Security Challenges and Opportunities in Future Networks

IEEE 7th World Forum on the Internet of Things (WF-IoT 2021)

June 22, 2021

Ashutosh Dutta, Ph.D.,
JHU APL,
Fellow of the IEEE,
IEEE Future Networks Founding Co-Chair
Security Working Group Co-Chair

Eman Hammad, Ph.D.
University of Texas A&M, RELLIS,
Security Working Group Co-Chair

Talk Outline

- Security WG Focus
- Key 5G Characteristics
- 5G Security Taxonomy
- Security for 5G Enablers
- Industry Standards Activities & Testbed
- Summary

Security WG Scope

The working group scope fundamentally addresses the following:

- **Security must be must be taken into consideration throughout 5G system layers**
- **5G architecture and characteristics extends a unique set of security challenges and opportunities that need to be studied and evaluated**
- **Develops and adopts a systematic and structured approach for threats identification and risk evaluation**

Security WG Activities

Technical

- Development of a system-level security taxonomic model
- Identification and development of an updated threat landscape and risk profiles for the End-to-End systems
- Identification of risk scenarios and performing system-level risk assessments across the different domain/WGs
- Development of roadmap chapters identifying opportunities, challenges, and gaps
- Identification and development of potential security standardization opportunities

Professional

- Engagement with relevant industries, organization and standardization bodies
- Development and dissemination of quality publications, white papers and roadmap chapters
- Creation and facilitation of engagement activities with scientific and professional society: conferences, industry days, workshops, webinars, podcasts, etc.

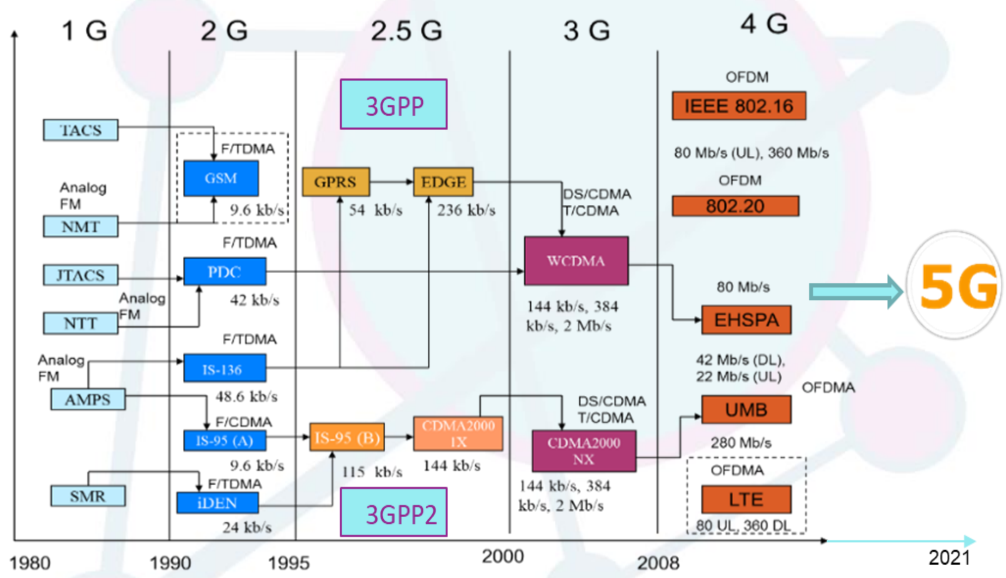
3-5-10-year Vision

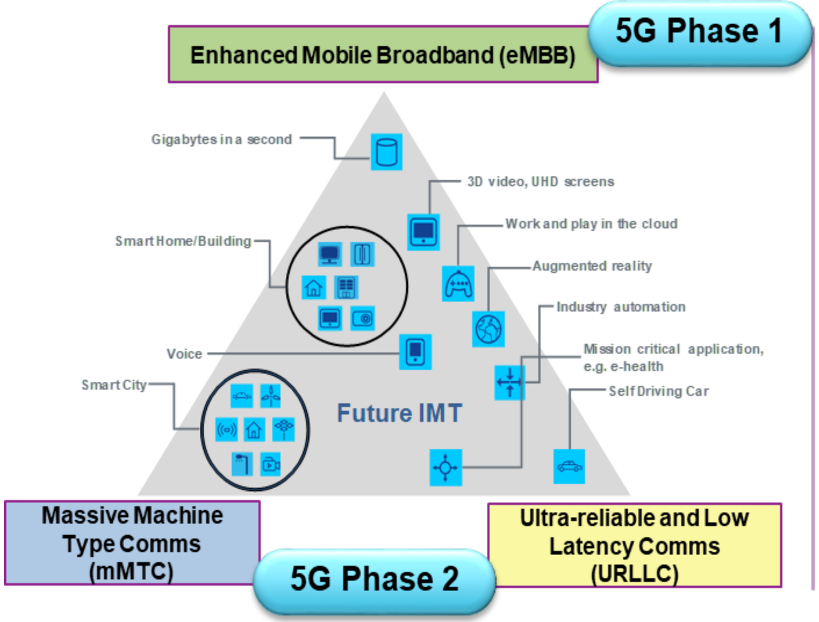
Domain	Sub-domain	1st Ed. Coverage	2nd Ed. Coverage	Future Editions
Foundational				
System Model (Taxonomy)				
Cybersecurity Frameworks (e.g., NIST)				
Risk Management				
Security and Privacy Domains				
Management and Orchestration Security	Optimization/orchestration security			
	Virtualization/softwarization security			
	SDN/NFV security			
	Network slicing			
Edge Security				
Third Party Security	Supply chain security			
	Open source/application programming interface (API) security			
	Device/Hardware Security			

3-5-10-year Vision (Contd.)

Domain	Sub-domain	1st Ed. Coverage	2nd Ed. Coverage	Future editions
Data Security and Privacy				
Satellite Security				
Radio Access Network Security	Massive MIMO Security			
	Physical Layer Security			
	O-RAN Security			
Security Monitoring & Analytics	Predictive / Proactive security			
	Digital forensics solutions			
Application Security Use-case	Application Security Requirements			
	Critical Infrastructure Systems			
	Emergency and first responder networks			
	Smart City (e.g. intelligent transportation)			
	Industrial IoT and SCADA			
AI/ML Security				
Interoperability				

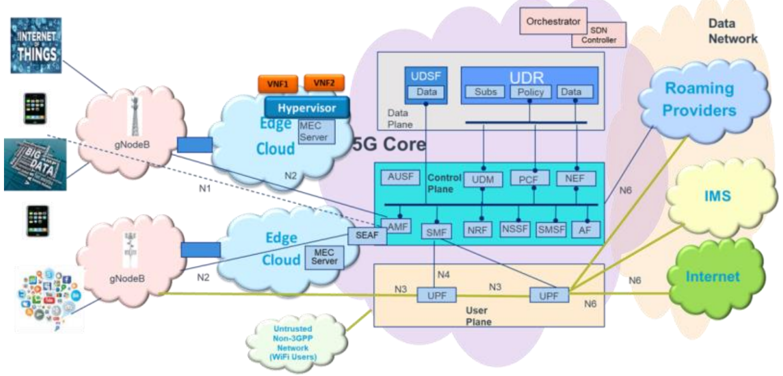
Evolution of cellular access technologies

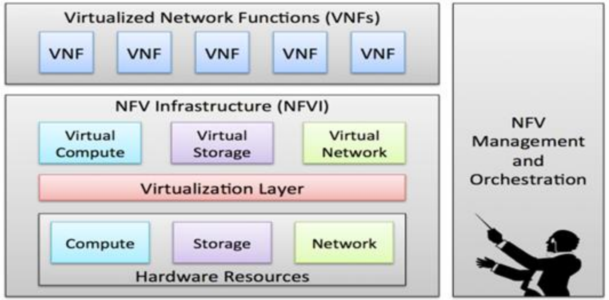


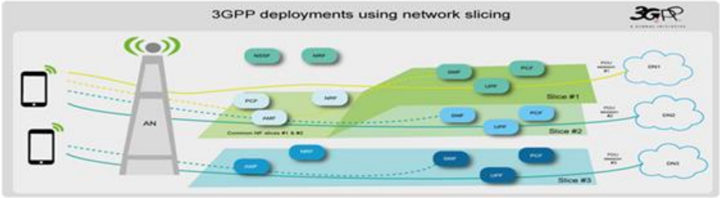


5G and Beyond Characteristics

- New Flexible Radio Access Technology (RAT) / Waveform
- Millimeter-wave (mmWave) Communications
- Massive MIMO
- Densification of Small Cells
- Wireless Backhaul / Access Integration
- Converged Networks
- Software Defined Networking / Network Function Virtualization
- Closed Loop Automation/Orchestration
- Mobile Edge Cloud
- Network Slicing
- Cloud Radio Access Network (C-RAN) / O-RAN
- Service-based architecture
- Heterogeneous Networks
- Device-Centric Architectures
- Native Machine-Type-Communications (MTC) Support







5G & Beyond: Security Perspective

5G Security

Cyber security risks to 5G

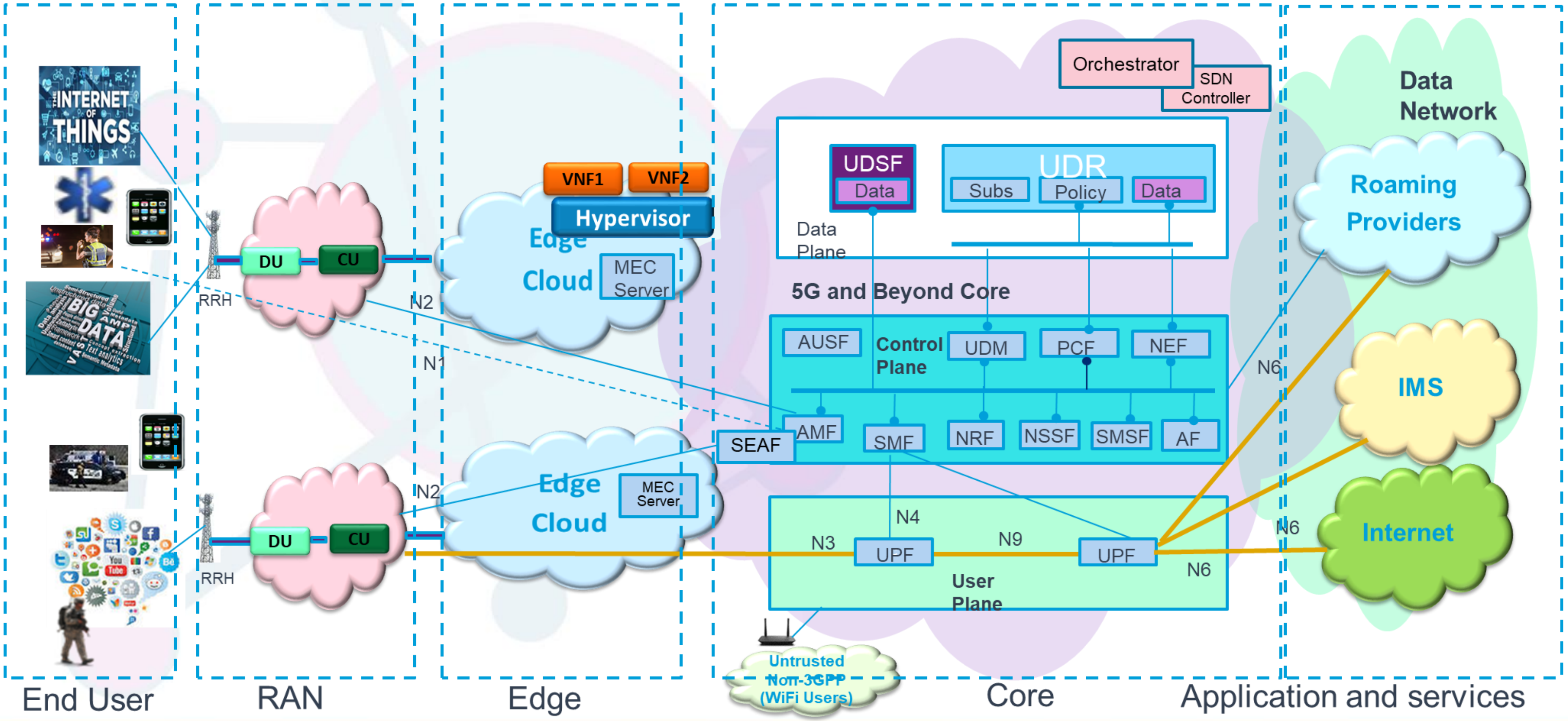
5G-enabled security (Opportunities)

Risks to 5G-enabled applications and use-cases

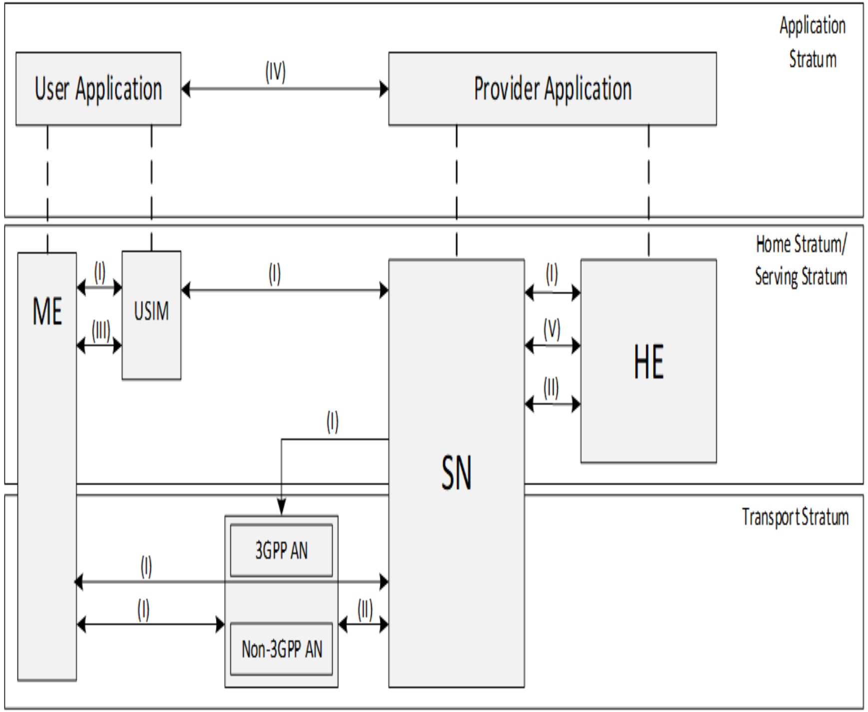
Risks to 5G networks and infrastructure

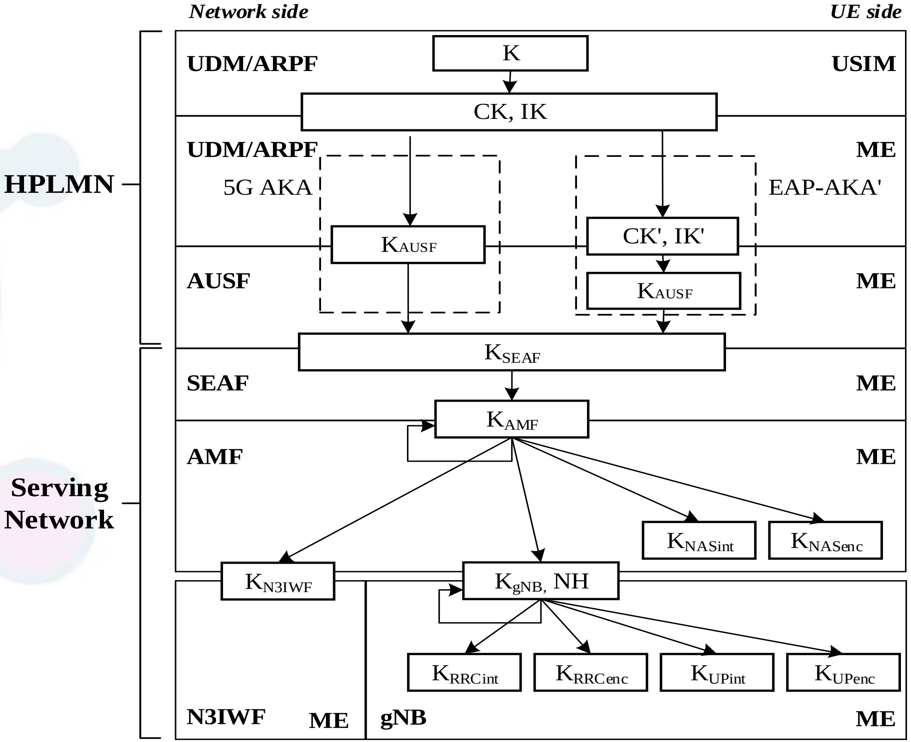
The progress of the 5G and beyond revolution may well be hindered if security issues are not tackled early on while the systems are being designed, standardized and deployed.

5G End-to-End System Model



5G Security Architecture and Key Hierarchy





Reference 3GPP TS 33.501

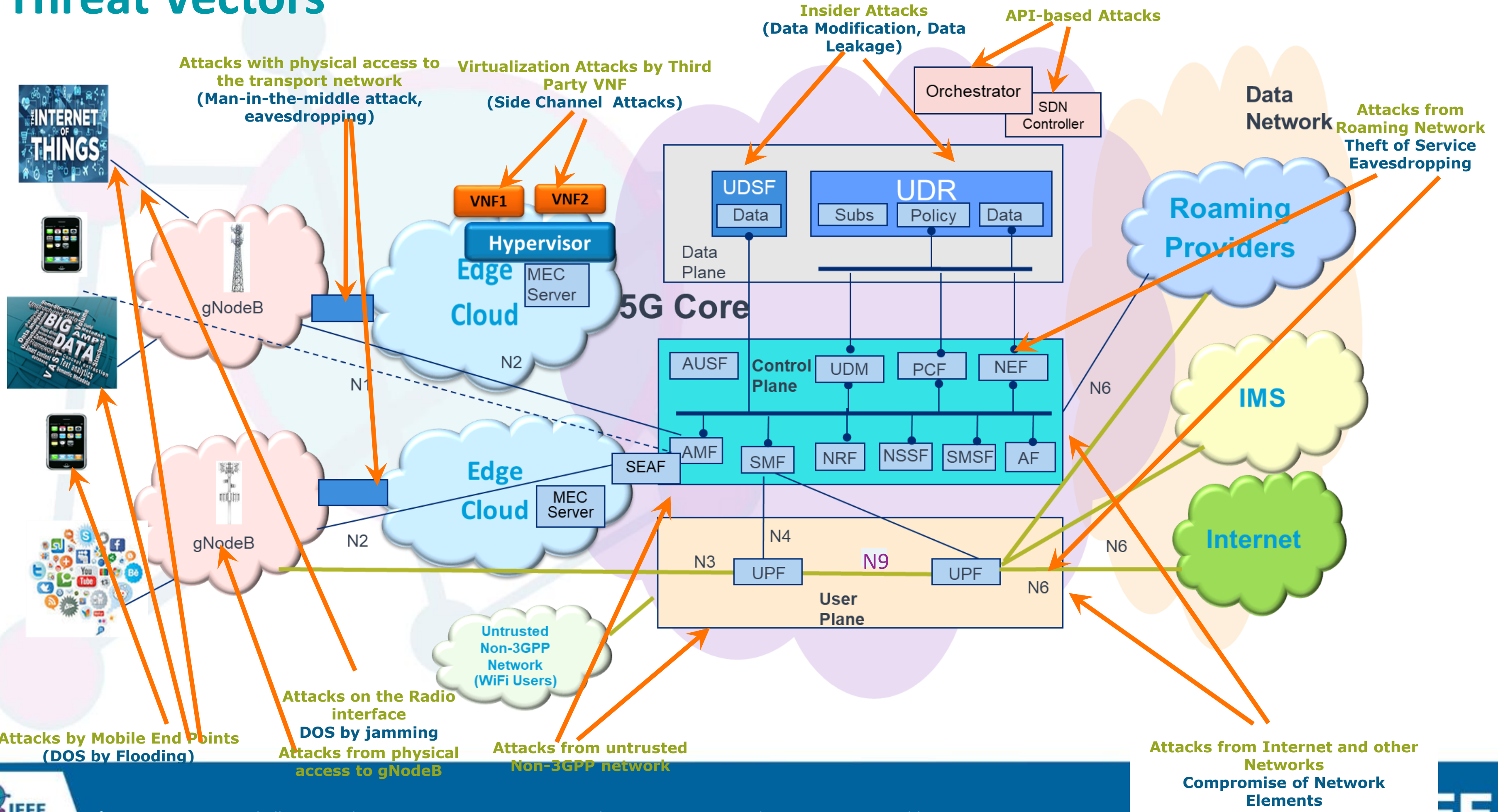
AUSF: Authentication Server Function

ARPF: Authentication Credential Repository and Processing Function, SEAF: Security Anchor Function

Comparison of 4G and 5G Security Authentication

		4G Authentication	5G Authentication		
		EPS-AKA	5G-AKA	EAP-AKA'	EAP-TLS
ENTITIES (LOCATED IN)	USER EQUIPMENT (UE)	USIM	USIM		USIM/Non-USIM
	SERVING NETWORK (SN)	MME	SEAF		
	HOME NETWORK (HN)	HSS	AUSF UDM/ARPF/SIDF		
MESSAGE FORMAT	UE <--> SN	NAS	NAS	NAS|EAP	NAS|EAP
	SN <--> HN	Diameter	HTTP-based web APIs		
TRUST MODEL		Shared symmetric key	Shared symmetric key		Public key certificate
UE IDENTITY	UE -> SN	IMSI/GUTI	SUCI/5G-GUTI		
	SN -> HN	IMSI	SUCI/SUPI		
SN IDENTITY		SN id (MCC+MNC)	SN name (5G:MCC+MNC)		
AUTHENTICATION VECTOR GENERATED BY		HSS	UDM/ARPF	UDM/ARPF	N/A
AUTHENTICATION OF UE DECIDED BY		MME	SEAF & AUSF	AUSF	AUSF
HN INFORMED OF UE AUTHENTICATION?		No	Yes	Yes	Yes

5G Threat Vectors



Reference: 5G Security Challenges and Opportunities: A System Approach, A. Dutta, E Hammad, 2020, IEEE 5G World Forum

5G Threat Taxonomy (RAN)

Category	Threat	Attack Description
Loss of Availability	Flooding an interface	DOS on gNodeB via RF Jamming
	Crashing a network element	DDOS on gNodeB via UE Botnets
Loss of Confidentiality	Eavesdropping	Eavesdropping on N2/N3 interfaces
	Data leakage	Unauthorized access to sensitive data on the gNodeB
Loss of Integrity	Traffic modification	Man-in-the-Middle attack on UE via false gNodeB
	Data modification	Malicious modification of eNodeB configuration data
Loss of Control	Control the network	Attackers control the eNodeB via protocol or implementation flaw
	Compromise of network element	Attackers compromise the eNodeB via management interface
Malicious Insider	Insider attacks	Malicious Insider makes unauthorized changes to gNodeB configuration
Theft of Service	Service free of charge	Theft of Service via Spoofing/Cloning a UE/

Reference: 5G Security Challenges and Opportunities: A System Approach, A. Dutta, E Hammad, 2020, IEEE 5G World Forum

5G Threat Taxonomy (Core)

Category	Threat	Attack Description
Loss of Availability	Flooding an interface	Attackers flood an interface and network assets (AMF, AUSF) resulting in DDoS condition on the signaling plane (e.g. multiple authentication failure on N1, N2 interface)
	Crashing a network element	Attackers crash a network element (e.g., AMF) by sending malformed packets
Loss of Confidentiality	Eavesdropping	Attackers eavesdrop on sensitive data on control and bearer plane to retrieve user location and device details and sensitive user data
	Data leakage	Unauthorized access to sensitive data (e.g., user profile) stored in UDR, UDSF
Loss of Integrity	Traffic modification	Attackers modify information during transit in user plane interface N3 (SIP header modification, RTP spoofing)
	Data modification	Attackers modify data on network element (e.g., change the gNodeB configurations through admin interface)
Loss of Control	Control the network	Attackers control the network via protocol or implementation flaw
	Compromise of network element	Attackers compromise of network element via management interface
Malicious Insider	Insider attacks	Insiders make data modification on network elements, make unauthorized changes to NE configuration, etc.
Theft of Service	Service free of charge	Attackers exploit a flaw to use services without being charged

5G Threat Taxonomy (IMS)

Category	Threat	Attack Description
Loss of Availability	Flooding an interface	DDoS/TDoS via Mobile end-points
	Crashing a network element	DoS/TDoS via rogue media streams and malformed packets
Loss of Confidentiality	Eavesdropping	Eavesdropping via sniffing the N6 interface
	Data leakage	Unauthorized access to sensitive data on the IMS-HSS
Loss of Integrity	Traffic modification	Man-in-the-middle attack on N3 and N6 interface
	Data modification	SIP messaging impersonation via spoofed SIP messages
Loss of Control	Control the network	SPIT (Spam over Internet Telephony) / unsolicited voice calls resulting in Voice-SPAM/TDoS
	Compromise of network element	Compromise of network element via attacks from external IP networks
Malicious Insider	Insider attacks	Malicious Insider makes unauthorized changes to IMS-HSS, SBC, P/I/S-CSCF configurations
Theft of Service	Service free of charge	Theft of Service via SIP messaging impersonation

Systematic Approach: Cyber Risk Assessment & Management

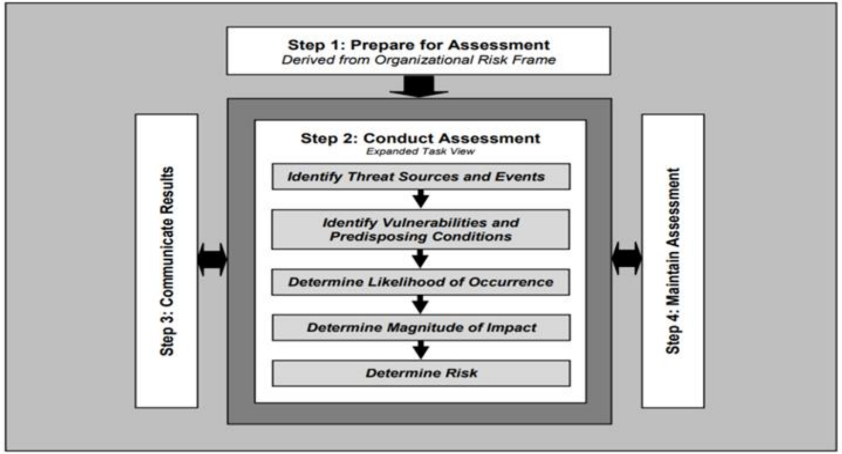
$$risk = \underbrace{likelihood}_{likelihood\,=\,f(vulnerabilities,\ exposure,\ threats,\ mitigating\ controls)} \times \overbrace{impact}^{impact\,=\,g(business\ criticality)}$$

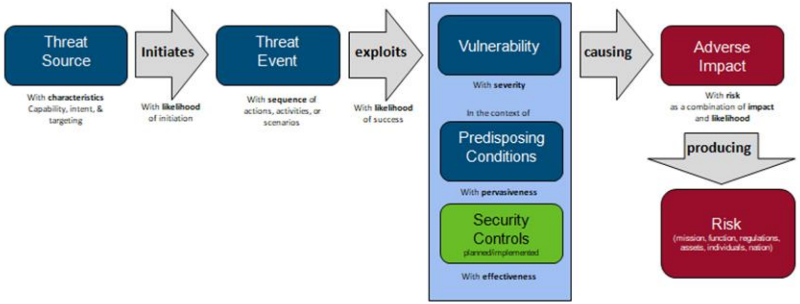
- *Vulnerability severity*
- *Threat level*
- *Business criticality*
- *Exposure/usage to the risk*
- *Risk-negating effect of any compensating controls an enterprise has in place*

https://www.balbix.com/insights/cyber-risk-heat-map/

Risk Management Framework

Function Identifier	Function	Category Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications





https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf

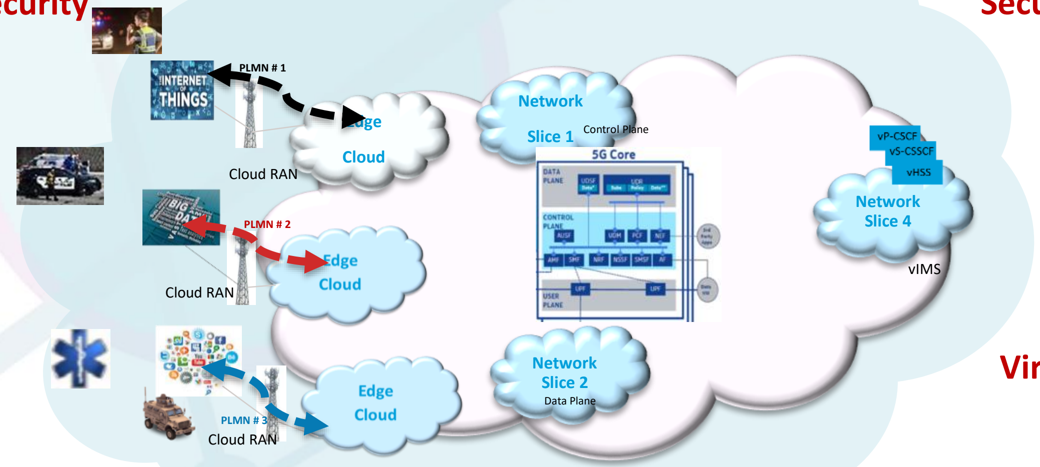
Key Pillars of "5G and Beyond" Security

SDN Security

Open RAN Security

Open Source / API Security

Edge Cloud Security



Network Slicing Security

Supply Chain Security

Virtualization Security

Predictive Security

Orchestration Security

Data Security and Privacy

Reference: 5G Security Challenges and Opportunities: A System Approach, A. Dutta, E Hammad, 2020, IEEE 5G World Forum

Security Virtualization

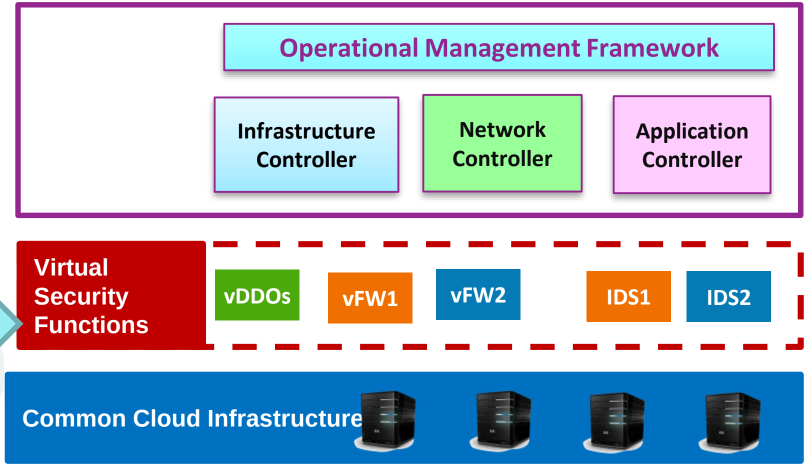
Virtual Firewall/Virtual DDOS/Virtual IPS

Non-Virtualized Security

Intel Security GUAVUS Tektronix HP f5 ARBOR NETWORKS ALLOT A10 NETWORKS NETSCOUT Check Point paloalto networks radware Alcatel-Lucent FORTINET JUNIPER NETWORKS sandvine movik FireEye

- 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

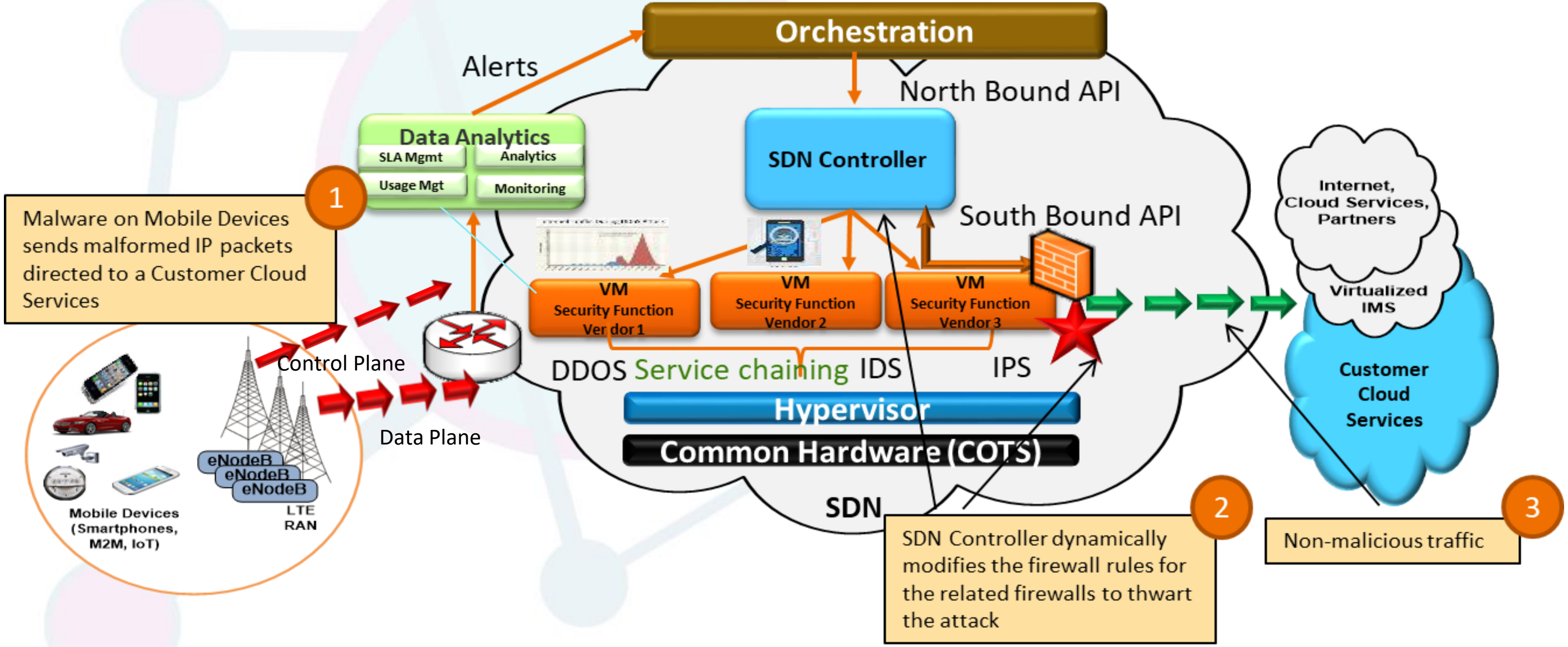
Virtualized Security Function



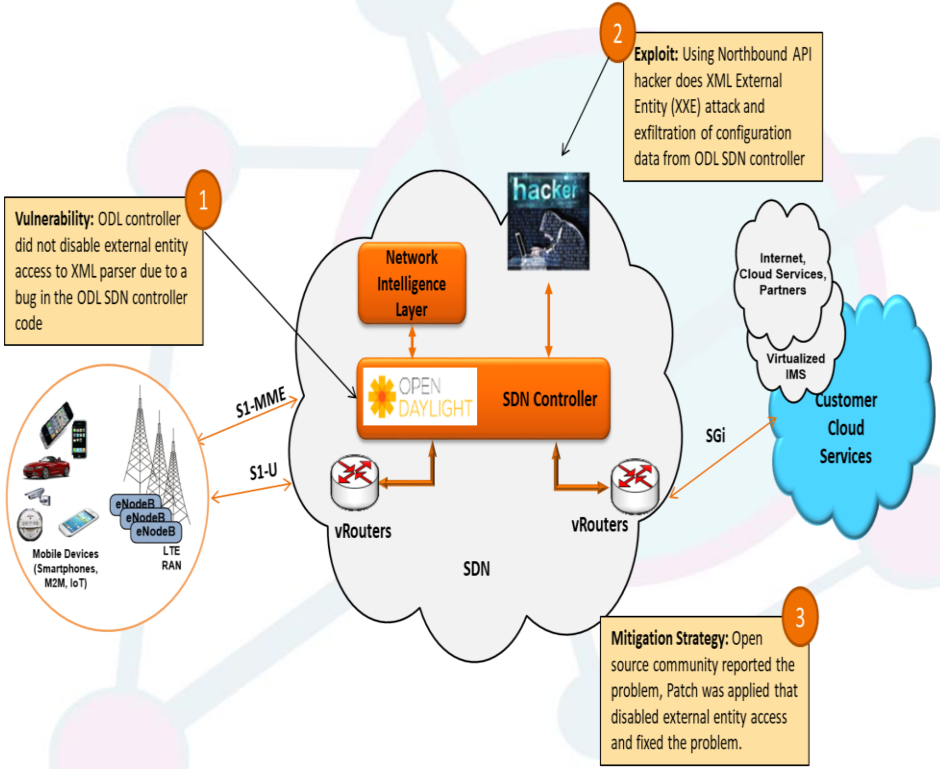
- Security functions will be cloud-based
- Security dynamically orchestrated in the cloud as needed
- Streamlined supplier integration
- Centralized common management platform
- Creates a standard operations/support model

SDN/NFV Security

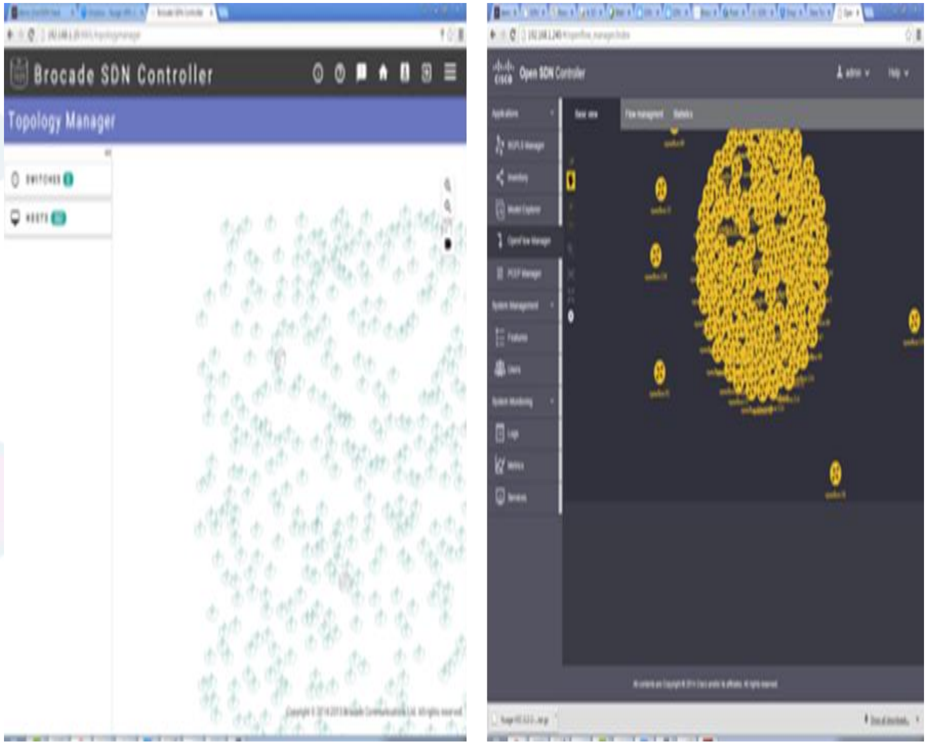
Security-As-a-Service – An Opportunity for Closed Loop Automation



SDN Controller Vulnerability



XML External Entity Attack



South Bound API Attack

SDN Controller – Security Opportunities, Challenges, Mitigation, and Risks

Security Opportunities	Potential Security Challenges	Potential Mitigation Techniques	Risk Severity	Threat Likelihood
SDN controller provides resilience to the attack and overload **Enhances programmability and adaptability** for the network routers and firewalls **Facilitates dynamic service chaining for** closed loop automation **Provides Dynamic Security Control mechanism** to stop attacks on signaling plane and data plane	Denial of service attack through South Bound Interface	• Security monitoring • Access control	🟠	🟢
	REST API Parameter Exploitation (North Bound API)	• API Authentication • SDN controller Code Scanning • System Logging and Auditing	🔴	🟠
	North Bound API Flood Attack	• API Monitoring • Closed Loop Automation	🟠	🟢
	Man-In-The Middle Attack (Spoofing Attack)	• SDN Scanner • Closed Loop Automation	🔴	🟠
	Protocol Fuzzing Attack (South Bound API)	• Hardening mechanism for SDN Controller	🟠	🟢
	Controller Impersonation (South Bound API)	• Access Control • API monitoring	🔴	🟢

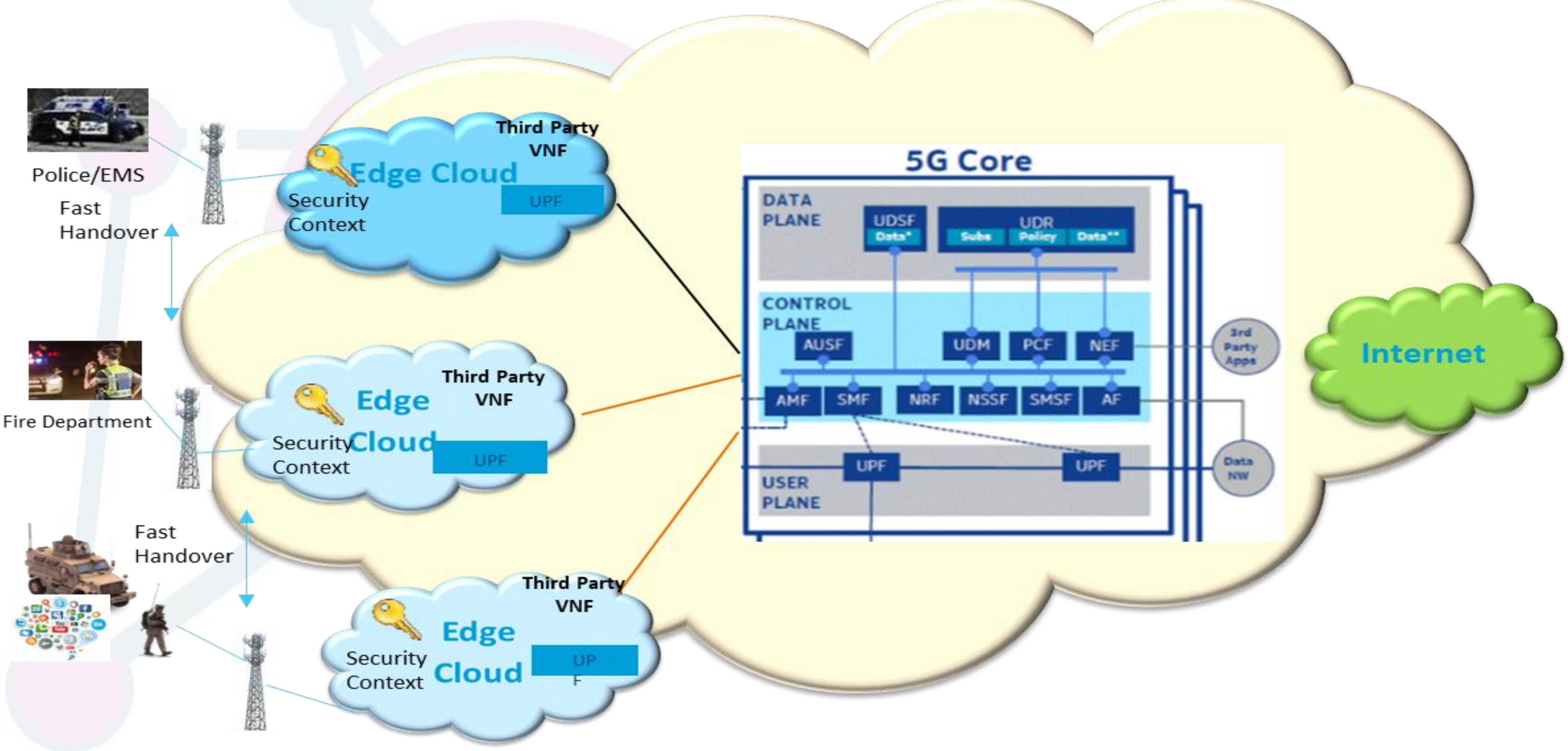
🔴 High 🟠 Medium 🟢 Low

Virtualization – Security Opportunities, Challenges, Mitigation, and Risks

Security Opportunities	Potential Security Challenges	Potential Mitigation	Risk Severity	Threat Likelihood
Provides resiliency in the event of DDOS attack Closed loop automation	Lack of visibility into Network Traffic	API-based monitoring Embed security monitoring in the Hypervisor	🟠	🟠
Multi-tenant operation	Execution of VMs with different Trust levels	Firewalls should be used to isolate VM groups from other groups for east-west traffic	🔴	🟠
Sharing of resources to support priority applications	VNF Catalog is compromised	Apply encryption for Data at Rest Harden Access Control	🔴	🟠
Ability to scale up and scale down the network based on the load by way of orchestration	Communication between VNF Catalog, Orchestrator, and Virtual Infrastructure Manager is compromised	API Security Hardening Security monitoring	🟠	🟠
Distributed inventory control	Wrong placement of VNF	Verification of VNF placement API Security	🔴	🟢

🔴 High 🟠 Medium 🟢 Low

Mobile Edge Cloud Security

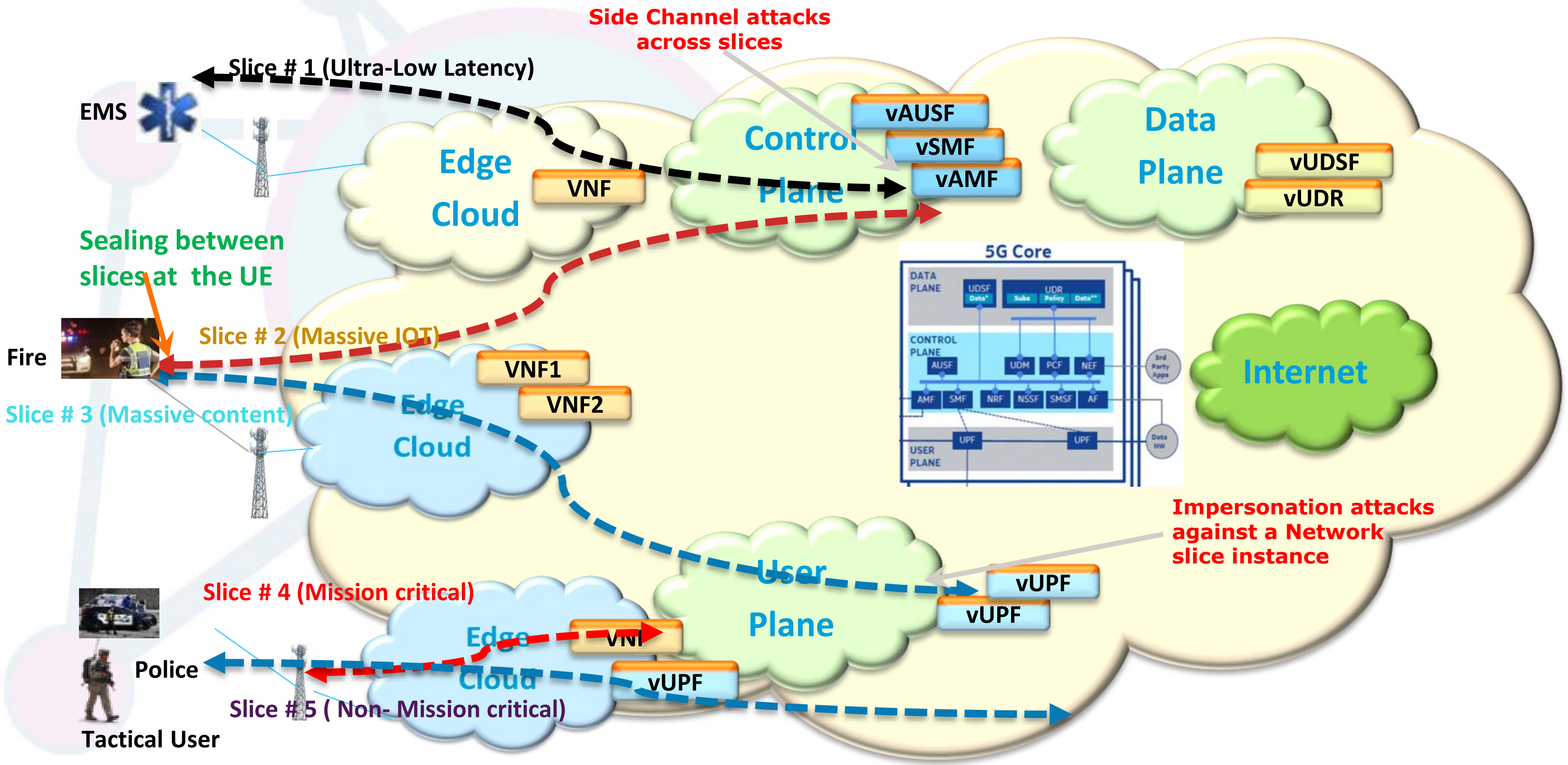


Mobile Edge Cloud - Security Opportunities, Challenges, Mitigation and Risks

Security Opportunities	Security Challenges	Potential Mitigation Techniques	Risk Severity	Threat Likelihood
Embed Security monitoring at the Edge of the network Application aware **performance optimization** **Reduced latency** by way of edge authentication for time sensitive applications **Secured and fast data** offloading during handover	Co-existence of the third party applications with the virtual network functions allow the hackers to infiltrate the platform	• Run both the edge computing applications and the network function(s) in robustly segregated virtual machines. • Higher priority for network functions		
	Storage of security context at the edge can lead to malicious spoofing attack	• Apply proper encryption mechanisms for the security context at the edge		
	User plane attacks in mobile edge including cache poisoning, cache overwhelming	• Access Control • Hardening Mechanism • Investigate the new security implications		
	Spoofing, eavesdropping or data manipulation attack during context transfer	• Encrypted transfer of security context • IDS/IPS for proper monitoring and mitigation,		
	Subscriber authentication within the visited networks leads to fraud and lack of control by home operator	• Reuse old security association (SA) while running AKA with the home network and acquiring a new security association. • Timely expiry of temporary security association • Proper authentication between DSS and UE		

High Medium Low

Network Slicing Security

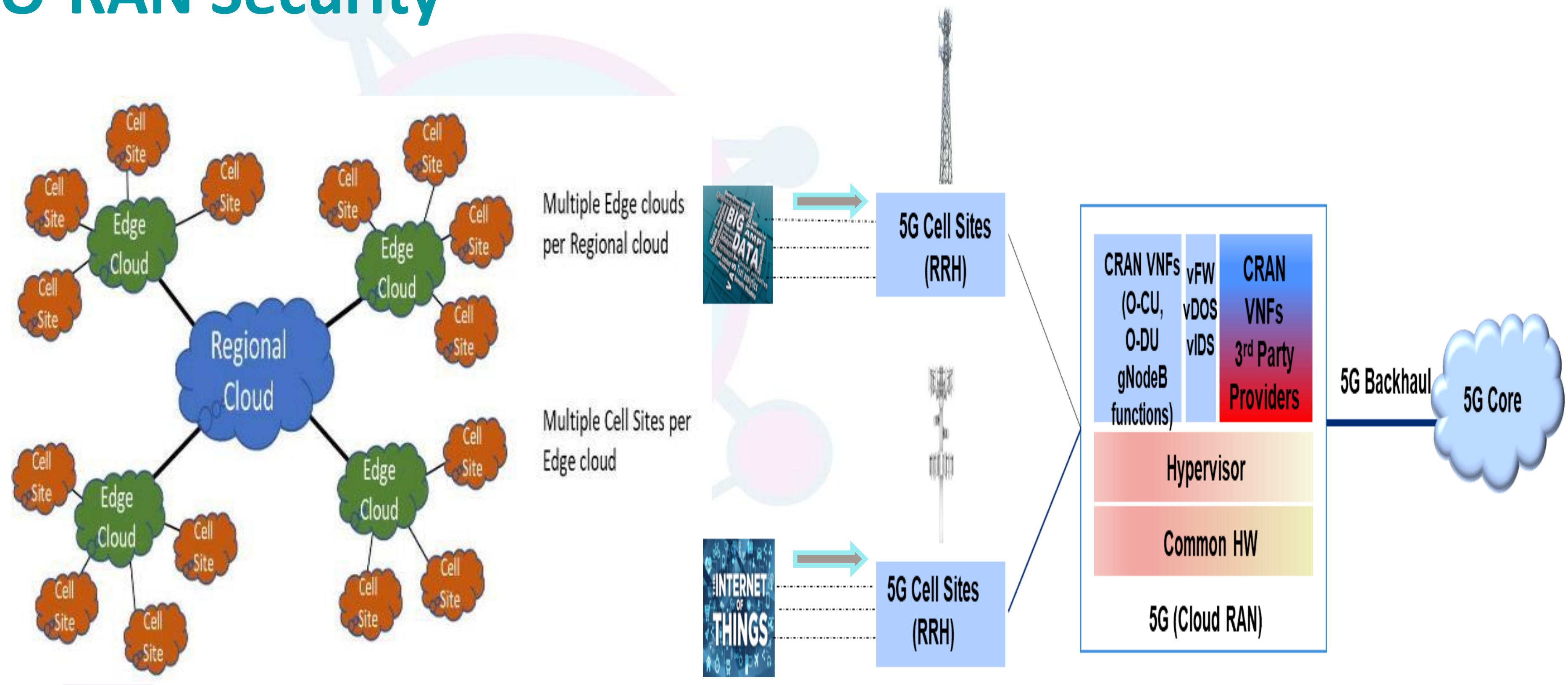


Network Slicing – Security Opportunities, Challenges, Mitigation, and Risks

Security Opportunities	Potential Security Challenges	Potential Mitigation	Risk Severity	Threat Likelihood
Network slicing enables service differentiation and meeting end user SLAs. **Isolates highly sensitive contexts or applications** from other non-critical applications Slice specific SLAs enable a **context-aware orchestration and optimization** of security virtual functions. **Slicing reduces security overhead** by avoiding additional layer of authentication	Different security protocols or policies in different slices results in higher probability of attack	• Adequate isolation of slices with different security levels • Separate authentication of a UE accessing multiple slices at once	Medium	Low
	Denial of service to other slices resulting in resource exhaustion	• Capping of resources for individual slices • Ring-fencing resources for individual slices	High	Medium
	Side Channel attacks across slices extract information about cryptographic keys	• Avoid co-hosting the slices with different levels of sensitivity on the same hardware • Hypervisor hardening	High	Low
	Sealing between slices when the UE is attached to several slices	• Security monitoring mechanisms should exist in the network and potentially in UE.	High	Medium
	Impersonation attacks against a network slice instance within an operator network	• All virtual functions within a Network Slice instance need to be authenticated and their integrity verified.	Medium	Low

High Medium Low

O-RAN Security



Ref: O-RAN Alliance White Paper

O-RAN - Security Opportunities, Challenges, Mitigation and Risks

Security Opportunities	Security Challenges	Potential Mitigation Techniques	Risk Severity	Threat Likelihood
Programmability and Virtualization of RAN will adapt to dynamic nature of traffic and multi provider access SoftRAN (cRAN) in 5G networks will have **embedded DDoS detection and mitigation** functions **Dynamic Radio Resource Scheduling** significantly reduces the risk of jamming attacks targeting mission critical devices **Correlation of control plane and data plane traffic** will enable security monitoring of traffic via correlation	DDOS (Distributed Denial of Service) attack will result in resource starvation at cRAN Virtual Network Functions due to instantiation of additional vFirewalls	• Intelligent VM resource allocations • Capping of resources • Scale up functionality • Security monitoring at the edge	🟠	🟠
	VM (Virtual Machine) manipulation, Data exfiltration due to virtualization	• Hypervisor Separation • Hypervisor Hardening	🔴	🟠
	Programmable and Software RAN will increase the chance of Man-In-The-Middle Attack at the base station	• Traffic monitoring and closed loop orchestration will detect the attacks and mitigate these attacks	🔴	🟠
	Orchestration attack during scaling up and scaling down of VNFs in the cloud RAN	• Deploy detection and mitigation techniques for orchestration and API-based attacks	🟠	🟢
	Jamming can be launched against control-plane signaling or user-plane data messages	• Deploy DDOS detection, IDS and vFirewall functions • Dynamic Service Chaining • Access Class Barring	🟠	🟢

🔴 High 🟠 Medium 🟢 Low

Open Source Security

Open Source Advantages

- flexibility and agility
- faster time to market
- cost-effectiveness
- experimentation
- accelerate innovation
- solid information security
- attract better talent
- long-term cost savings
- reduce vendor lock-in the future

Open Source Disadvantages

- level of support
- intellectual property concerns
- lack of documentation/guides
- customization can jeopardize support

International Network Generations Roadmap

Supply Chain Security

Political and Governance

- *Trustworthiness*
- *Avoid predatory trade practices*
- *Acquisition process include environmental standards, human rights etc*

Business Practices Assessment

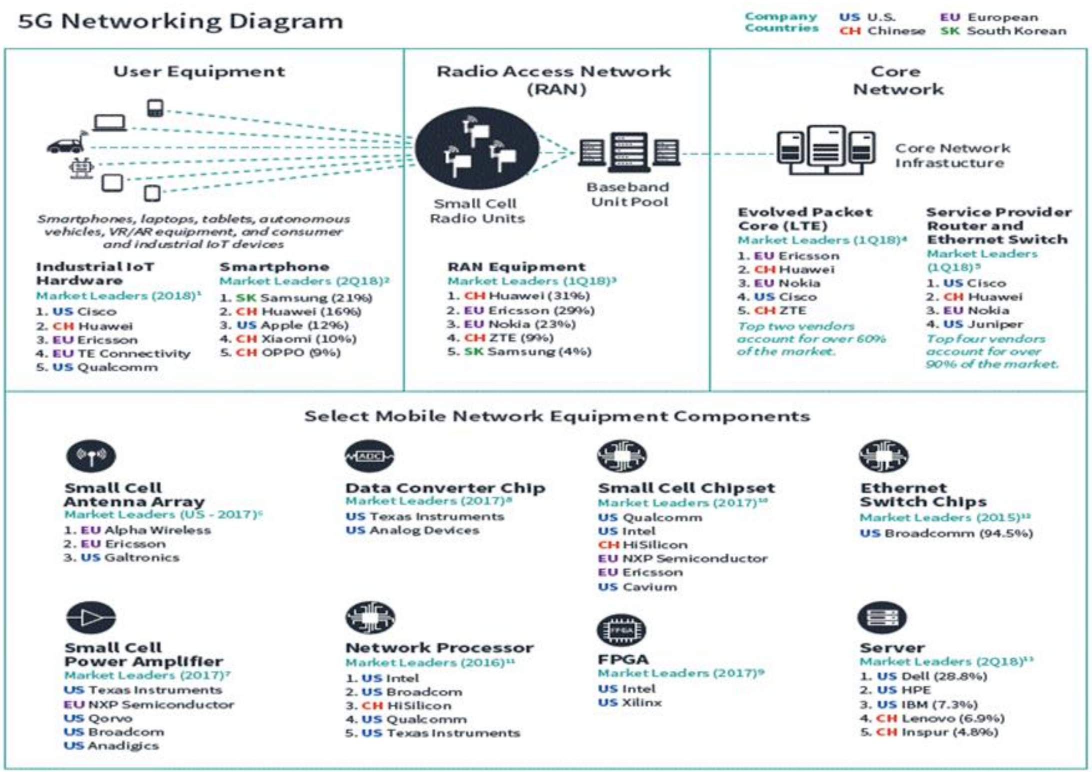
- *Adhere to & observe accounting*
- *Are financed openly and transparently*
- *Adopt best practices in procurement, investment, and contracting*

Cybersecurity Risk Mitigation

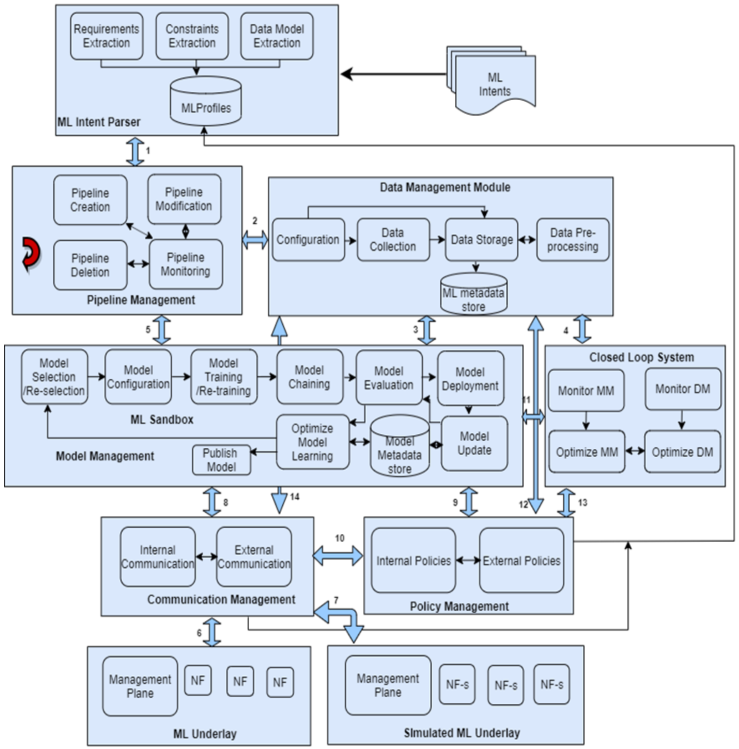
- *Successfully passed independent & credible 3rd party assessment*
- *Products & services are designed, built and maintained according to international standards*
- *Timely & effectively address and remediate security flaws identified by customers*

Government Actions

- *Policy and legal tools to assess supplier's risk profile*
- *Conduct periodic vulnerability assessment with private sector*
- *Support the adoption of best security practices for network operators and the implementation of security measures*



Use Case I: Enabling Technology (AI/ML Security)



Architecture of the Machine Learning Function Orchestrator

AI/ML – Based Security

- **Enhanced Threat Detection for Network Intrusion Detection and Prevention**
  - New models will be developed that can learn from larger sources of data.
- **Online Learning of Threat Models**
  - AI/ML techniques such as GAN and Reinforcement Learning (RL), among other techniques will play an important role in the AI/ML Security Ecosystem.
- **Smart Network Controllers**
  - New algorithms can be loaded in real-time as the threat profile changes.
- **Adaptive and proactive DDOS, Jamming and Spoofing Mitigation**
  - AI/ML models can be used to detect these threats as the continue to evolve.
  - Develop better situational awareness based on the environment that the attacks are taking place.

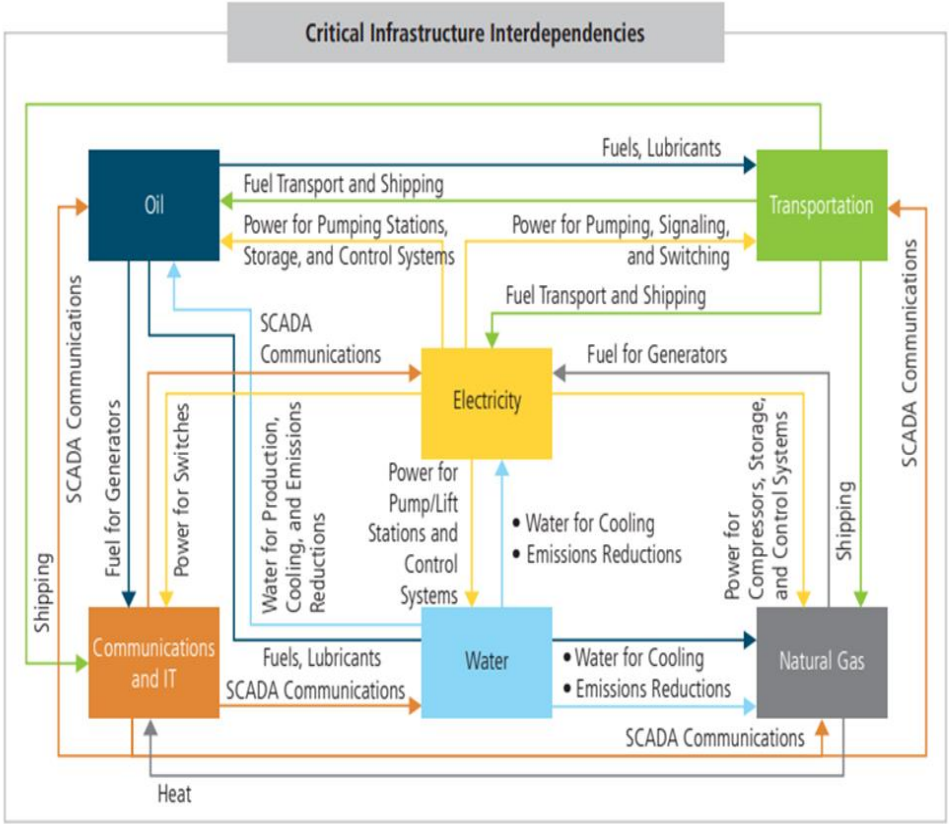
Use Case I: Enabling Technology (AI/ML Security)

	Data Collection	Model Training	Model Inference
Evasion	Adversarial Samples	Network Distillation Adversarial Training	Adversarial Detection Input Reconstruction DNN Model Verification
Poisoning	Data Filtering Regression Analysis	Ensemble Analysis	
Backdoor		Model Pruning	Input Pre-processing
Stealing	Differential Privacy	PATE Model Watermarking	

Security Risks of AI/ML

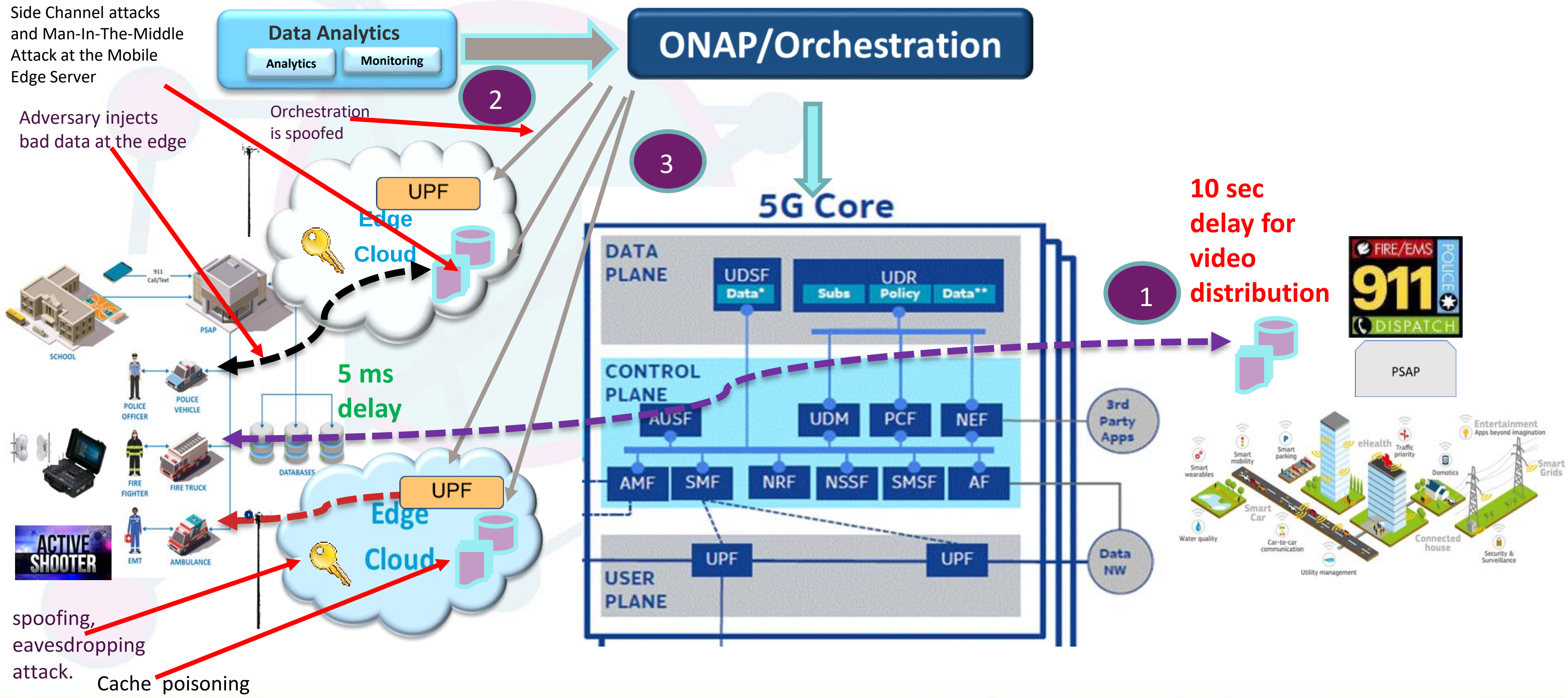
- **Evasion Attacks**
  - attacker modifies input data so that the AI model cannot correctly identify the input.
- **Poisoning Attacks**
  - - The attacker may inject carefully crafted samples to contaminate the training data in a way that eventually impairs the normal functions of the AI system.
- **Backdoor Attacks**
  - Model with a backdoor responds in the same way as the original model on normal input, but on a specific input, the responses are controlled by the backdoor.
- **Model Extraction Attacks**
  - Attacker analyzes the input, output, and other external information of a system to speculate on the parameters or training data of the model.

Use Case II: Application (Smart Grids/SCADA)



- **Transformation:**
  - Driven by innovation in new energy sources, power electronics, data communications and changing regulation
- **B5G and Smart Grids**
  - An important enabler to support next generation power grid architectures and operational models
  - Enhancing data connectivity for power grids holds societal, regulatory and economic value
  - Situational awareness, advanced automated controls and protection, reliability and resilience can be significantly enhanced using 5G technologies
  - Edge and network slicing use-cases
- **B5G and Smart Grid Security**
  - Cyber-physical security and resilience
  - Adaptive and proactive security controls
  - Closed-loop security-aware applications

Use Case III: Application (Public Safety – Active Shooter)

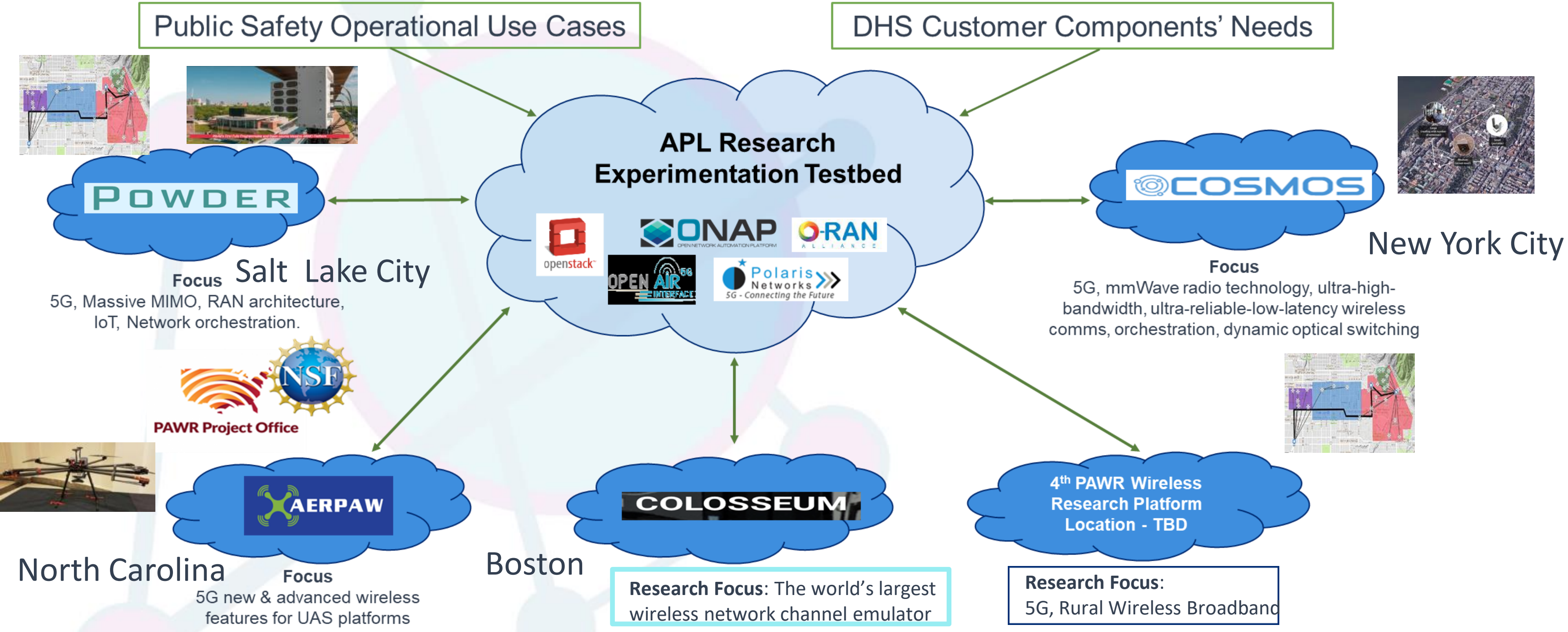


Automation instantiates edge cloud to support ultra low latency and priority applications but exposes additional communication and platform related threats that need to be investigated.

Relevant SDN/NFV/5G Standards Organization

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
IEEE	IEEE Future Networks Initiative, IEEE 802.11 ax/ac/ay
ONF	OpenFlow SDN Controller Standards
OPNFV	NFV Open Platform/eCOMP/OPNFV Community Test Labs
OAI	5G Open Source Software Alliance
OpenDaylight	Brownfield SDN Controller Open Source
ONOS	OpenFlow SDN Controller Open Source
Open RAN Alliance	Open and Interoperable RAN Virtualization
KVM Forum	Hypervisor
NSF PAWR Testbed	COSMOS (NYC), POWDER-RENEW (Salt Lake City), RENEW (NCSU), Rural Broadband (Iowa State)
Linux Foundation	Operating System, Container Security
ITU	The ITU Telecommunication Standardization Sector coordinates standards for telecommunications
ATIS/NIST/FCC/CSA	Regulatory Aspects of SDN/NFV/5G

NSF/PAWR/APL/DHS S&T Partnership – An Example



Operational use cases and customer components drive research initiatives, test bed capabilities and feature priorities that result in increased knowledge of 5G technologies and their impact to the DHS S&T Community

Summary

- Network needs to be designed to be adaptable, resilient, and flexible to support emerging applications
- 5G network gives rise to additional security pillars that offer both in-built security opportunities, and challenges
  - Opportunities: Resiliency, Automation, Isolation of mission critical applications, edge detection
  - Challenges: Side Channel attacks, inter-slice communication, resource starvation, orchestration attacks
- A systematic approach to threat analysis and threat taxonomy is essential to understanding associated risks and mitigation techniques
- A careful analysis of existing security controls is necessary to investigate the gaps in mitigating new threats
- Implement best current practice to augment security controls to mitigate the risks associated with new threats
- Collaboration among operators, vendors, regulators and academia is essential
- Standards, Testbeds and POCs act as catalyst for 5G and beyond evolution

Contact Information

For questions about the INGR, please contact: 5GRoadmapInfo@ieee.org

International Network Generations Roadmap (INGR) Leadership Team:

- IEEE Future Networks Initiative Co-chairs:
  - Ashutosh Dutta – ad37@caa.columbia.edu
  - Timothy Lee – tt.lee@ieee.org
- IEEE International Network Generations Roadmap Co-chairs:
  - Chi-Ming Chen – chimingchen_ieee@yahoo.com
  - Rose Hu – rose.hu@usu.edu
  - Paolo Gargini – paologargini1@gmail.com
  - Narendra Mangra - nmangra@ieee.org
- IEEE Program Director, Future Directions
  - Brad Kloza – b.kloza@ieee.org
- IEEE INGR Project Manager
  - Matthew Borst <m.borst@ieee.org>

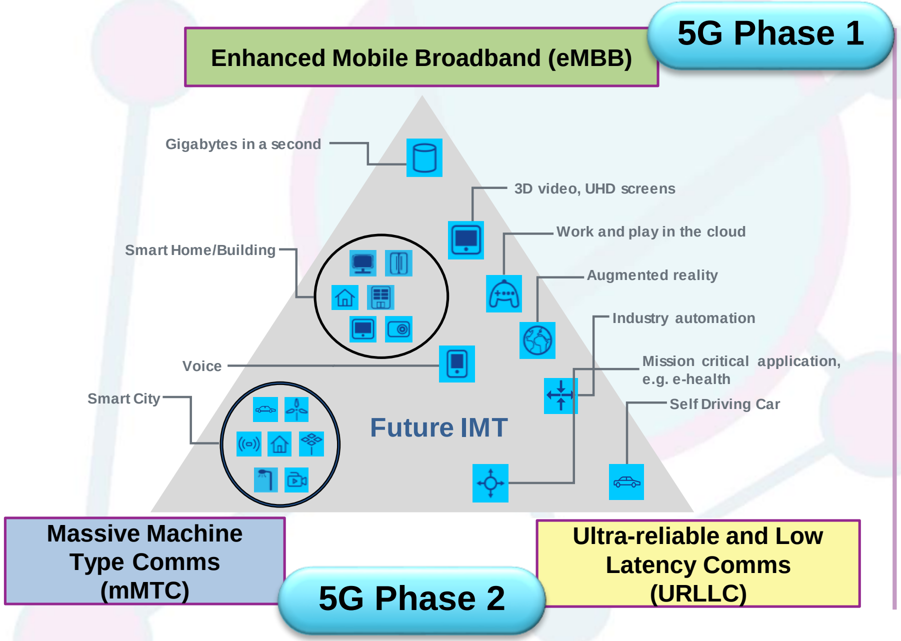
THANK YOU

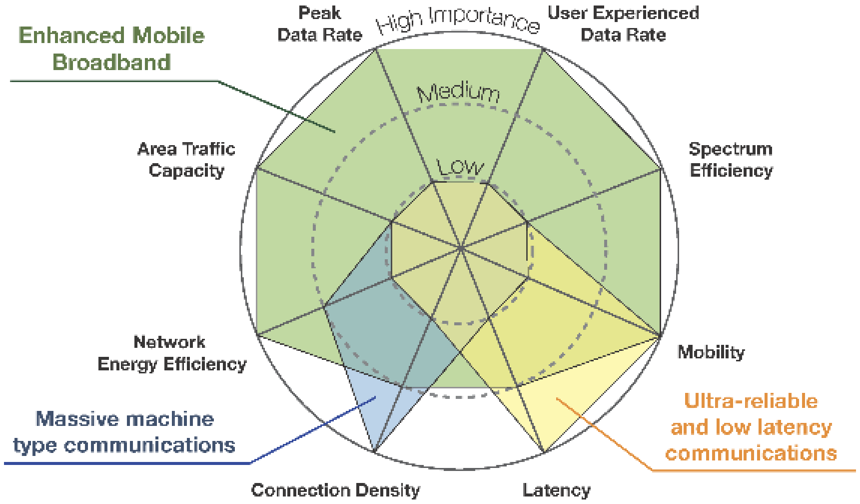
and

JOIN US FOR THE INNOVATION REVOLUTION

Additional Slides Section

5G KPIs, Use Cases & Verticals





Three high-level use cases defined by ITU & endorsed by 3GPP

Ref: ITU-R Recommendation M.2083-0, "IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond," Sept 2015.

Key Points for 5G Adoption and Usage

Technical Barriers

- Densification of Cells
- Spectrum Sharing
- Flexible Networks
- Short range communication
- Security
- Spectrum
- Heterogeneous Mobility Support

Cultural Barriers

- Health and Safety
- Environmental Issues
- Digital Divide
- Legacy Network

RF

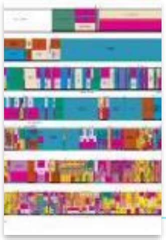
- Performance issues
- Backhaul and mid-haul
- Co-existence with Satellite networks

Policy Barriers

- Vendor Interoperability
- Supply chain issues
- Roaming among operators
- Spectrum Interoperability

Complexity

- Transition and co-existence
- Core Network Architecture
- SDN/NFV Deployment
- Micro Services
- Open Source



Spectrum

- Dynamic Spectrum Sharing
- Use of Low-Band, Mid-Band and High-Band
- Use of Unlicensed band

Physical Layer Security (PLS)

Radio channel and hardware Entropy:
PLS explores exploiting both the communication radio channel and the hardware as sources of uniqueness or of entropy. It is usually this second aspect of PLS that is considered in the literature, around the concept of the secrecy capacity and of the secret key generation capacity. As a source of uniqueness, we can leverage PHY by using RF fingerprinting and high precision localization and/or physical unclonable functions for authentication purposes. In essence, as the line of sight conditions and the channel quality changes, there is a clear interplay between the use of the CSI for high precision localization (i.e., as an authentication factor) or as the means to distil entropy for use in confidentiality and integrity schemes. This unique setting can only be exploited with enhanced monitoring of the wireless channel and of the context in general. Overall, PLS can provide information-theoretic security guarantees with lightweight mechanisms (e.g., using Polar or LDPC encoders) as opposed to computationally expensive elliptic curve-based cryptography. At the same time, it is more probable that PLS will be incorporated in hybrid PLS-crypto systems along with symmetric key block ciphers to sustain reasonable communications rates or will act as an extra security layer, complementing other approaches.
In the longer 10-year perspective, the foundational work of formally interconnecting PLS and semantic security can be envisioned by characterizing the predictability / unpredictability of the channel coefficient realizations in the three dimensions of time, frequency and space, as unpredictability is related to indistinguishability, a central concept in crypto proofs.