5G & Emerging Security Landscape

Suresh Nair,

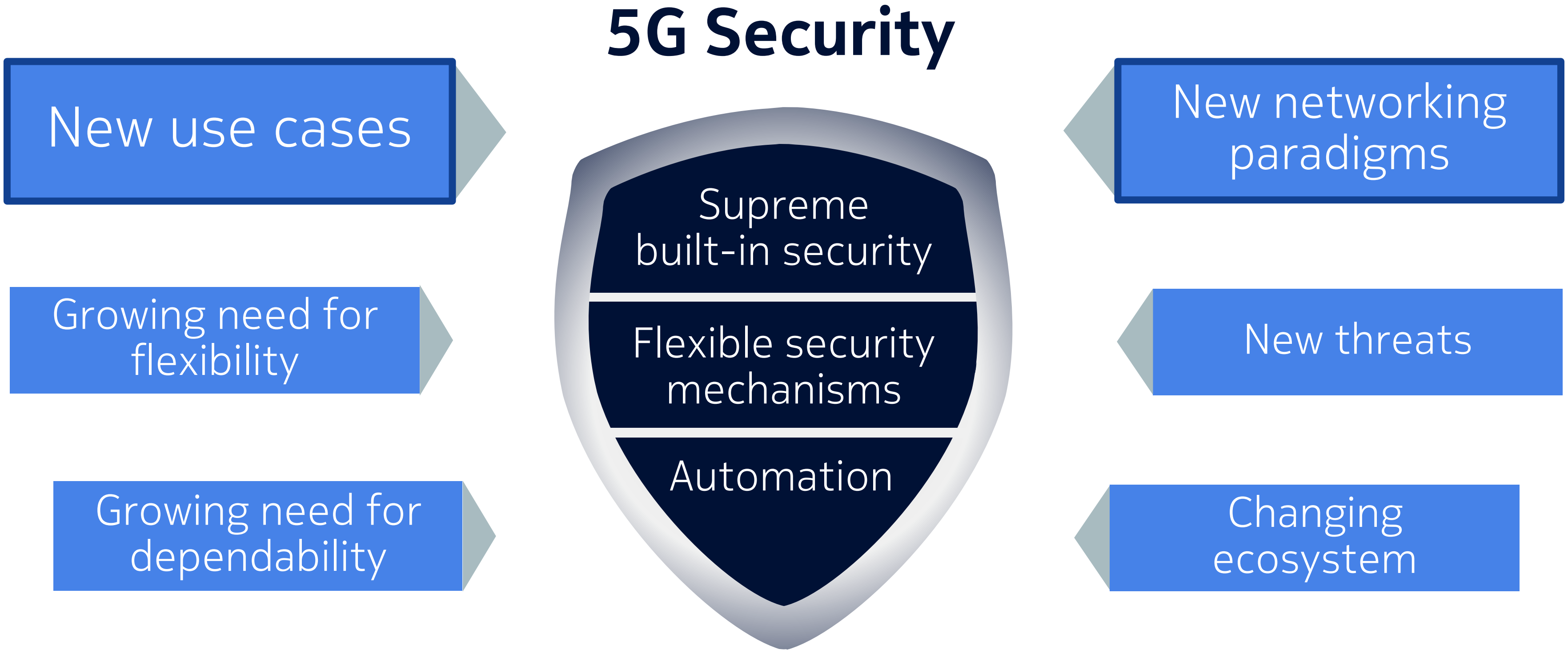
Chair 3GPP Security WG,

Principal Security Standardization Engineer, Nokia

Agenda

1. 5G Security Drivers and Overall Vision
2. 5G Potential Attack Vectors
3. 5G Security Standardization: Rel-15 Features
4. 5G Security Standardization: Rel-16 Features
5. 5G Security Standardization: Rel-17 Features
6. 5G Security Standardization: Rel-18 Features
7. 6G: Emerging technology drivers
8. 6G: Emerging threat landscape
9. Post quantum Cryptography
10. Open issues and need for collaboration

5G Security Drivers and Overall Vision



5G Security

New use cases

Growing need for flexibility

Growing need for dependability

Supreme built-in security

Flexible security mechanisms

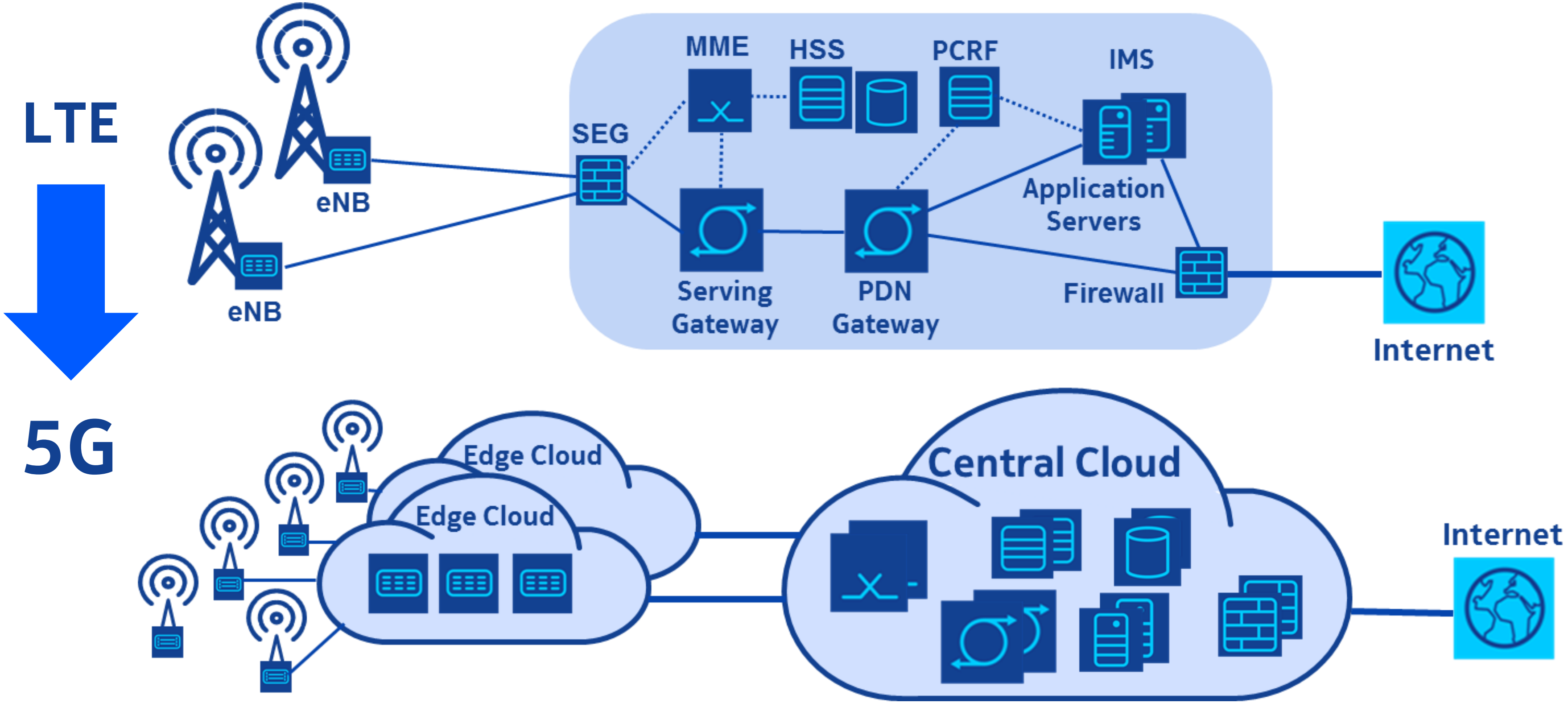
Automation

New networking paradigms

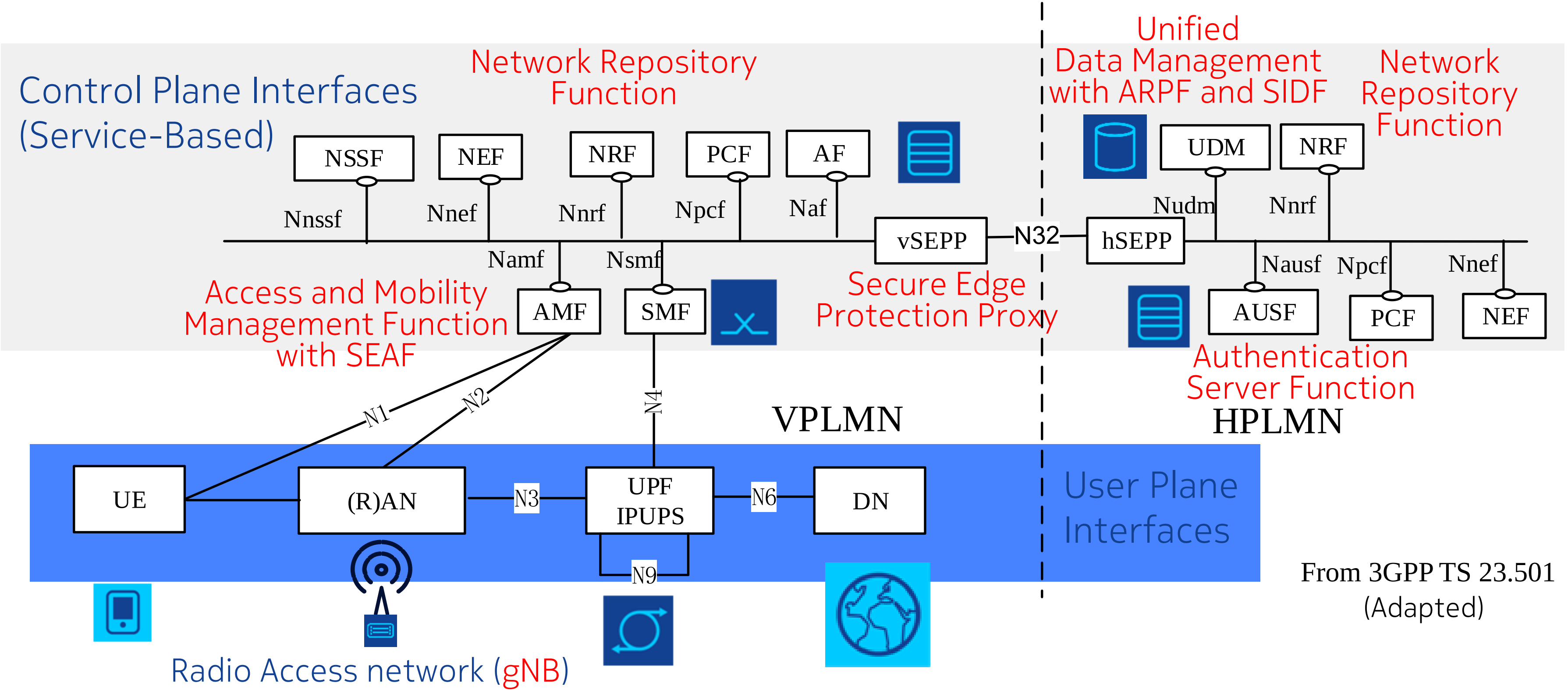
New threats

Changing ecosystem

From LTE to 5G: Adopting New Networking Paradigms



Crucial Security Functions in the 3GPP 5G System

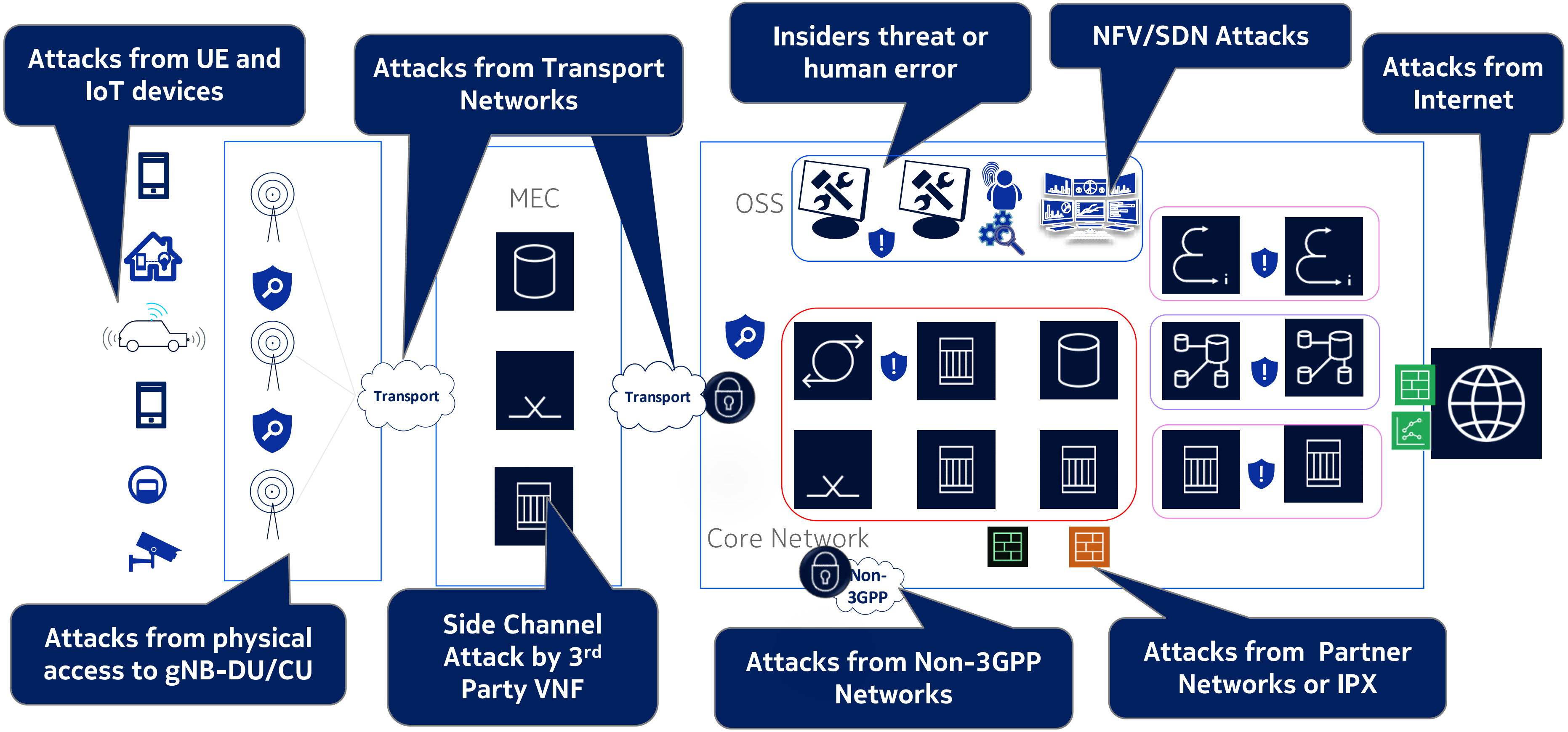


Control Plane Interfaces (Service-Based)
Network Repository Function
NSSF
NEF
NRF
PCF
AF
Nnssf
Nnef
Nnrf
Npcf
Naf
Namf
Nsmf
Access and Mobility Management Function with SEAF
AMF
SMF
vSEPP
N32
hSEPP
Secure Edge Protection Proxy
Unified Data Management with ARPF and SIDF
Network Repository Function
UDM
NRF
Nudm
Nnrf
Nausf
Npcf
Nnef
AUSF
PCF
NEF
Authentication Server Function
VPLMN
HPLMN
N1
N2
N4
UE
(R)AN
N3
UPF IPUPS
N6
DN
N9
User Plane Interfaces
Radio Access network (gNB)

From 3GPP TS 23.501 (Adapted)

Red: Functions crucial for the security architecture

5G Potential Attack Vectors



Attacks from UE and IoT devices

Attacks from Transport Networks

Insiders threat or human error

NFV/SDN Attacks

Attacks from Internet

Attacks from physical access to gNB-DU/CU

Side Channel Attack by 3rd Party VNF

Attacks from Non-3GPP Networks

Attacks from Partner Networks or IPX

5G Security Standardization: Rel-15 Features

Unified authentication framework	Access-agnostic authentication	Enhanced subscriber privacy (SUPI is encrypted to SUCI)	Split RAN (CU+DU) security
Secondary authentication (Access to ext. DN)	Network Slice security	Service based architecture in 5GC	PLMN Interconnect security for roaming
5GS-EPS interworking security	LTE-NR Dual Connectivity	user plane integrity protection	Ultra Reliable Low Latency Communication (URLLC)

5G Security Standardization: Rel-16 major features

- Non-Public Networks
- Enhanced SBA
- Network Slice Specific authentication
- CIOT Enhancements
- Wireless Wireline convergence
- Integrated access backhaul
- Enhanced UPIP
- Longterm Root key update
- Authentication Key management for Applications (AKMA)
- V2X (Vehicle to anything)
- Security Impact of Virtualization
- Security Assurance for all 5G NFs

5G Security Standardization: Rel-17 major features

5G Proximity services	5G Multicast Broadcast Services	Network Automation	Uncrewed Aerial systems
Integration of GBA in to 5GC	Industrial IoT	5G Messaging	Multi USIM
LTE UPIP	V2X (Vehicle to anything)	Non-Public Networks	Security Assurance

5G Security Standardization: Rel-18 major features

- Zero Trust Architecture
- AI/ML Security aspects in RAN
- AI/ML Security aspects CN
- Certificate management
- Proximity Based services
- Subscriber-aware northbound API access in CAPIF (SNAAPPY)
- Security Impact in Virtualization
- Roaming HUB support
- Id Privacy
- Non-Public Networks
- Security Assurance
- 24 study topics

6G- Emerging Technology drivers

- Enabling ultra-low-latency applications
- Supporting intermittent connectivity
- Creating wireless service platforms
- Densifying cells
- Scaling up edge/fog computing
- Sharing spectrum
- Using sub-THz spectrum bands
- Sharing infrastructure
- Using open interfaces
- Utilizing artificial intelligence and machine learning
- Internetworking with Wi-Fi
- Internetworking with satellite networks

6G: Emerging Security & threat landscape

Platform evolution

- Zero trust security principles need to be adopted from the beginning
- Quantum safe algorithms need to adopted
- Security procedures to certify and verify the integrity of virtualized products
- Dynamic Security Assurance

Device evolution

- Different types of devices: simple IoT, smart sensors, XR/VR devices, smart phones, wearables etc
- Access security as per the need of device
- Different security algorithms and protocols
- High security storage within the device

Access network evolution

- Disaggregated RAN in multiple security domains
- Mobility security for multiple RAN AP providers
- Security for AIML models

Core network evolution

- Dynamic authentication and authorization
- Block Chain applicability in Roaming Security

6G: Post Quantum Cryptography

NIST selection of algorithms

- CRYSTALS-Kyber: For general encryption.
- CRYSTALS-Dilithium: For digital signatures.
- Expected follow up work:
  -Adoption of the algorithms in different application domains

Follow up in 3GPP

- New authentication protocol and algorithm for UE-network authentication
- Flexible protocols to support any algorithm including PQC algorithm.
- Authentication based on device capability

6G Security: Open issues and need for further collaboration

Open issues

- Achievements and progress from 2G to 5G is quite impressive.
- But there are gaps as well, obvious ones are:
  - Lack of Security for PWS messages.
  - Technology progress makes it increasing easy to mount False Base Stations and mount different privacy and security attacks.
  - Roaming security loopholes, no clear regulations

Follow up in 3GPP

- Regulatory inputs are lacking in SDOs, hence no impetus to adopt security solutions.
- Global regulations are difficult to achieve, may vary from country to country.
- Atleast major geographical areas need to be represented.
- Solutions need to formulated in flexible manner, easy to adopt to have security or not have security.

Unless multiple parties work together, good standardization doesn’t happen resulting in strong secure networks !

NOKIA