IEEE Future Networks Webinar
Security in SDN/NFV and 5G Networks – Opportunities and Challenges

Ashutosh Dutta, Ph.D.
Senior Scientist, Johns Hopkins University Applied Physics Lab (JHU/APL), USA
Co-Chair, IEEE Future Network Initiative
IEEE Communications Society Distinguished Lecturer
Email: ashutosh.dutta@ieee.org; Ashutosh.Dutta@jhuapl.edu
03/26/2019
Talk Outline

- Drivers for SDN/NFV and 5G
- Cellular Technology Evolution
- Key 5G Characteristics
- Threat Taxonomy
- Opportunities and Challenges in Security Virtualization and 5G
- Security Use Cases
- Industry Standards Activities and Testbed
- Summary

Part II: IEEE Future Networks Initiative Overview

Parts of this presentation have been discussed in various ETSI/NFV and IEEE Security and SDN/NFV Working Groups
Emerging Services and Applications
A Driver for Network Evolution
SLAs associated with Types of Applications

Capturing maximum value during 4G to 5G evolution

Source: Nokia
Evolution of wireless access technologies

1 G
- TACS
- Analog FM
- NMT

2 G
- GSM
- 9.6 kb/s
- GPRS
- 14.4 kb/s
- EDGE
- 236 kb/s
- WCDMA
- 144 kb/s, 384 kb/s, 2 Mb/s

2.5 G
- EDGE
- 236 kb/s
- CDMA2000 1X
- 144 kb/s, 384 kb/s, 2 Mb/s

3 G
- DS/CDMA T/CDMA
- UMB
- 280 Mb/s
- LTE
- 80 UL, 360 DL

4 G
- IEEE 802.16
- OFDM
- 80 Mb/s (UL), 360 Mb/s
- 802.20

5G
- 10 Gbps DL Speed
Co-existence of IEEE and 3GPP Technologies
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
- Densification of Small Cells
- Wireless Backhaul / Access Integration
- Flexible Networks
- Flexible Mobility
- Context Aware Networking
- Information Centric Networking
- Moving Networks
5G – Emerging Architecture and Enabling Technologies

5G Architecture Themes: Flexibility, Scalability

5G New Radio

- Fiber-like performance
- However, 5G is Multi-RAT

- Network Function Virtualization
  - Network realized in software: Core and RAN
  - Cloud resources throughout the network

- Programmable Network
  - Flexible orchestration of network resources and infrastructure: RAN, core, transport, etc.

- Network Slicing
  - Self-contained, independent network partition including all segments: radio, core, transport, and edge.
  - Multi-domain, multi-tenant

Source: 5G-PPP Architecture WG
View on 5G Architecture (Version 2.0)
5G Dimensions and 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

Courtesy: Gerhard Fettweis
Enhanced Mobile Broadband & UHRLLC Use Cases

• Enhanced Mobile Broadband (eMBB)
  • Expected throughput of 5 Gbps +
  • UHD video (4k, 8k), 3D video (including broadcast services)
  • Virtual Reality
  • Augmented Reality
  • Tactile Internet
  • Cloud gaming
  • Broadband kiosks
  • Vehicular (cars, buses, trains, aerial stations, etc.)

• High reliability / low latency
  • Industrial control
  • Remote manipulation
  • Mission-critical applications e.g. ehealth, hazardous environments, rescue missions, etc.
  • Self-driving vehicles

Source: ITU-R
What “5G and Advanced Communication Systems” is About
Key Pillars of SDN/NFV and 5G Security
SDN/NFV is the Foundation of 5G Core Network

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

Independent Software Vendors

Orchestrated, automatic & remote install.

Standard High Volume Servers

Standard High Volume Storage

Standard High Volume Ethernet Switches
Overview of NFV (Network Function Virtualization) Sample Use cases

Virtualization of Mobile CORE and IMS

Virtualization of CDNs

Virtualization of CDN

Virtualization of Base Stations

Virtualization of Fixed Access

Virtualization of Fixed Access

Virtualization of Home and Enterprise Networks

Legend

VNF
HW
Hardware resources
Hardware resource pool

IEEE
NFV Use Case: Virtualization of Mobile Core Network (EPC) and IMS
An Example - Security Transformation – Virtual Firewall/Virtual DDOS/Virtual IPS

**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

**Virtualized Security Function**

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

**Virtual Security Functions**

- vDOs
- vFW1
- vFW2
- IDS1
- IDS2

**Common Cloud Infrastructure**
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)
General Threat Taxonomy (EPC) – Ref. ETSI/NFV Monitoring and Management (Draft 13)

LTE/EPC Security Threats Categories
## Mobile Network Security - EPC

### Threat Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1 Loss of Availability</td>
<td>Flooding an interface</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 Loss of Confidentiality</td>
<td>Eavesdropping</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 Loss of Integrity</td>
<td>Traffic modification</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 Loss of Control</td>
<td>Control the network</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 Malicious Insider</td>
<td>Insider attacks</td>
<td>Insiders make data modification on network elements, make unauthorized changes to NE configuration, etc.</td>
</tr>
<tr>
<td>T10 Theft of Service</td>
<td>Service free of charge</td>
<td>Attackers exploits a flaw to use services without being charged</td>
</tr>
</tbody>
</table>
Attacks Taxonomy – VoLTE/IMS/USP

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

Attacks via SIP messaging impersonation (Theft of service)

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)

Circuit Switched Domain (eMSC, MGCF, 3G-MSC, MGW )

Other VoIP & PSTN

VoLTE/IMS/USP

Insider attacks (compromise of network element)
## IMS Threat Categories

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

- Attacks on the Radio Interface
- Attacks with physical access to eNodeB
- Attacks with physical access to the transport network (includes: S1-MME, S1-U, OAM, X2)
- Attacks by Mobile end points

Diagram showing connections between mobile devices, eNodeB, RAN, EPC, MME, S-GW, and OAM.
<table>
<thead>
<tr>
<th>Category</th>
<th>Threat</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>T1 Loss of Availability</td>
<td>Flooding an interface</td>
<td>DOS on eNodeB via RF Jamming</td>
</tr>
<tr>
<td>T2</td>
<td>Crashing a network element</td>
<td>DDOS on eNodeB via UE Botnets</td>
</tr>
<tr>
<td>T3 Loss of Confidentiality</td>
<td>Eavesdropping</td>
<td>Eavesdropping on S1-MME/S1-U interfaces</td>
</tr>
<tr>
<td>T4</td>
<td>Data leakage</td>
<td>Unauthorized access to sensitive data on the eNodeB</td>
</tr>
<tr>
<td>T5 Loss of Integrity</td>
<td>Traffic modification</td>
<td>Man-in-the-Middle attack on UE via false eNodeB</td>
</tr>
<tr>
<td>T6</td>
<td>Data modification</td>
<td>Malicious modification of eNodeB configuration data</td>
</tr>
<tr>
<td>T7 Loss of Control</td>
<td>Control the network</td>
<td>Attackers control the eNodeB via protocol or implementation flaw</td>
</tr>
<tr>
<td>T8</td>
<td>Compromise of network element</td>
<td>Attackers compromise the eNodeB via management interface</td>
</tr>
<tr>
<td>T9 Malicious Insider</td>
<td>Insider attacks</td>
<td>Malicious Insider makes unauthorized changes to eNodeB configuration</td>
</tr>
<tr>
<td>T10 Theft of Service</td>
<td>Service free of charge</td>
<td>Theft of Service via Spoofing/Cloning a UE</td>
</tr>
</tbody>
</table>
SDN/NFV-based Evolved Packet Core

Common Hardware (COTS)

Management & Orchestration
- vMME
- vHSS
- vPCRF
- vS-GW
- vP-GW
- vPCEF

Hypervisor

Data Analytics
- SLA Mgmt
- Usage Mgt
- Monitoring

Internet, Cloud Services, Partners
SGi
Virtualized IMS

SDN Controller

Mobile Devices (Smartphones, M2M, IoT)
LTE RAN
eNodeB
Security Advantages of SDN/NFV
A Comprehensive View of SDN/NFV Security Advantages

**Design Enhancements:**
- Centralize Control and Management Functions
- Security Embedded at Design Time
- Security that Exceeds Existing Perimeter
- Multivendor Security Service

**Performance Improvements:**
- Streamline and Reduce Incident Response Cycle Time
- Streamline and Reduce Patching Cycle Time

**Real-Time capabilities:**
- Real-Time Scaling to Absorb DDOS Attacks
- Real-Time Integration of “Add-on” Security Functions
Security Opportunities from Virtualization

DDoS Attack Resiliency – Control Plane

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.

Orchestrator instantiates new VM to scale-out vMME function to sustain the higher traffic load while we investigate.
Security Opportunities from Virtualization

SDN Controller Dynamic Security Control – Data Plane

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

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

Non-malicious traffic
Security Challenges from Virtualization

Hypervisor Vulnerabilities

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,

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

Malware compromises VMs:
- VM/Guest OS manipulation
- Data exfiltration/destruction

Common Hardware (COTS)

Hypervisor (Host OS)

Tenant 1

Tenant 2

Tenant 3

VNF

VM Guest OS

VNF

VM Guest OS

VNF

VM Guest OS
Security Vulnerability in ODL SDN Controller

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

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

**Mitigation Strategy:**
- Open source community reported the problem, a patch was applied to disable external entity access and fix the problem.

- Denial of Service Attack through South Bound Interface
- REST API Parameter Exploitation – North Bound API
- North Bound API Flood Attack
- MAN-IN-THE MIDDLE ATTACK/Spoofing
- Protocol Fuzzing – South Bound
- Controller Impersonation – South Bound
SDN Controller Security Use Cases

- Denial of Service Attack through South Bound Interface
- REST API Parameter Exploitation – North Bound API
- North Bound API Flood Attack
- MAN-IN-THE MIDDLE ATTACK/Spoofing
- Protocol Fuzzing – South Bound
- Controller Impersonation – South Bound
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 servers 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
Network Function Virtualization
Security Challenges and Opportunities

- Existing Threats
- New Virtualization Threats
- Security Opportunities

**Network Function Virtualization**

**Security Challenges and Opportunities**

- DDoS Mitigation Scheme
- Hypervisor
- Orchestration
- SDN
- vEPC
- vMME
- vHSS
- vPCRF
- vS-GW
- vP-GW
- vPCEF

**DDoS Mitigation Scheme**

- Signaling Storm by Mobile Devices
- Attacks from User Plane by Mobile Devices

**Exploit Orchestration Vulnerability**

- Orchestration
- DDoS/ Attacks from the Internet

**Exploit Hypervisor Vulnerability**

- Hypervisor
- Common Hardware
- SDN

**DDoS/ Attacks from the Internet**

- vEPC
- Real Time Services
- Internet
- Cloud Services
- Partner Networks

**Amplification Attacks Enhanced by Elasticity Function**

- Attacks from Mobile Devices
- LTE RAN
- eNodeB

**Mobile Devices (Smartphones, M2M, IoT)**

**IEEEE**
Threat Scenarios in NFV (Reference - ETSI NFV)

1. Attack from VMs in the same domain
2. Attack to host, hypervisor and VMs from applications in host machine
3. Attacks from host applications communicating with VMs
4. Attacks to VMs from remote management path
5. Attack to external communication with 3rd party applications
6. Attacks from external networks via edge network
7. Attacks from VMs from external network

Hacker
- Social engineering attack
- APT attack
- Application vulnerabilities
- Misoperation
- Improper security policy configuration
- Malicious behaviour

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 Use Cases for 5G RAN

DDOS attacks against Network Infrastructure

• Overload of the signaling plane by a huge number of infected M2M/IOT devices that attempt to gain access
• Overload of the signaling plane by a huge number of infected M2M/IOT devices that transmit intermittently and simultaneously
• Resource Starvation at cRAN vFW
• Leverage IOT for Distributed Denial of Service
• Resource Sharing by multiple service providers at cRAN
• Deliberate triggering of network and overload mechanisms
• Bulk configuration
Security Use Cases for Mobile Edge Computing

- Storage of Sensitive Security Assets at the Edge
- Third party applications on the same platform as network functions
- User Plane attacks in Mobile Edge Computing Environment
- Exchange of Sensitive Security Assets between core and Mobile Edge
- Trust establishment between functions at the core and at the edge
- Subscriber authentication within the visited network
- Secure storage of credentials to access IMS network
- Access to 5G core over non-3GPP network access
- User plane data security over less trusted 3GPP network accesses
- Management of credentials to access non-3GPP network access
Security Use Cases for Network Slicing

- Controlling Inter-Network Communications
- Instantiation time Impersonation attacks against Network Slice Manager
- Impersonation attacks against a Network Slice instance within an Operator Network
- Impersonation attacks against different Network Slice managers within an Operator Network
- Different Security Protocols or Policies in different slices
- Denial of Service to other slices
- Exhaustion of security resources in other slices
- Side Channel Attacks Across Slices
- Hybrid Deployment Model
- Sealing between slices when UE is attached to several slices
Relevant SDN/NFV/5G Standards

<table>
<thead>
<tr>
<th>Forum</th>
<th>Focus</th>
</tr>
</thead>
<tbody>
<tr>
<td>IETF</td>
<td>Network Virtualization Overlay, Dynamic Service Chaining, Network Service Header</td>
</tr>
<tr>
<td>3GPP</td>
<td>Mobility and Security Architecture and Specification</td>
</tr>
<tr>
<td>IEEE</td>
<td>Develop Technologies for that can be used by other Standards Bodies. There are 42 societies to contribute to 5G Eco System</td>
</tr>
<tr>
<td>ONF</td>
<td>OpenFlow SDN Controller Standards</td>
</tr>
<tr>
<td>OPNFV</td>
<td>NFV Open Platform/eCOMP/OPNFV Community TestLabs</td>
</tr>
<tr>
<td>Openstack</td>
<td>Cloud OrCHEstrator Open Source</td>
</tr>
<tr>
<td>OpenDaylight</td>
<td>Brownfield SDN Controller Open Source</td>
</tr>
<tr>
<td>ONOS</td>
<td>OpenFlow SDN Controller Open Source</td>
</tr>
<tr>
<td>DPDK/ODP</td>
<td>CPU/NIC HW API – Data Plane Development Kit</td>
</tr>
<tr>
<td>KVM Forum</td>
<td>Hypervisor</td>
</tr>
<tr>
<td>OVS</td>
<td>Open Source vSwitch</td>
</tr>
<tr>
<td>Linux</td>
<td>Operating System, Container Security</td>
</tr>
<tr>
<td>ATIS/NIST/FCC/CSA</td>
<td>Regulatory Aspects of SDN/NFV</td>
</tr>
</tbody>
</table>
Virtual IDS Prototype for Mobility CORE

1. Malicious URL Detection and Mitigation
2. Malware Detection and Mitigation
3. Application and Overload Control

Subscriber accesses Blacklisted URL

UE cannot access this URL anymore but other URLs

UE, eNodeB Emulator

Real UE

eNodeB

Virtualized EPC

Virtualized IDS

vMME

vS-GW

vPGW/
PCEF

vPCRF

Application Function (AF)

Rx (Diameter)

Simulated Internet

Internet, IMS or Other PDNs (e.g. WiFi)

Blacklisted WEB Server

Malware Web Server

UE, eNodeB Emulator

Subscriber accesses Blacklisted URL

vIDS/vIPS detects the subscriber and Malicious URL

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

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

Virtualized EPC

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

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control

vPCRF

SIMS

Rx (Diameter)

Malware Web Server

Blacklisted WEB Server

Ineternet, IMS or Other PDNs (e.g. WiFi)

Simulated Internet

UE, eNodeB Emulator

UE cannot access this URL anymore but other URLs

Dynamic Security Control Points

3GPP E-RAB Modification Request

Malware Detection and Mitigation

Application and Overload Control
Blacklist Detection for DSC
Malware Download Detection for GDSC
Before Throttling

After Throttling
2018 FDC Initiatives & Activities

Small Projects
- Environmental Engineering
- Roadmaps Strategy and Governance (IRSG)
- Quantum Computing

Graduated Initiatives
- IEEE Big Data
- IEEE Smart Cities
- IEEE Cloud Computing
- IEEE Cyber Security
- IEEE Software Defined Networks
- IEEE Internet of Things
- IEEE Transportation Electrification Community
- IEEE Sustainable ICT
- IEEE Technology Time Machine
- IEEE Future Directions

ieee.org/futureredirections
Key Stakeholders

IEEE Societies (22 so far)

Initiative Profile
- Launched August 2016
- Technical Activities Board Funded
- 20+ Participating Societies/OUs
Led by a steering committee of 30 leaders from a diverse set of Future Networks-related IEEE Societies

The global team of experts involved in IEEE Future Networks are producing programs and activities including...

- **The Future Networks Roadmap**
  - short-term (~3 years), mid-term (~5 years), and long-term (~10 years) research, innovation, and technology trends

- **Conferences & Events**
  - IEEE 5G Summits
  - IEEE 5G World Forums
  - Future Networks-related IEEE conferences

- **Standards**
  - Global, open, and collaborative

- **Education**
  - IEEE Future Networks Learning Series
  - IEEE Live Online Courses, Webinar series
  - Videos from IEEE 5G Summits

- **Expert Articles**
  - Published on IEEE Future Networks web portal and in industry media

- **Publications**
  - IEEE Future Networks Transmissions podcast series
  - IEEE Future Networks Tech Focus Newsletter
  - IEEE Future Directions Talks Future Networks Q&A article series
IEEE Future Networks Initiative Organization Structure

Steering Committee Co-Chairs
A. Dutta
G. Fettweis
T. Lee

Staff Program Director
H. Tepper

Education Working Group
R. Ting
R. Annaswamy

Publications Working Group
C-L. I
G. Yi

Roadmap Working Group
C-M. Chen
R. Hu

Conferences & Events Working Group
L. Ladid
A. Dutta

Standards Working Group
M. Ulema
A. Gelman

Content & Community Development Working Group
J. Irvine
A. Wyglinski

Testbed Working Group
I. Seskar
T. Van Brackle

Industry Engagement Working Group
M. Lu
S. Dixit
Roadmap Structure – Leadership and Working Group Co-chairs

**Standardization Building Blocks**
- Paul Nikolich
- Alex Gelman
- Purva Rajkotia
- Mehmet Ulema

**mmWave and Signal Processing**
- Timothy Lee
- Harish Krishnaswamy
- Earl McCune

**mmWave and Signal Processing**
- Paul Nikolich
- Alex Gelman
- Purva Rajkotia
- Mehmet Ulema

**Massive MIMO**
- Rose Quingyang Hu
- Dongming Wang
- Chris Ng
- Chi Ming Chen
- Haijian Sun

**Applications and Services**
- Ravi Annaswamy
- Narendra Mangra

**Hardware**
- Dylan Williams

**Security**
- Ashutosh Dutta
- Ana Nieto
- Ahmad Cheema

**Satellite**
- Sastri Kota
- Prashant Pillai
- Giovanni Giambene

**Applications and Services**
- Ravi Annaswamy
- Narendra Mangra

**Edge Automation Platform**
- Meryem Simsek
- Cagatay Buyukkoc
- Kaniz Mahdi
- Paul Littlewood

**NEW FOR 2019**
- Systems Optimization
  - Ashutosh Dutta
  - Kaniz Mahdi
- Optics
  - Feras Abou-Galala
  - Paul Littlewood
- Deployment
  - David Witkowski

**Connecting the Unconnected**
- Sudhir Dixit, Ashutosh Dutta
Summary

• Emerging services are evolving rapidly
• Network needs to be designed to be adaptable, resilient, and flexible
• Operators need to reduce Capex and Opex
• SDN/NFV is an enabler for 5G
• Opportunities and Challenges in this new virtualized environment
• 5G-specific application adds new security requirements
• 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
Thank you