IEEE Future Networks

Enabling 5G and Beyond

International Network Generations Roadmap (INGR)

Virtual Industry Forum

Security Working Group

Ashutosh Dutta, Eman Hammad
Co-Chairs

15 October 2020

IEEE

Scope

The working group scope fundamentally addresses the following:

- **5G security considerations need to overlay and permeate through the different layers of the 5G systems** (physical, network, and application) as well as different parts of an E2E 5G architecture including a risk management framework that takes into account the evolving security threats landscape.

- **5G exemplifies a use-case of heterogeneous access and computer networking convergence, which extends a unique set of security challenges and opportunities** (e.g. related to SDN/NFV and edge cloud, etc.) to 5G networks. Similarly, 5G networks by design offers potential security benefits and opportunities through harnessing the architecture flexibility, programmability and complexity to improve its resilience and reliability.

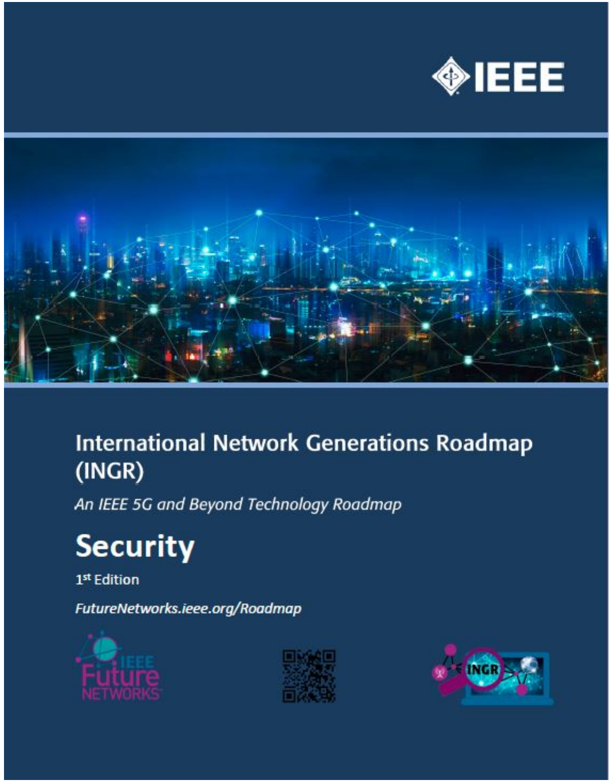
- **The IEEE FNI security WG's roadmap framework follows a taxonomic structure, differentiating the 5G functional pillars and corresponding cybersecurity risks.** As part of cross collaboration, the security working group will also look into the security issues associated with other roadmap working groups within the IEEE Future Network Initiative.

Highlights from First Edition

First Edition of Security Working Group was published in December 2019

- 3-Year, 5-Year and 10-Year Roadmap
- Today's Landscape
- Ongoing Standards Efforts
- Linkages and Key Stakeholders
- Needs, Challenges, Enablers, and Potential Solutions
- Future State

https://futurenetworks.ieee.org/roadmap/ingr-edition-1-2019/



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			
Management and Orchestration Security	Optimization/orchestration security			
	SDN security			
	Network slicing			
Edge Security				
Third Party Security	Supply chain security			
	Open source/application programming interface (API) security			
Hardware Security				

10-year Vision

Domain	Sub-domain	1st Ed. Coverage	2nd Ed. Coverage	Future editions
Radio Interface & Satellite Security				
Data Security and Privacy				
Predictive Security/ Monitoring & Analytics	Proactive security for 5G and IoT (Internet of Things)			
	Digital forensics solutions for 5G environments			
	AI/ML Security			
Use-case	Critical Infrastructure Systems			
	Emergency and first responder networks			
	Smart City (e.g. intelligent transportation)			

Key Pillars of "5G and Beyond" Security

SDN Security

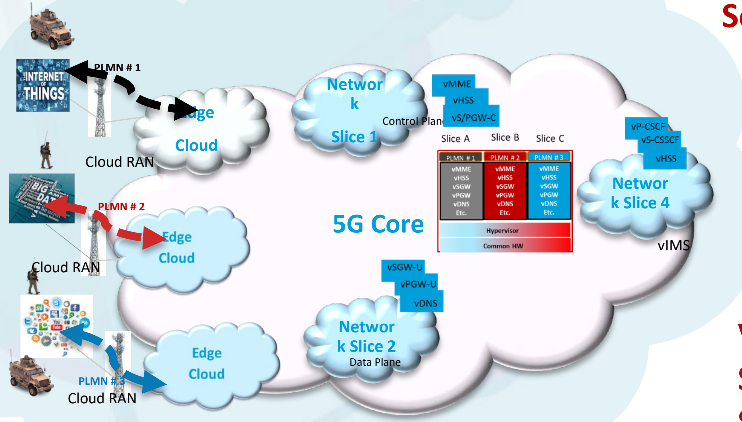
Virtual RAN Security

Open Source / API Security

Edge Security

Network Slicing Security

Supply Chain Security



Virtualization / Softwarization Security

Predictive Security / Monitoring and Analytics

Optimization / Orchestration Security

Data Security and Privacy

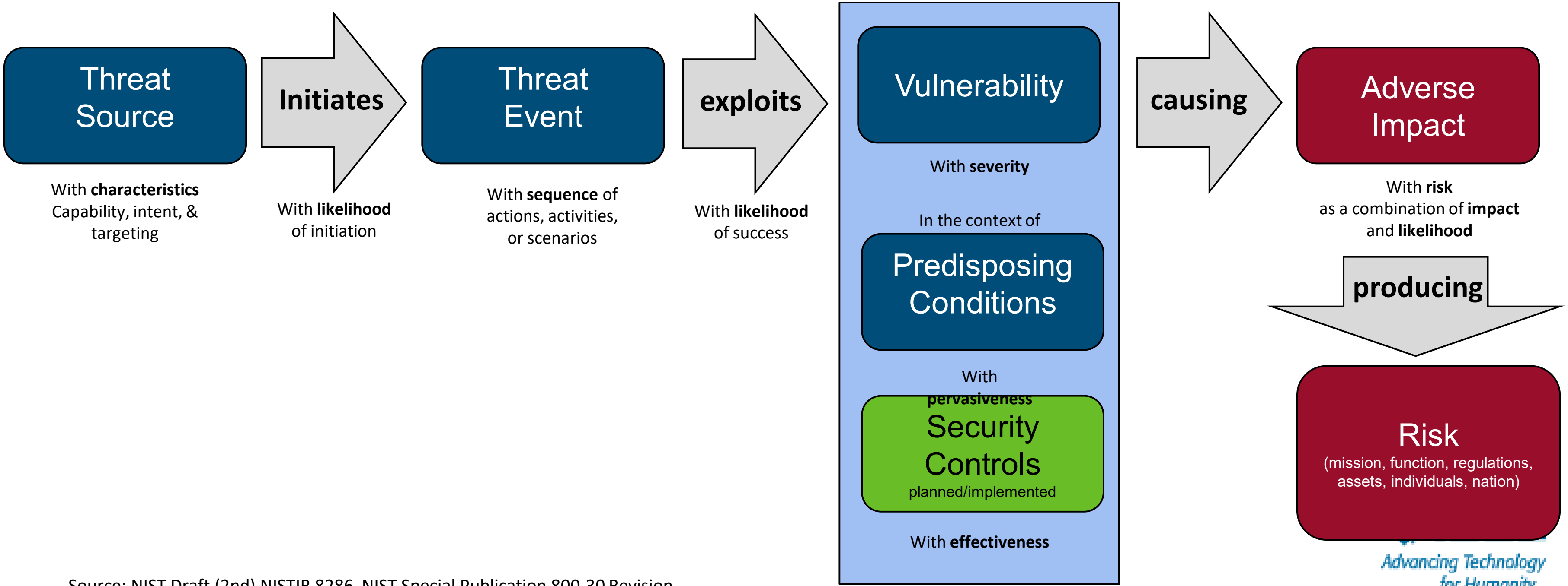
Systematic Approach: Cyber Risk Assessment & Management

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

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

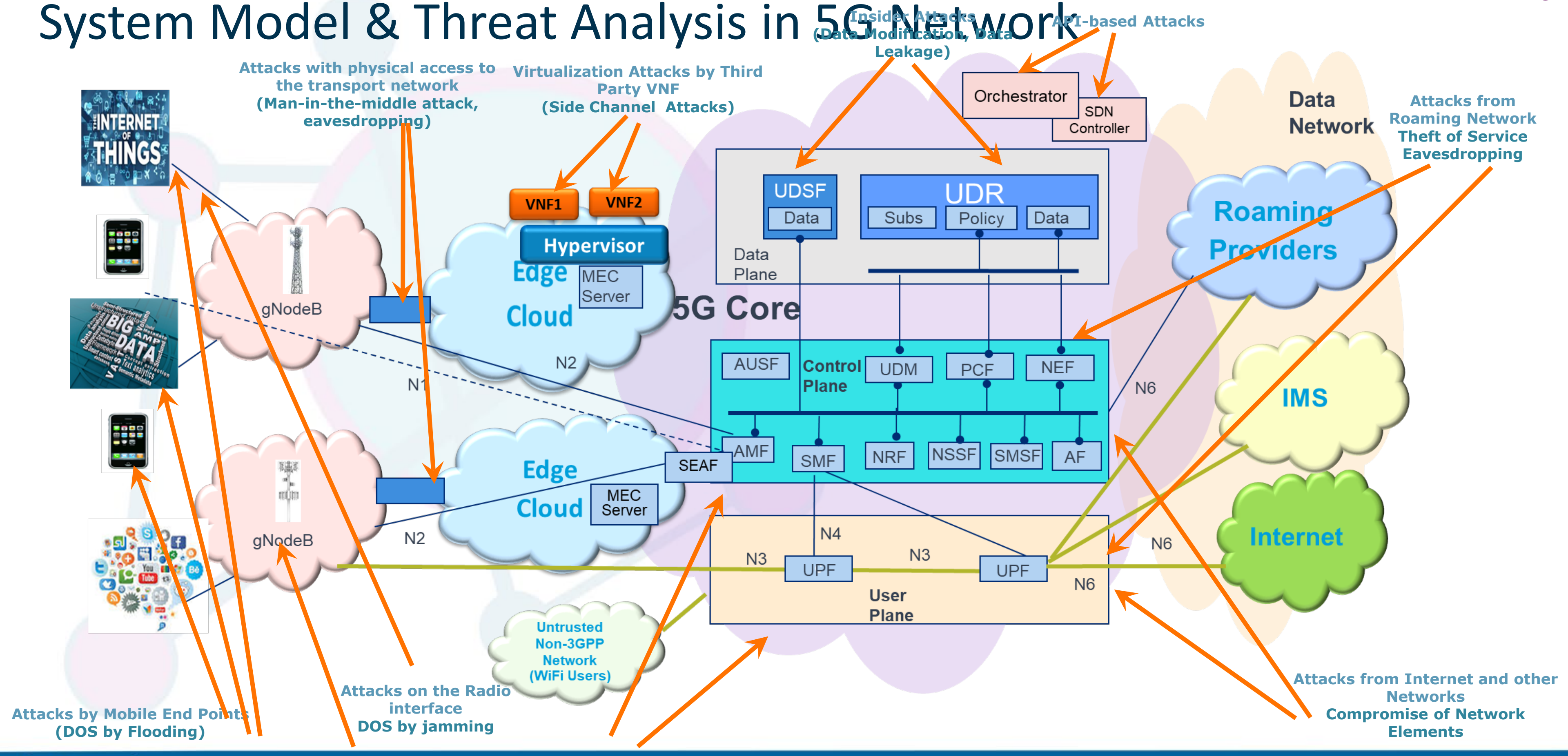
https://www.balbix.com/insights/cyber-risk-heat-map/

Risk Assessment & Management



Source: NIST Draft (2nd) NISTIR 8286, NIST Special Publication 800-30 Revision 1

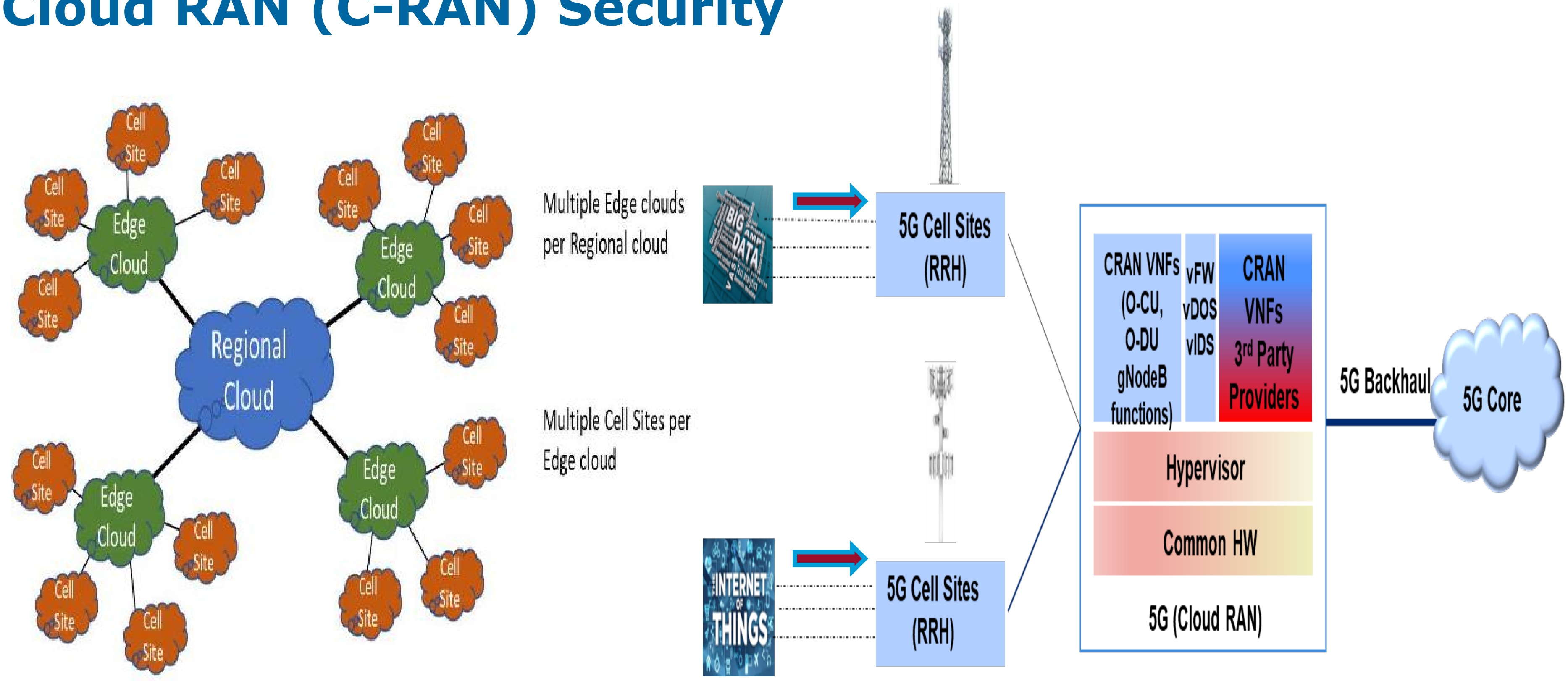
System Model & Threat Analysis in 5G Network



5G Threat Taxonomy

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 exploits a flaw to use services without being charged

Cloud RAN (C-RAN) Security



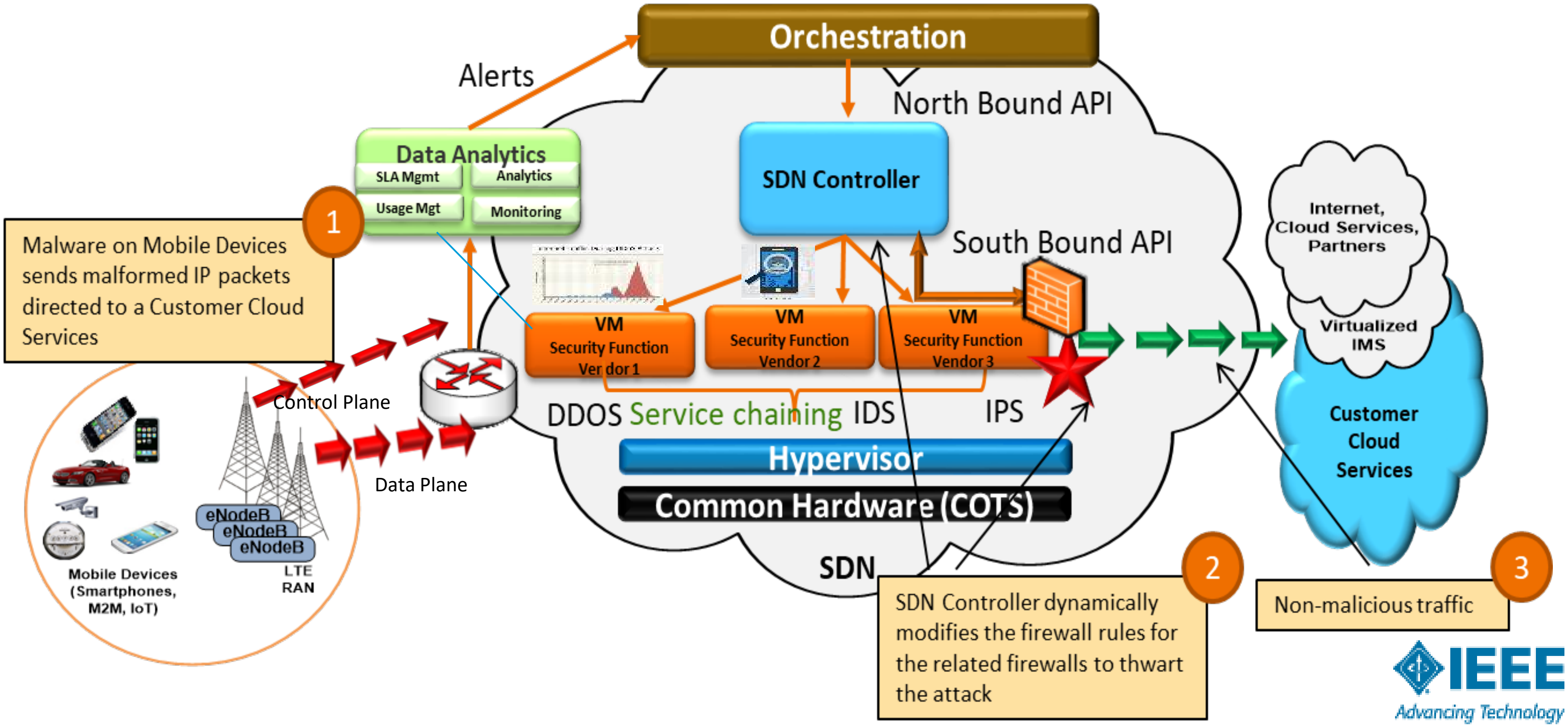
Ref: O-RAN Alliance White Paper

Cloud 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		

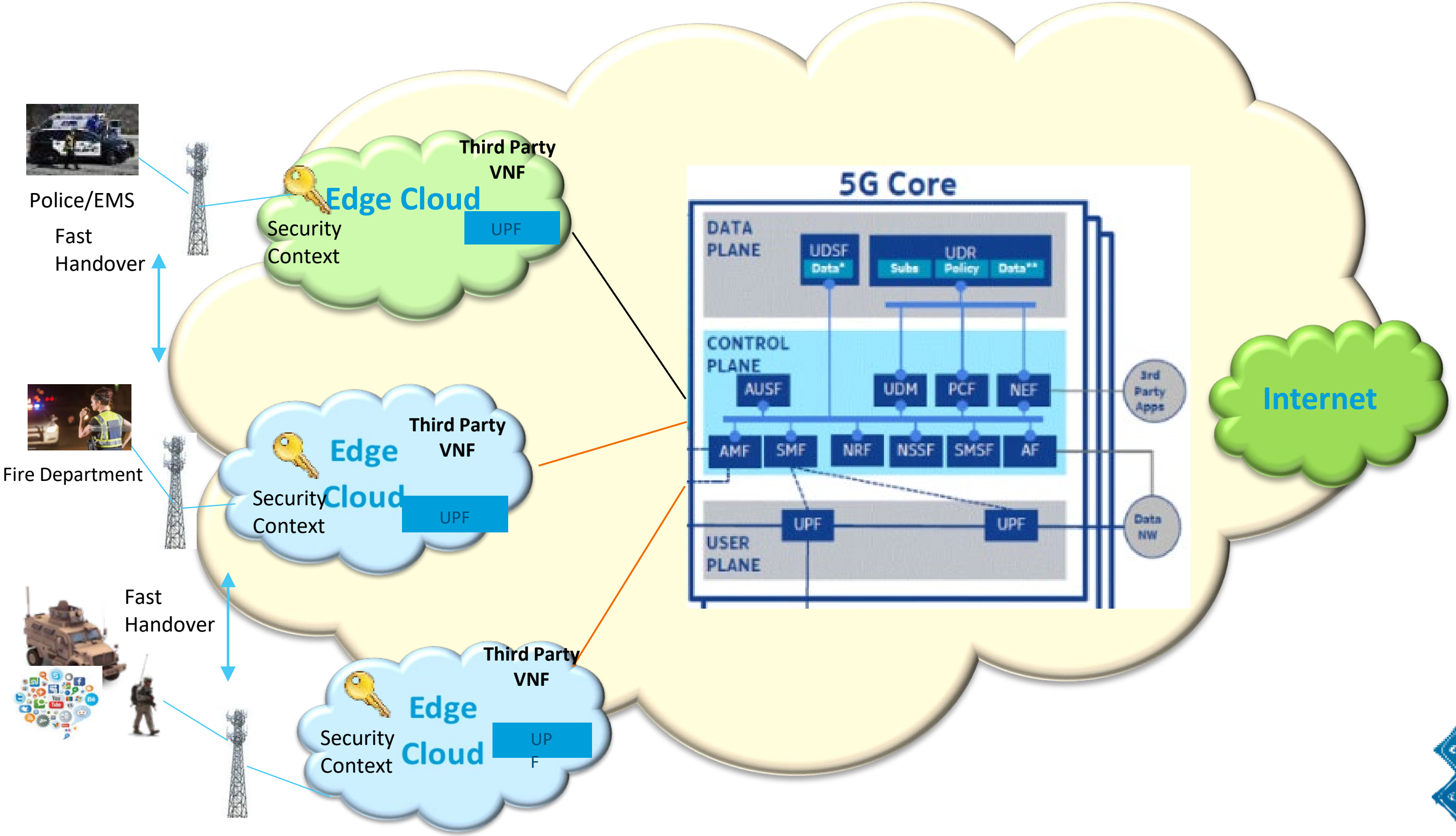
High Medium Low

Security-As-a-Service – Predictive Security with AI/ML



IEEE Advancing Technology for Humanity

Mobile Edge Cloud Security

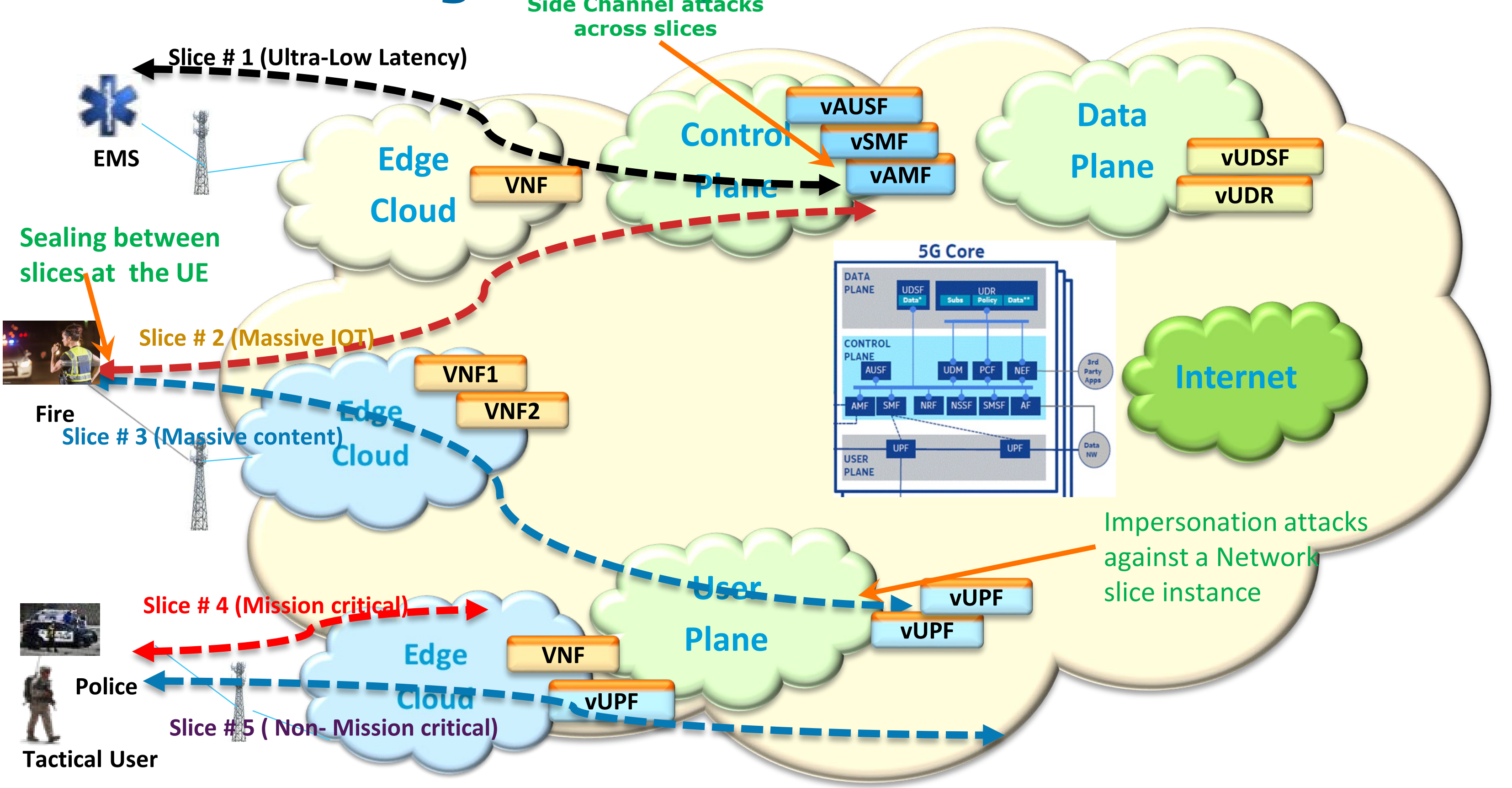


Mobile Edge Cloud - Security Opportunities, Challenges, Mitigation and Risks

Security Opportunities	Security Challenges	Potential Mitigation Techniques	Risk Severity	Threat Likelihood
Embed Security monitoring at the Edge of the network	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		
Application aware **performance optimization**	Storage of security context at the edge can lead to malicious spoofing attack	• Apply proper encryption mechanisms for the security context at the edge		
Reduced latency by way of edge authentication for time sensitive applications	User plane attacks in mobile edge including cache poisoning, cache overwhelming	• Access Control • Hardening Mechanism • Investigate the new security implications		
Secured and fast data offloading during handover	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



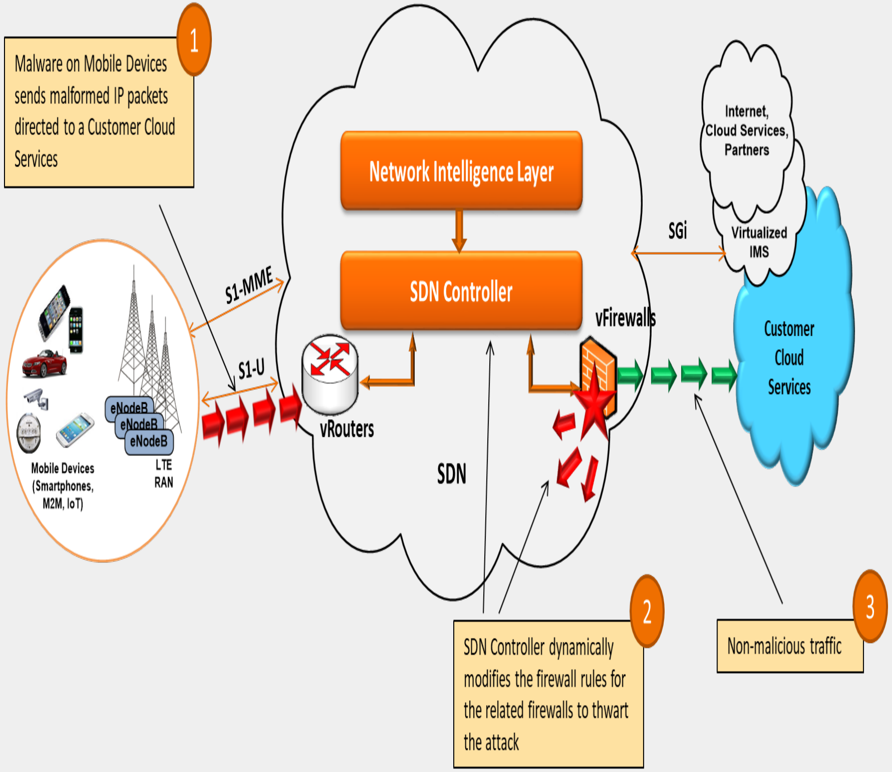
Network Slicing – Security Opportunities, Challenges, Mitigation, and Risks

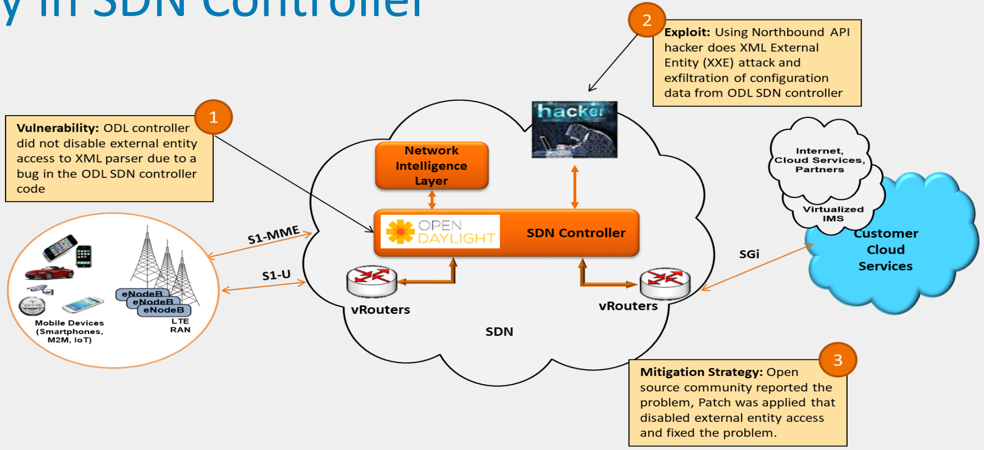
Security Opportunities	Potential Security Challenges	Potential Mitigation	Risk Severity	Threat Likelihood
Network slicing enables service differentiation and meeting end user SLAs. **Isolates highly sensitive contexts or applications** from other non-critical applications Slice specific SLAs enable a **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

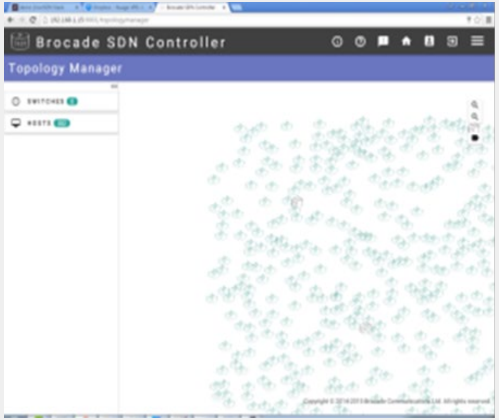
High Medium Low

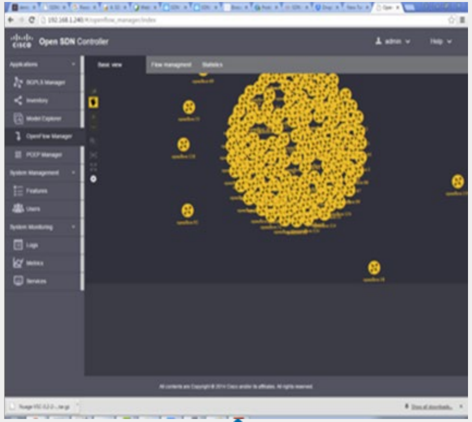
IEEE Advancing Technology for Humanity

Security Opportunities and Vulnerability in SDN Controller









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

Security Opportunities	Potential Security Challenges	Potential Mitigation	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

Technology Challenges (1/2)

- Identity and access management is essential in the end-to-end security of 5G. Future evolution of identity management to enable use-cases such as URLLC will require the development of fast and reliable distributed authentication.
- Edge computing is instrumental to enable 5G agnostic connectivity and use-cases. Standards development for edge devices must evolve to enable tampering proofing, API security, etc.
- Standards and policy development regarding encryption and certificate management in 5G needs to evolve to ensure a seamless user experience for the different use-cases and across carriers/slices.
- Cross-layer development incorporating security constraints in the design must be adopted in a top-down approach for 5G resilient on the system level.
- ML/AI will be increasingly used in 5G orchestration functionalities (SDN/NFV). Security monitoring and anomaly detection of ML/AI algorithms is still not developed.
- Lack of reliability and scalability for Open Source software and APIs that are used to support foundational 5G capabilities (SDN/NFV)
- Adaptive SDN/NFV would need to be further defined and developed to incorporate cyber risk and support multiple security contexts.

Technology Challenges (2/2)

- Further development is required in trust platforms that are computationally feasible and tamper proof. This would help establish trust in supply chain (hardware/software).
- Cyber hardware/software testing and verification to detect malicious executables/backdoors/unapproved functionality must evolve and continue to evolve.
- Scalability of security controls & solutions: e.g. PKI key management, DDoS protection, etc.
- Robustness & Trustability of algorithms (ML/AI, encryption) against an evolving technology and adversary models
- Distribution of security contexts
- Cross-layer and cross-domain security requirements
- High uncertainty on anticipated new vulnerabilities and attack vectors
  The right balance between automation and human-augmented threat/attack detection and response

Security Chapter: Linkages and Stakeholders

- Linkages (other INGR roadmap working groups)
  - Edge Automation Platform Group
  - Massive MIMO & mmWave
  - 5G Testbed
  - Optimization
  - Applications & Services
  - Standards
  - AI/ML
  - Systems Optimization
  - Satellite

- Stakeholders (Who should read this report)
  - Security will provide input and guidance for all stakeholders including: carriers, service providers, vendors, end-user applications and services, government agencies (DARPA, DoD, etc.), and various verticals, (e.g., R&D (academia, industry)

Next Steps: Working Group Activities

- Meet at Bi-Weekly Meetings
- Bring Your Research Ideas, Talks to discuss
- Engage Industry Stakeholder: Industry Webinars to collect input
- Assess what else is going on: Environment Scan Analysis
- Develop security use-cases for various application verticals
- Develop Threat Taxonomy for end-to-end system
- Develop a risk assessment approach for a selected set of unique threats
- Develop E2E System Model
- Align with Cybersecurity Framework
- Develop some Key Security Indicators and map this to some key KPIs

Get involved!

LISTSERV: 5g-roadmap-security@ieee.org

Collabratec Private Group: Security - IEEE 5G Roadmap

Ahmad Cheema	acheema@LAKEHEADU.CA
Ahmed LImam	ahmedlimam@IEEE.ORG
Alex Gelman (Guest for standards)	
Ana Nieto	nieto@LCC.UMA.ES
Anton Kaska	anton.kaska@BOREALIS-TRADERS.COM
Arsenia Chorti	arsenia.chorti@ensea.fr
Ashutosh Dutta	ad37@CAA.COLUMBIA.EDU
Brad Kloza	b.kloza@ieee.org
Colby Harper	colby@PATHFINDERWIRELESS.COM
Dr. david R Varner	David.varner@CENTURYLINK.COM
Eman Hammad	eman.hammad@gmail.com
Fred Chu	fred.chu@adtran.com
Jason Titlow	jaytitlow@gmail.com
John Lester	jdlester@MITRE.ORG
Jong-Geun Park	queue@etri.re.kr
Joseph Bio-Ukeme	joseph.boiukeme@carleton.ca
Julia Urbina-Pineda	julita.up@GMAIL.COM
Kassi Kadio	kadk03@uqo.ca
Khaled Alam	khaledshriar@gmail.com
Kingsley Okonkwo	KOkonkwo@CHEVRON.COM
Linda Wilson	linda_wilson1225@IEEE.ORG
Lyndon Ong	lyong@Ciena.com
Marc Emmelmann	emmelmann@IEEE.ORG
Mona Ghassemian	Chair@ieee-ukandireland.org
Omneya Issa	omneya.issa@CANADA.CA
Prakash Ramchandran	cloud24x7@ieee.org
Rajakumar Arul	rajakumararul@GMAIL.COM
Sanjay S Pawar	drsanjayspawar@GMAIL.COM
Sherri Ireland	sherri@securityexclusive.com
Sireen Malik	Sireen.malik@T-MOBILE.COM
Sivarama krishnan	sivaram26@IEEE.ORG
Suresh Sugumar	suresh.sugumar@ieee.com
Tk Lala	tk2929@GMAIL.COM

Contacts: Security Working Group Co-Chairs

Ashutosh Dutta
ashutosh.dutta@ieee.org

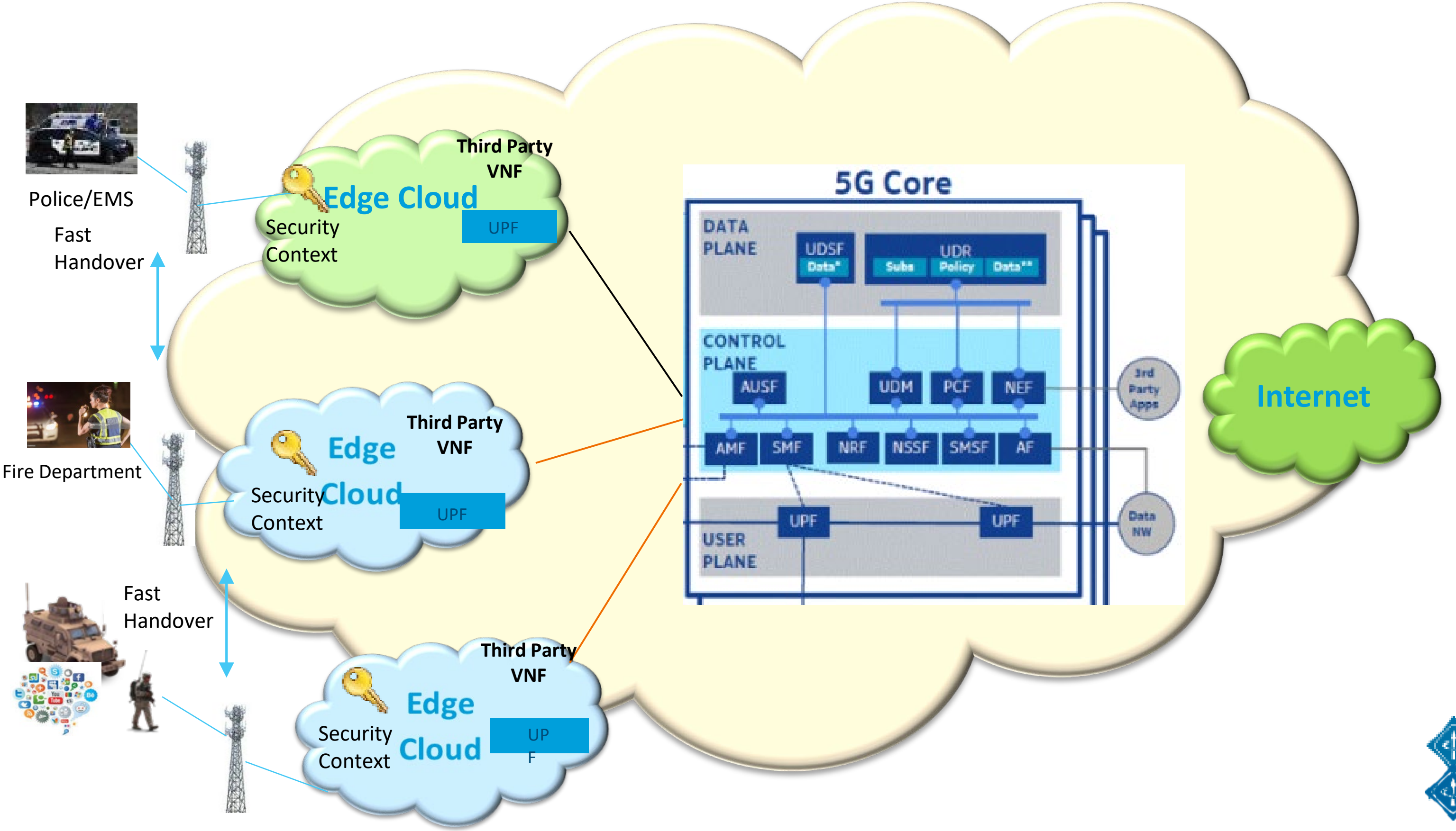
Eman Hammad
eman.hammad@gmail.com

Send mail to 5GRM-security@ieee.org if you would like to join the working group

QUESTIONS?

Additional Slides

Mobile Edge Cloud Security



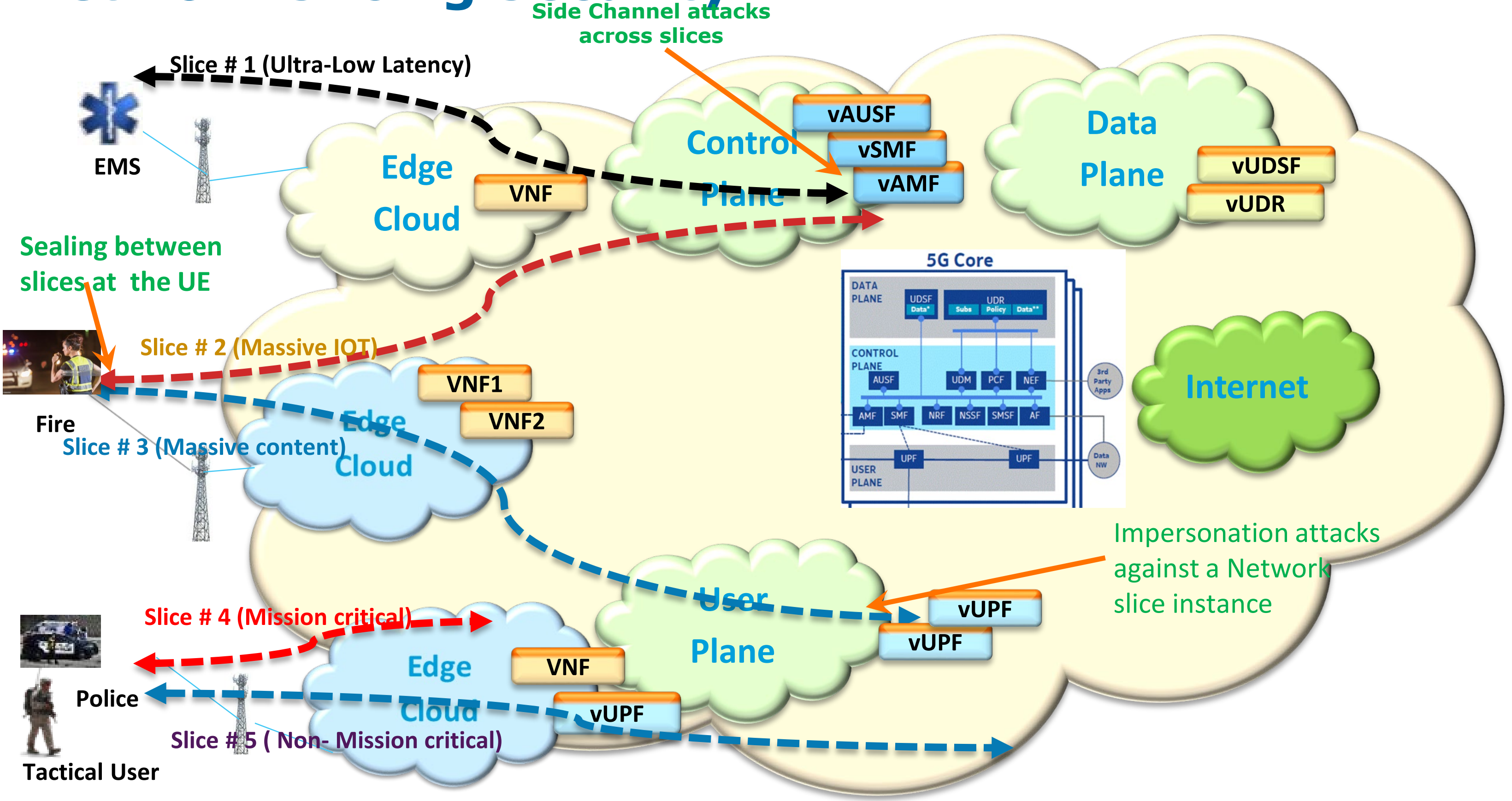
Mobile Edge Cloud - Security Opportunities, Challenges, Mitigation and Risks

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

IEEE
Advancing Technology for Humanity

Network Slicing Security

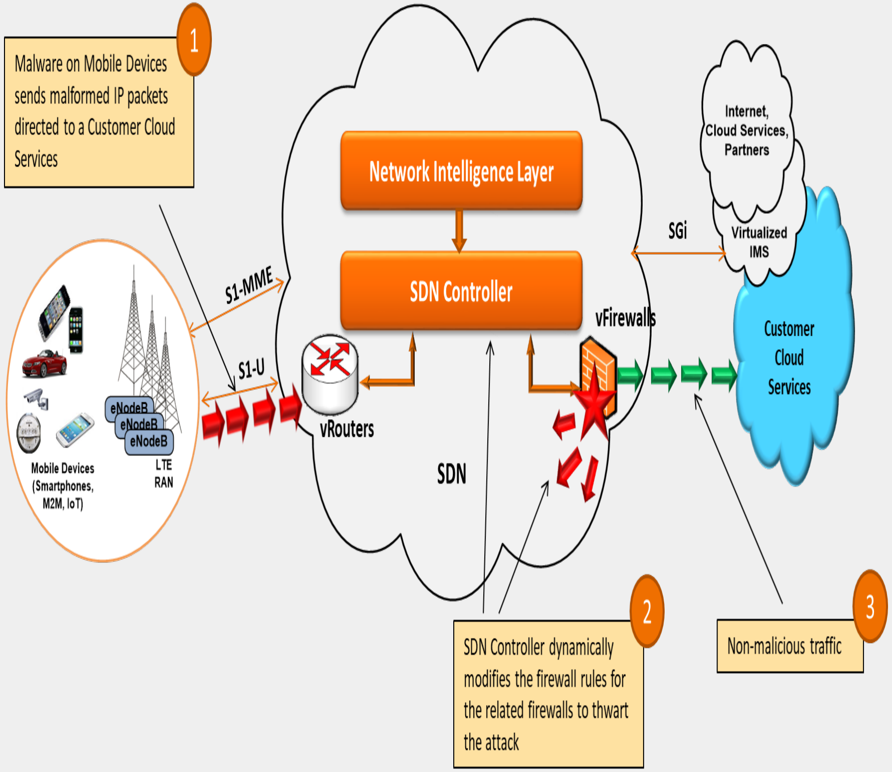


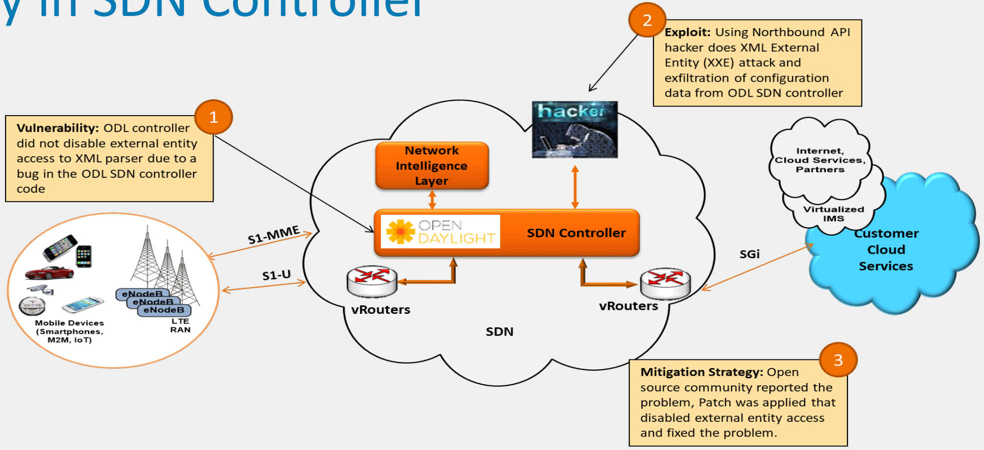
Network Slicing – Security Opportunities, Challenges, Mitigation, and Risks

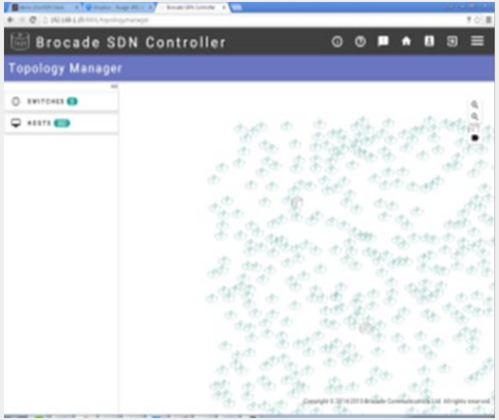
Security Opportunities	Potential Security Challenges	Potential Mitigation	Risk Severity	Threat Likelihood
Network slicing enables service differentiation and meeting end user SLAs.	Different security protocols or policies in different slices results in higher probability of attack	• Adequate isolation of slices with different security levels • Separate authentication of a UE accessing multiple slices at once	🟠	🟢
Isolates highly sensitive contexts or applications from other non-critical applications	Denial of service to other slices resulting in resource exhaustion	• Capping of resources for individual slices • Ring-fencing resources for individual slices	🔴	🟠
Slice specific SLAs enable a **context-aware orchestration and optimization** of security virtual functions.	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	🔴	🟢
Slicing reduces security overhead by avoiding additional layer of authentication	Sealing between slices when the UE is attached to several slices	• Security monitoring mechanisms should exist in the network and potentially in UE.	🔴	🟠
	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.	🟠	🟢

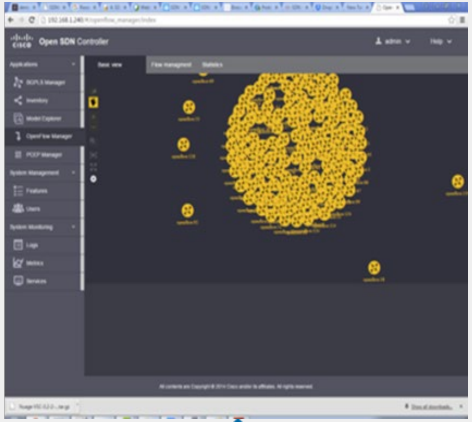
🔴 High 🟠 Medium 🟢 Low

Security Opportunities and Vulnerability in SDN Controller









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

Security Opportunities	Potential Security Challenges	Potential Mitigation	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

Open Source / API Security

Open Source Advantages

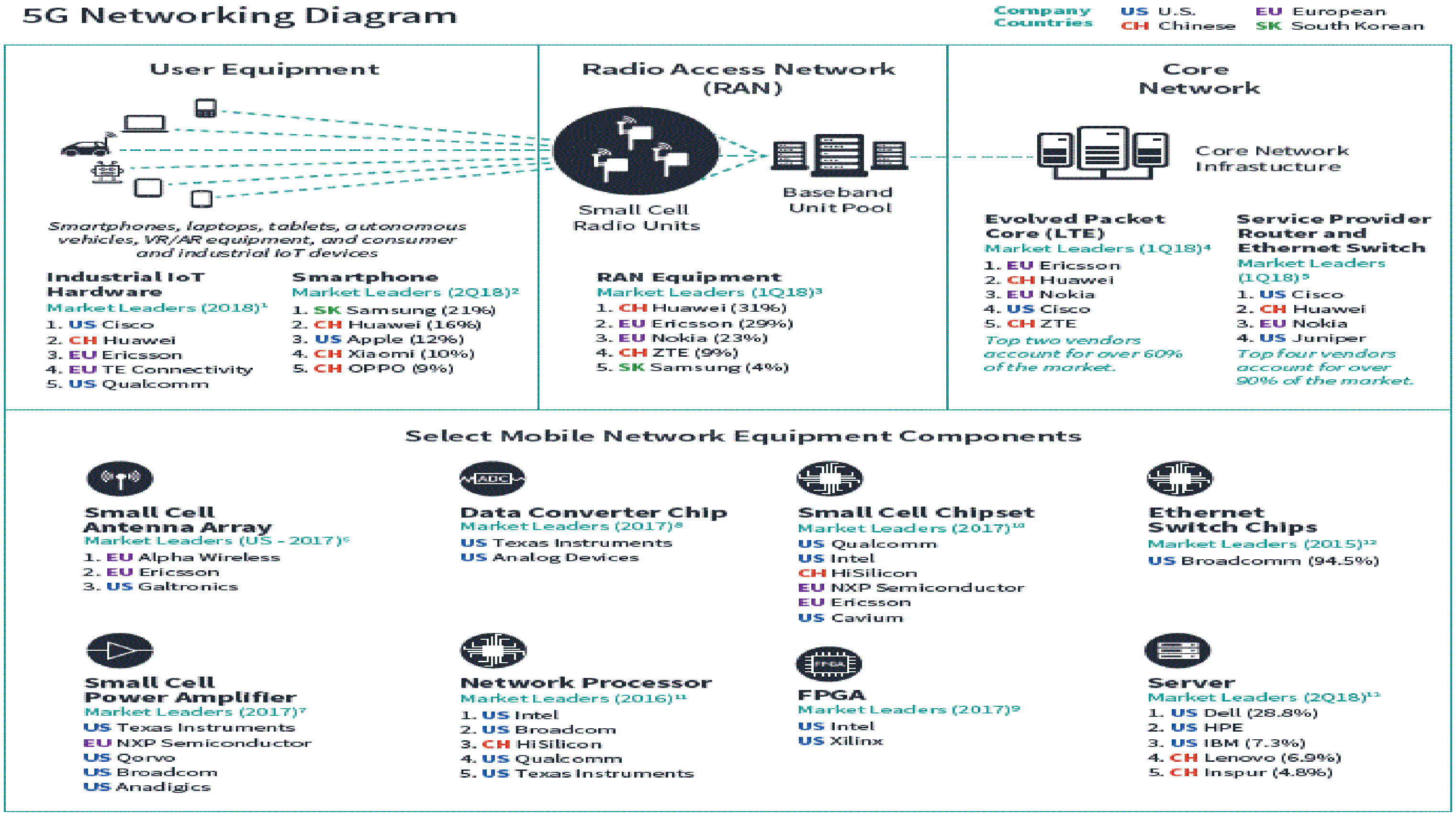
- flexibility and agility
- faster time to market
- cost-effectiveness
- experimentation
- accelerate innovation
- solid information security
- attract better talent
- long-term cost savings
- reduce vendor lock-in
- the future

Open Source Disadvantages

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

support

Supply Chain Security – Equipment Penetration



1: "IoT ONE Connectivity Hardware 10 (2018)," IOT One, https://www.iotone.com/top10-2018/connectivity-hardware
2: "Smartphone Vendor Market Share," IDC, https://www.idc.com/promo/smartphone-market-share/vendor
3: Baburajan K, "RAN market: How Huawei, Ericsson, Nokia, ZTE, Samsung performed," Telecomlead, July 31, 2018, https://www.telecomlead.com/telecom-equipment/ran-market-how-huawei-ericsson-nokia-zte-samsung-performed-85605
4: Mike Robuck, "Report: EPC is pushing network functions virtualization to new heights," Fierce Telecom, June 5, 2018, https://www.fiercetelecom.com/telecom/report-epc-pushing-network-functions-virtualization-to-new-heights
5: "Service Provider Router and Switch Market Falls to a Five-Year Low in 1Q18 According to Dell'Oro Group," June 7, 2018, http://www.delloro.com/news/service-provider-router-and-switch-market-falls-to-a-five-year-low-in-1a18-according-to-delloro-group