IEEE Future NETWORKS

Enabling 5G and Beyond

International Network Generations Roadmap (INGR)

Virtual Workshop

Security Working Group

Ashutosh Dutta, Eman Hammad
Co-Chairs

16 June 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.

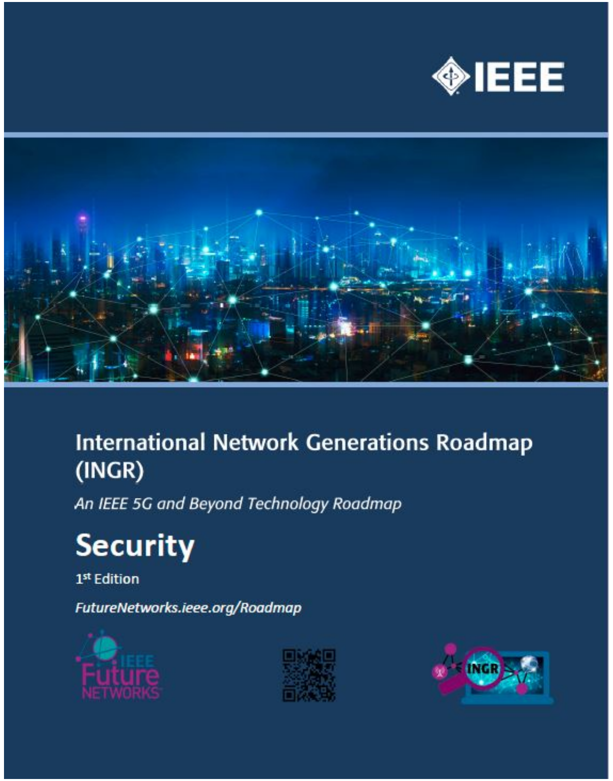
- The IEEE FNI security WG's roadmap framework follows a taxonomic structure, differentiating the 5G functional pillars and corresponding cybersecurity risks. As part of cross collaboration, the security working group will also look into the security issues associated with other roadmap working groups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



IEEE

International Network Generations Roadmap (INGR)

An IEEE 5G and Beyond Technology Roadmap

Security

1st Edition

FutureNetworks.ieee.org/Roadmap

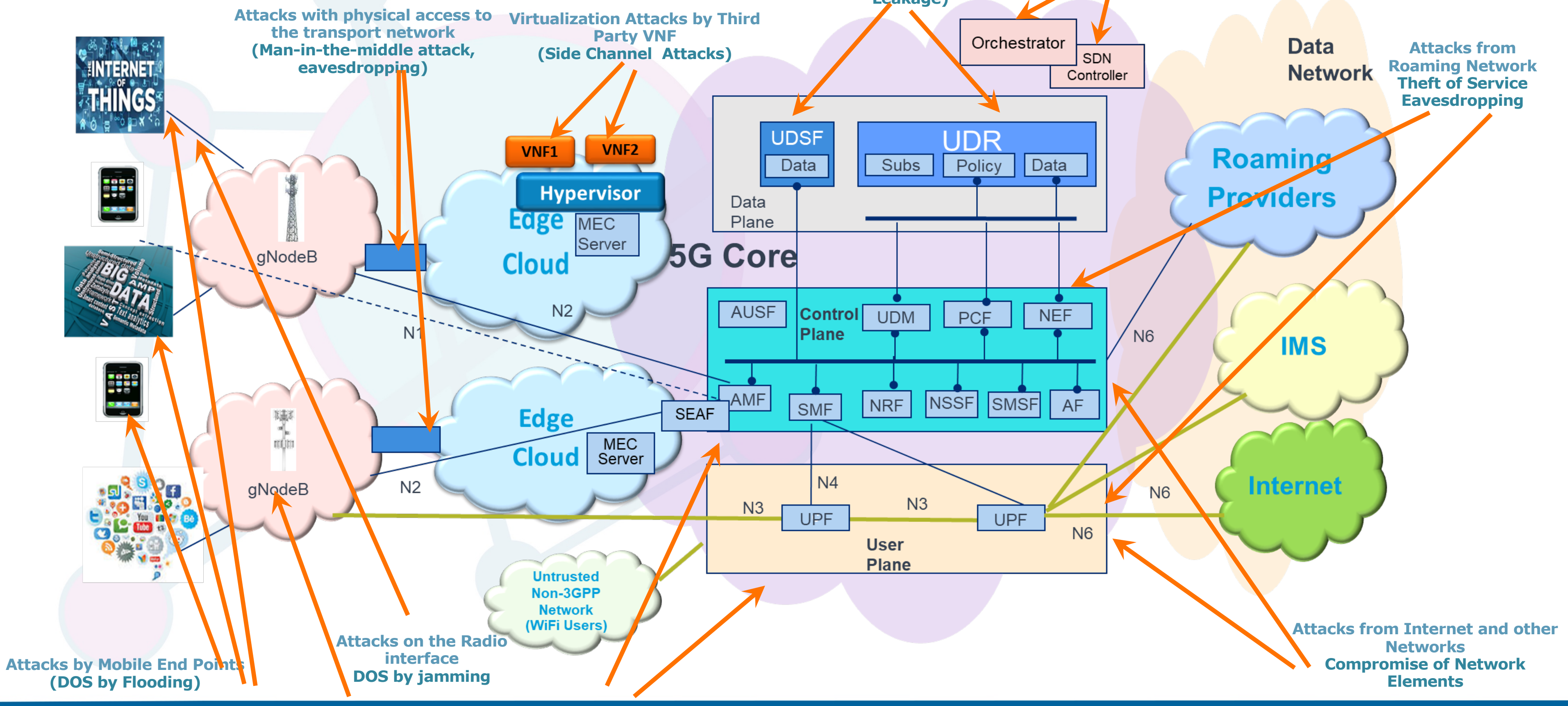
10-year Vision

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)		◕	

System Model & Threat Analysis in 5G Network



Insider Attacks (Data Modification, Data Leakage)

API-based Attacks

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

Virtualization Attacks by Third Party VNF (Side Channel Attacks)

Attacks from Roaming Network Theft of Service Eavesdropping

Attacks by Mobile End Points (DOS by Flooding)

Attacks on the Radio interface DOS by jamming

Attacks from Internet and other Networks Compromise of Network Elements

Attacks from physical access to gNodeB

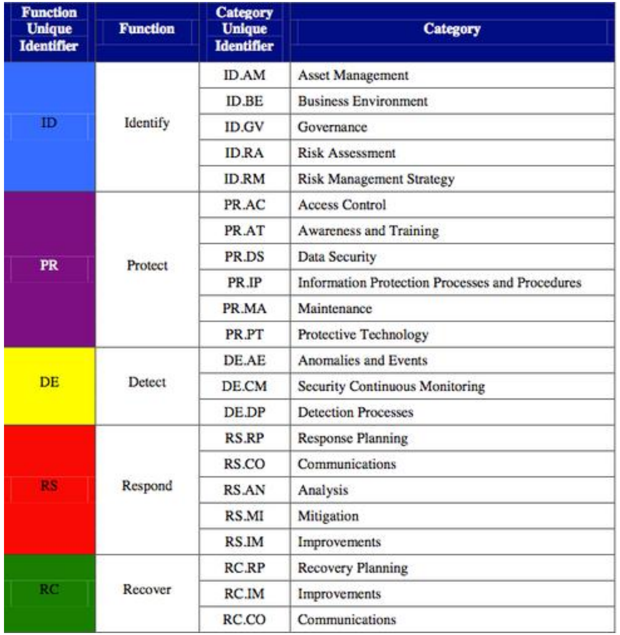
Attacks from untrusted Non-3GPP network

Foundational: Cybersecurity Framework

CYBERSECURITY FRAMEWORK VERSION 1.1
IDENTIFY
PROTECT
DETECT
RESPOND
RECOVER

The working group will be aligning its roadmap items and recommendations with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

- The framework provides a high-level structure and categorization of security control and functions: identify, protect, detect, respond & recover.
- The framework is freely available and is widely adopted.
- https://www.nist.gov/industry-impacts/cybersecurity-framework

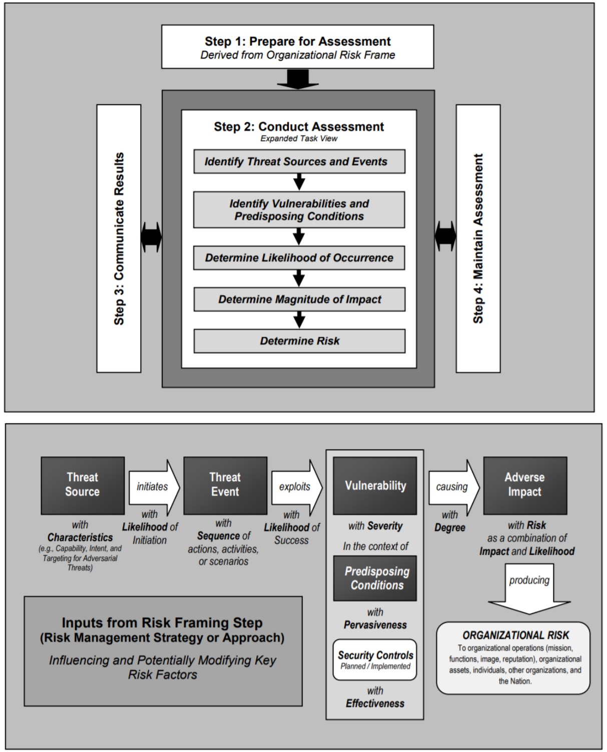


Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	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

Foundational: Risk Assessment & Management

The working group will be aligning its roadmap items and recommendations with the National Institute of Standards and Technology (NIST) Cybersecurity Risk Assessment & Management Guidelines.

- Adopt a cyber risk definition & management framework that supports describing the roadmap 3,5 and 10 years vision and recommendations.
- The guidelines are generic, freely available and compatible with most risk assessment methodologies.
- https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf


Step 1: Prepare for Assessment
Derived from Organizational Risk Frame
Step 2: Conduct Assessment
Expanded Task View
Identify Threat Sources and Events
Identify Vulnerabilities and Predisposing Conditions
Determine Likelihood of Occurrence
Determine Magnitude of Impact
Determine Risk
Step 3: Communicate Results
Step 4: Maintain Assessment
Threat Source
initiates
Threat Event
exploits
Vulnerability
causing
Adverse Impact
with Characteristics
(e.g., Capability, Intent, and Targeting for Adversarial Threats)
with Likelihood of Initiation
with Sequence of actions, activities, or scenarios
with Likelihood of Success
with Severity
In the context of
Predisposing Conditions
with Pervasiveness
Security Controls
Planned / Implemented
with Effectiveness
with Degree
with Risk as a combination of Impact and Likelihood
producing
ORGANIZATIONAL RISK
To organizational operations (mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation.
Inputs from Risk Framing Step
(Risk Management Strategy or Approach)
Influencing and Potentially Modifying Key Risk Factors

NIST Guide for Conducting Risk Assessments

Example: CLOUD RAN Unique 5G Security Opportunities, Challenges, and Mitigation

5G Capabilities	Potential Security Challenges/Risk Scenarios	Potential Mitigation
• The 5G networks will facilitate many more devices (IoT) accessing the RAN with shared access. • Programmability and Virtualization of RAN will adapt to dynamic nature of traffic and multi provider access	• Huge number of infected M2M/IOT devices that attempt to gain access resulting in shared resource starvation, VM/Guest OS manipulation, data exfiltration	• Hypervisor Separation • Intelligent VM resource allocations • vFirewalls
	• Programmable and Software RAN will increase the chance of Man-In-The-Middle Attack at the base station	• Use of analytical techniques like anomaly detection can be leveraged for such analysis
	• Resource starvation at cRAN VNFs by additional vFW functions during DDOS attack	• Hypervisor separation • Capping of resources
	• External flooding attacks may be launched by a botnet consisting of large number of bots and Distributed Denial of Service (DDoS)	• Develop DDoS detection and mitigation mitigation functions into Cloud RAN functions
	• Jamming can be launched against control-plane signaling or user-plane data messages	• Deploy DDOS detection, IDS and vFirewall functions • Dynamic Service Chaining

Potential Security Opportunities/Benefits

- SoftRAN (cRAN) in 5G networks will have embedded DoS detection and mitigation functions
- Dynamic Radio Resource Scheduling would significantly reduce the risk of jamming attacks targeting mission critical devices
- Access to control plane and media plane at the base station will enable security monitoring of traffic

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)

Cross Team Meeting Schedule

To attend: please contact the working group co-chairs & they will share the session details (webex link).

Contacts: Security Working Group Co-Chairs

Ashutosh Dutta
ashutosh.dutta@ieee.org

Eman Hammad
eman.hammad@gmail.com

June 17

Start Time										
8:00 AM	9:00 AM	10:00 AM	11:00 AM	12:00 PM	1:00 PM	2:00 PM	3:00 PM	4:00 PM	5:00 PM	6:00 PM
Apps & Svcs AI ML				Apps & Svcs Deployment		EE Hardware	Apps & Svcs EE		EE Deployment	
			EAP Massive MIMO	EAP Security		EAP Standards	EAP Testbed			
	Satellite Standards	Satellite Testbed		Massive MIMO Hardware		Massive MIMO Deployment	Massive MIMO Standards			Deployment CTU
				Standards CTU	Sys Opt CTU		Security Sys Opt		CTU Testbed	Sys Opt Testbed
					Satellite Security	Satellite AI ML				
			Security AI ML							

June 18

Start Time										
8:00 AM	9:00 AM	10:00 AM	11:00 AM	12:00 PM	1:00 PM	2:00 PM	3:00 PM	4:00 PM	5:00 PM	6:00 PM
	Apps & Svcs Satellite			AI ML EAP	Apps & Svcs EAP			Apps & Svcs Security		Apps & Svcs Sys Opt
	AI ML Massive MIMO				AI ML CTU		EAP EE	EAP Deployment		
					Security Testbed	Standards Testbed	Standards Security		EE Sys Opt	
								AI ML Testbed		

Next Steps: Working Group Activities

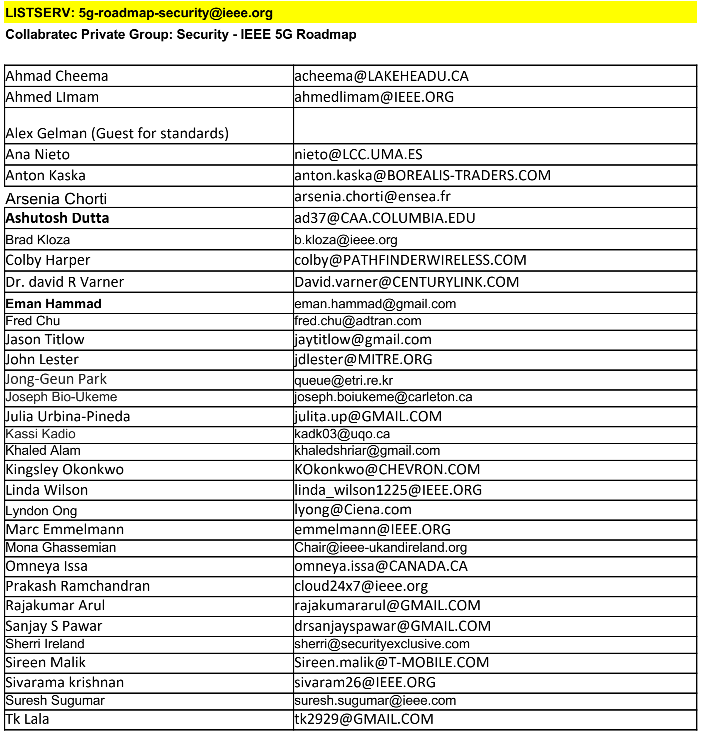
- Meet at Bi-Weekly Meetings
- Bring Your Research Ideas, Talks to discuss
- Engage Industry Stakeholder: Industry Webinars to collect input
- Assess what else is going on: Environment Scan Analysis
- Develop security use-cases for various verticals
- Develop Threat Taxonomy for end-to-end system
- Develop 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!

Contacts: Security Working Group Co-Chairs

Ashutosh Dutta	Eman Hammad
ashutosh.dutta@ieee.org	eman.hammad@gmail.com

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



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

QUESTIONS?

Additional Slides

Cross-team Alignment: Dependencies and Projections

Cross-team	
Edge Automation Platform	• Handover dependence of softwarization: which will impact the security context exchange, Considering temporary security context on the edge to support the handover. • Support of 3rd party applications: and required VNF and virtualization functions, higher risks on the edge when using the same platform for both • Distributed/decentralized functions on the edge: • Security context on the edge for fast authentication and URLLC use-cases: • Ensure protection mechanisms for temporary security contexts on the edge • Subscriber authentication within the visited network: distributed HSS • Consider eSIM server allocation with distributed HSS with proper protection controls • Traffic (security context) exchange between the Edge and the Core • Consider separating the security-related traffic exchange on a dedicated slice • Resilience: to enable the “always available”, the architecture (power, energy savings) • Less trusted 3GPP network access and user plane security • Proper encryption to enable edge-agnostic • Federated Private Networks: • Scenarios: managed service providers, MPNO, independent service providers • Proper isolation: slicing, caching/scheduling (will require edge computing)

Cross-team Alignment: Dependencies and Projections

Cross-team	
Massive MIMO/mmWave	• Physical security compromise • Modes of operations of MIMO will impact the security architecture • Proximity hacking: due to the radio interface of the communication (within 10 meters) • Jamming • Spectrum sensing for system identification and targeted jamming or MiTM • Side channel attacks: power profile for detection • System isolation: • Seamless isolation, • Consider in the standards time-out setting for software handoff. • Verification of node to deter rouge nodes • Coding: cross-layer security on the physical and data layers (check around status with Ashutosh) • ML/AL • Monitoring and reporting: centralized and distributed. • Graceful degradation • Consider adding a layer of redundancy (honeypot)

Cross-team Alignment: Dependencies and Projections

Cross-team	
Optimization	- Optimization: consider the impact when designing security controls around optimization ○ Operation/management ○ Control ○ User - Trust around ML/AI/open source that is used as part of the optimization platform across the architecture ○ Verifiable ML/AI algorithms ○ Verifiable open sources application - Multi-dimensional complexity: virtualization and softwarization ○ Prioritization to ensure security functions are provisioned and protected when needed ○ There should be more effort to generalize security contexts across the different layers ▪ Multiple control plane security contexts: to enabled prioritization ▪ Multiple management plane security contexts - Closed loop control: for use-cases that require more edge computing ○ Centralized, access, core - To enable URLLC user cases, we should consider the trade-off between security monitoring and security controls

Cross-team Alignment: Dependencies and Projections

Cross-team	
Testbeds	• Limitations with existing testbeds on topology, scale, and components. • Security: • Testbed security • Security testing using the testbeds • Ability to enable studies
Deployment	• Physical security: impossible to secure in the current state. • Vendor involvement to have device authentication, and tampering detection • Two way authentication • Public awareness and education • Less trusted access (access points) should be under close monitoring and detection functionality

Cross-team Alignment: Dependencies and Projections

Cross-team	
Applications	• Applications risks: ○ Device: user and edge device security ○ Infrastructure: behind the edge, should be able to provide the security functions regardless of the flexible/fluid architecture ○ User: privacy concerns ▪ Enabling user choice: consideration of separating identity from access. • Trade-off between energy/power optimization and security on the radio channel. What environments/applications would that be relevant? • Within the URLLC use-cases there will different classes of reliability requirements that must be classified and prioritized when provisioning security controls and system resources ○ Mission critical applications ○ Others
Standards	• IEEE 1915 ongoing softwarization & virtualization security standard are looking for contributions • Consider providing input (Mark Underwood) • Potential seed ideas for standards around device tampering, trade-offs between performance & security/privacy