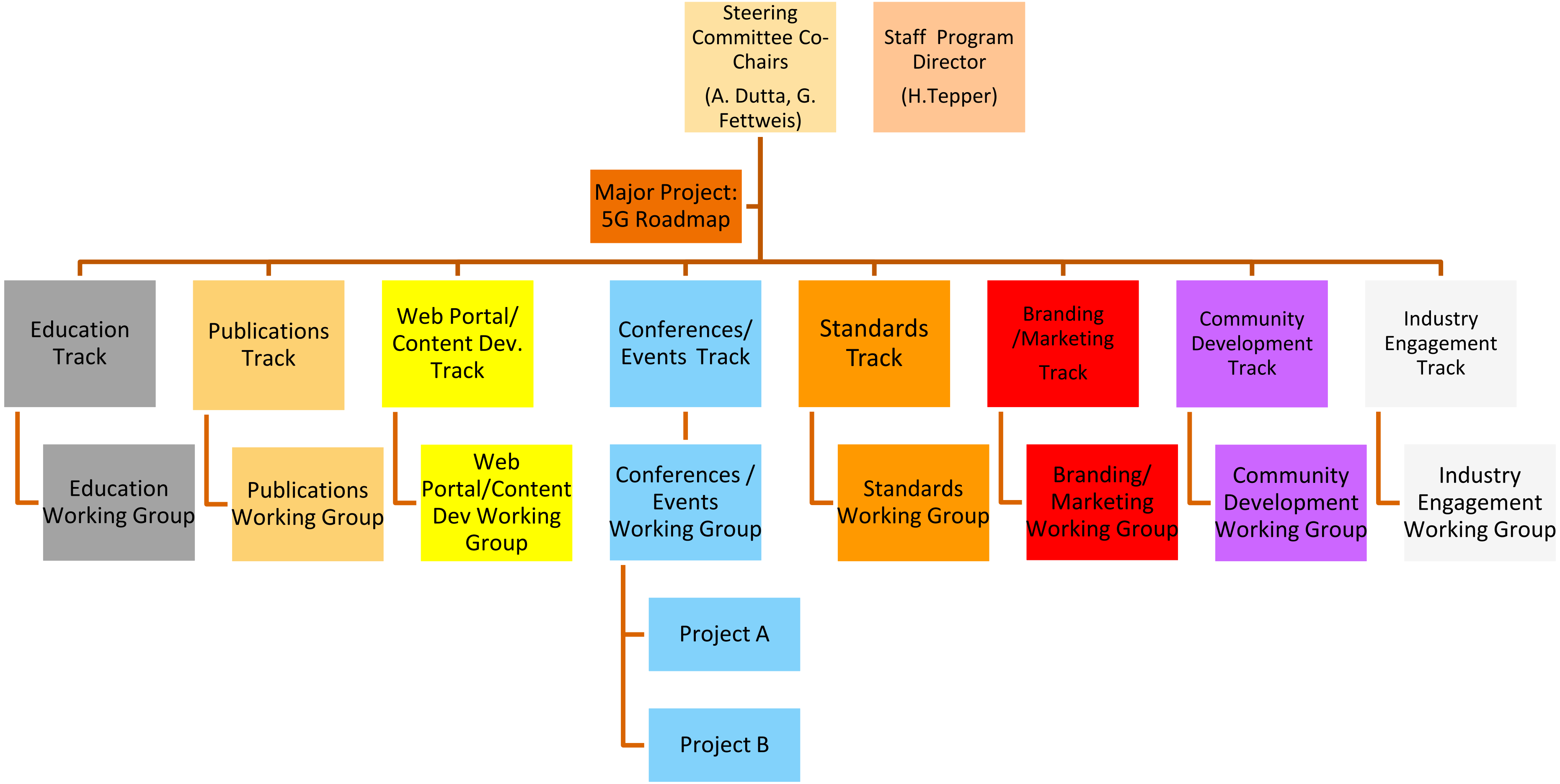
Kuwait City, Kuwait
March, 2017

IEEE 5G SUMMIT

IEEE ComSoc
IEEE Communications Society

IEEE
Advancing Technology for Humanity

- Convened Kick-Off Workshop in Princeton, NJ on 29-30 August 2016
  - Participation by over 30 volunteers and IEEE staff representing 12 Societies/OUs
    - Communications
    - Computer
    - Solid States Circuits
    - Signal Processing
    - Vehicular Technology
    - Technology and Engineering Management
    - Instrumentation & Measurement
    - Intelligent Transportation
    - Microwave Theory and Techniques
    - Standards Association
    - Educational Activities
    - Future Directions
- Identified Working Groups and Projects for 2016/2017



Steering Committee Co-Chairs

(A. Dutta, G. Fettweis)

Staff Program Director

(H.Tepper)

Major Project: 5G Roadmap

Education Track

Education Working Group

Publications Track

Publications Working Group

Web Portal/ Content Dev. Track

Web Portal/Content Dev Working Group

Conferences/ Events Track

Conferences / Events Working Group

Project A

Project B

Standards Track

Standards Working Group

Branding /Marketing Track

Branding/ Marketing Working Group

Community Development Track

Community Development Working Group

Industry Engagement Track

Industry Engagement Working Group

- Seeking volunteers
  - Broad range of opportunities
    - Technical Areas – Massive MIMO, mmWave, Mobile Edge Cloud……
    - Functional Areas – Publications, Education, Roadmap, Content/Community Development….
- Contact us directly
  - Ashutosh Dutta, Initiative Co-Chair:

    ashutosh.dutta@ieee.org
  - Gerhard Fettweis, Initiative Co-Chair: Gerhard.Fettweis@tu-dresden.de
  - Harold Tepper, Initiative Senior Program Director: h.tepper@ieee.org

Summary

- Transformation of Mobility to Cloud
- Emerging services are evolving rapidly
- SDN/NFV is an enabler for 5G
- Opportunities in this new virtualized environment
- Comprehensive security architecture is essential to take care of security challenges
- Operators and vendors need to work together to form a security ecosystem
- Standards, Testbeds and POCs act as catalyst for Virtualization

Dynamic Security Control Demo

IMS Threat Categories

	Category	Threat	Description
T1	Loss of Availability	Flooding an interface	DDoS/TDoS via Mobile end-points
T2		Crashing a network element	DoS/TDoS via rogue media streams and malformed packets
T3	Loss of Confidentiality	Eavesdropping	Eavesdropping via sniffing the SGi(Gm) interface
T4		Data leakage	Unauthorized access to sensitive data on the IMS-HSS
T5	Loss of Integrity	Traffic modification	Man-in-the-middle attack on SGi(Gm) interface
T6		Data modification	SIP messaging impersonation via spoofed SIP messages
T7	Loss of Control	Control the network	SPIT(Spam over Internet Telephony) / unsolicited voice calls resulting in Voice-SPAM/TDoS
T8		Compromise of network element	Compromise of network element via attacks from external IP networks
T9	Malicious Insider	Insider attacks	Malicious Insider makes unauthorized changes to IMS-HSS, SBC, P/I/S-CSCF configurations
T10	Theft of Service	Service free of charge	Theft of Service via SIP messaging impersonation

RAN Threat Categories

	Category	Threat	Description
T1	Loss of Availability	Flooding an interface	DOS on eNodeB via RF Jamming
T2		Crashing a network element	DDOS on eNodeB via UE Botnets
T3	Loss of Confidentiality	Eavesdropping	Eavesdropping on S1-MME/S1-U interfaces
T4		Data leakage	Unauthorized access to sensitive data on the eNodeB
T5	Loss of Integrity	Traffic modification	Man-in-the-Middle attack on UE via false eNodeB
T6		Data modification	Malicious modification of eNodeB configuration data
T7	Loss of Control	Control the network	Attackers control the eNodeB via protocol or implementation flaw
T8		Compromise of network element	Attackers compromise the eNodeB via management interface
T9	Malicious Insider	Insider attacks	Malicious Insider makes unauthorized changes to eNodeB configuration
T10	Theft of Service	Service free of charge	Theft of Service via Spoofing/Cloning a UE