中国移动
China Mobile

Security for 5G and beyond

China Mobile Research Institute

Security Evolution of Telecommunication Network

2G

one-way authentication (A3/A8)
encryption(A5)

False base station, clone card
User data cracking
Signaling forgery (SS7)

Network: closed network
IT: special equipment
Service: voice and SMS

3G

+mutual authentication (Kasumi)
+integrity protection of signalling
+GBA service
+domain isolation(inter-)

+residual risk to 2/3G Interoperability
Signaling forgery (SS7、Diameter)

Network: semi open, IP based
IT: special equipment
Service: voice, telephone, Internet

4G

enhanced algorithm (AES/SNOW3G/ ZUC)
+network domain security(intra-)
+SCAS，NESAS

+residual risk to 4G fallback to 2G
+virtualization risk
Signaling forgery (SS7、Diameter)

Network: open (external)
IT: partial decoupling
Service: voice, volte, Internet

5G

+AKMA service
+SBA security
+user identity privacy(SUCI)
SCAS、NESAS
+NWDAF security analysis

+Intranet attack risk
virtualization risk
low level of intelligence and coordination

Network: open (internal and external)
IT: virtualization, SDN
Service: voice, volte, Internet, private network

中国移动
China Mobile

Driving forces for Security Evolution of Future Telcom Network

Network driven

- Heterogeneous security for Internet of everything
- Cloud+computing+network convergence
- Security for exposed, distributed, automatic and builtin network

Service driven

Customized security for Internet of everything

- new
- strong
- different
- smart

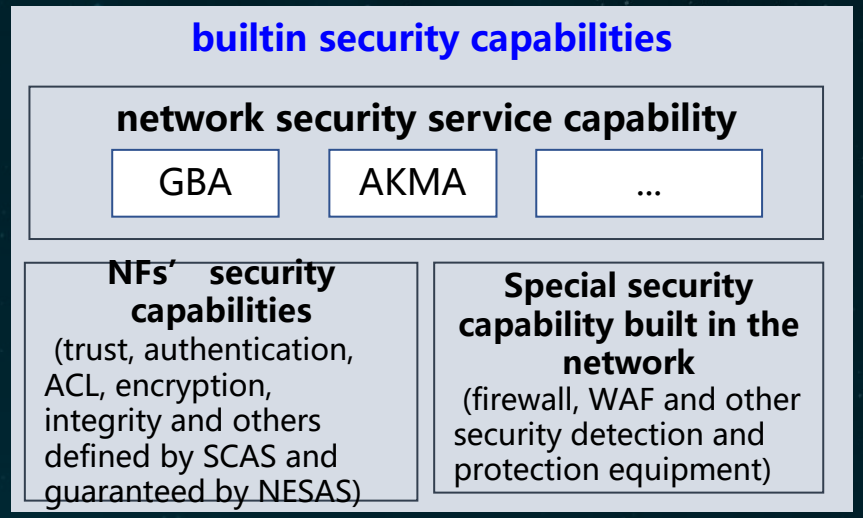
New technology driven

- Utilization of blockchian, trust computaion, QKD, SDN..
- Challenge introduced by new technologies

Telcom Security Evolution Trend

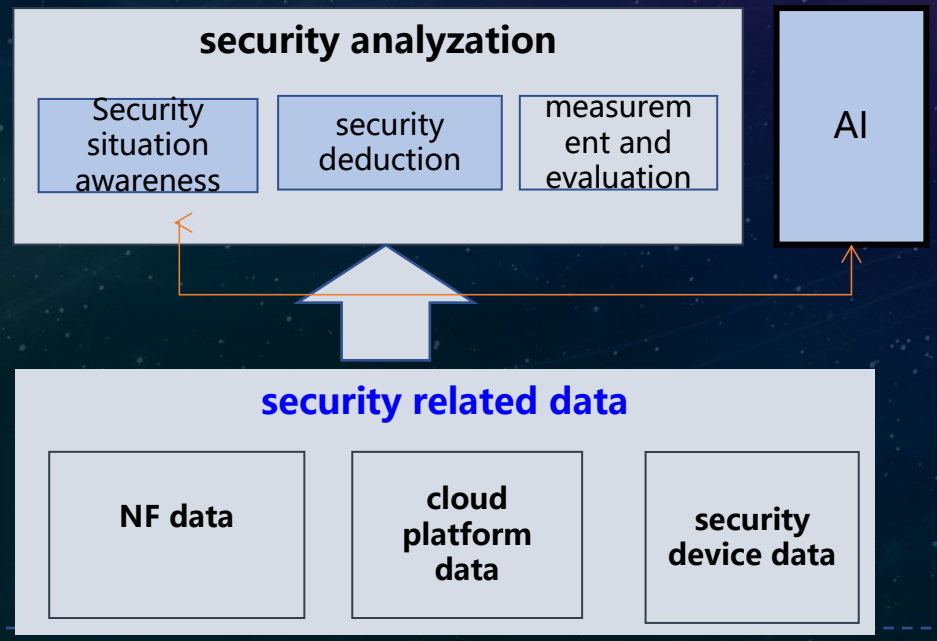
Builtin security capability

- Security capbilities built in NFs and network are continuously enhanced and enriched



Intelligent Security

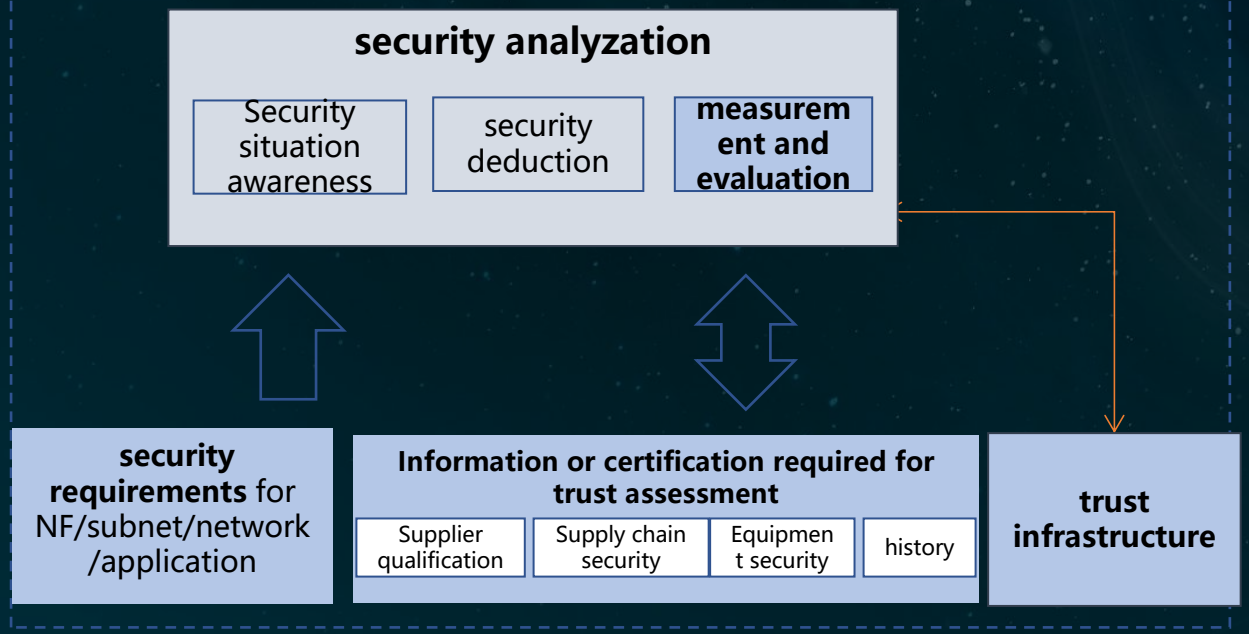
- **Data based**: analyzation security situation from network data, business data, user data
- **AI based**: modelling or feature extraction of attack behavior, security policy



Telcom Security Evolution Trend

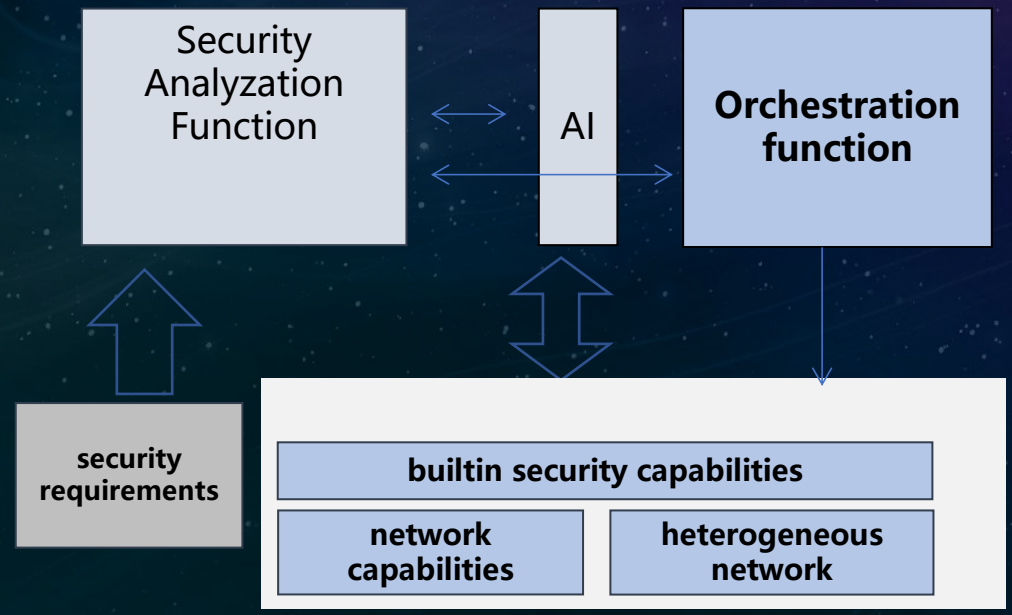
Adaptive security

- Build trust base, continuously evaluate security and trust status, deploy appropriate security measures as required in a flexible way.



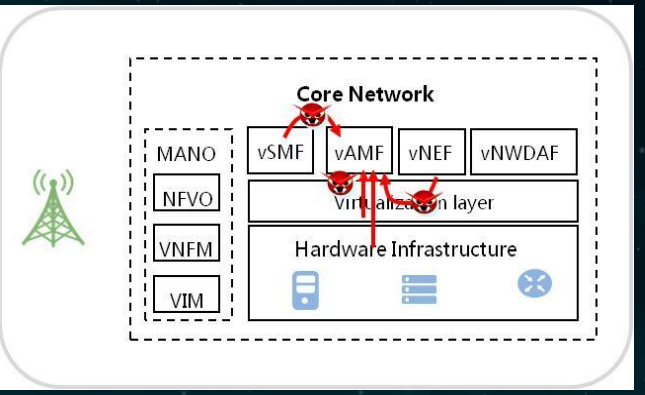
Coordination for security

- Collaboration of builtin security capabilities.
- Collaboration of security capability and other capabilities.
- Collaboration of security capability among heterogeneous networks.



Security of 5G-Advanced

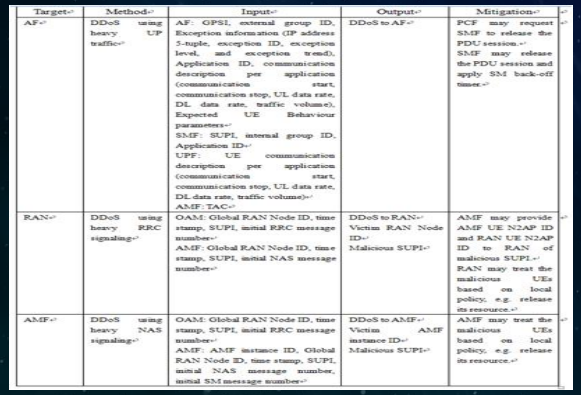
Builtin



- VNF vulnerability
- Traffic between some NF is invisible
- Insecure infrastructure access to network
- insecure cryptography

- SCAS for NF and VNF
- Security monitoring and perception mechanism inside intranet and NF
- Trust startup,remote attestation
- Quantum resistant cryptography

Intelligent

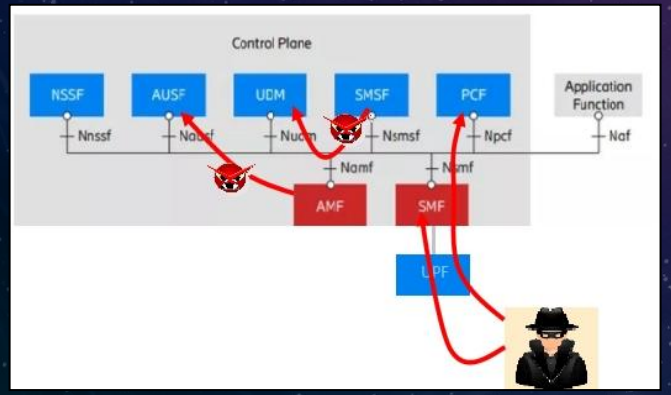


Target	Method	Input	Output	Mitigation
AF	DDoS using heavy UP traffic	AF: GPSI, external group ID, Exception information (IP address 5-tuple, exception ID, exception level, and exception trend), Application ID, communication description per application (communication start, communication stop, UL data rate, DL data rate, traffic volume), Expected UE Behaviour parameters; SMF: SUPI, internal group ID, Application ID; UPF: UE communication description per application (communication start, communication stop, UL data rate, DL data rate, traffic volume); AMF: TAC	DDoS to AF	PCF may request SMF to release the PDU session. SMF may release the PDU session and apply SM back-off timer.
RAN	DDoS using heavy RRC signaling	OAM: Global RAN Node ID, time stamp, SUPI, initial RRC message number; AMF: Global RAN Node ID, time stamp, SUPI, initial NAS message number	DDoS to RAN: Victim RAN Node ID; Malicious SUPI	AMF may provide AMF UE N2AP ID and RAN UE N2AP ID to RAN of malicious SUPI. RAN may treat the malicious UEs based on local policy, e.g. release its resource.
AMF	DDoS using heavy NAS signaling	OAM: Global RAN Node ID, time stamp, SUPI, initial RRC message number; AMF: AMF instance ID, Global RAN Node ID, time stamp, SUPI, initial NAS message number, initial SM message number	DDoS to AMF: Victim AMF instance ID; Malicious SUPI	AMF may treat the malicious UEs based on local policy, e.g. release its resource.

- Attack behaiver and abnormal NF behavior

- Automatic security detection and response based on NWDAF

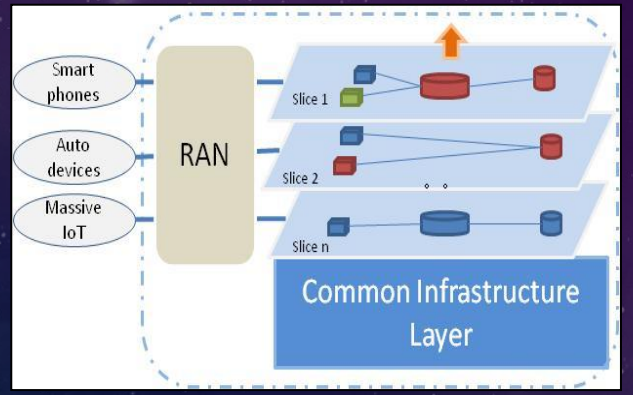
Adaptive:



- SBA architecture makes it easier for network elements to visit each other
- Static trust relationship cannot resist insider attacker

- Flexible and fine grained access control between NFs
- Zero trust access and dynamic evaluation

Coordination:



- Non-automatic slice security
- Network security capabilities (GBA, akma, etc.) are expected to be provided as service

- Orchestrating security for Slice / private network
- Security exposure as service

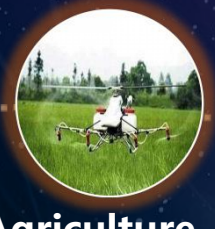
6G Timeline


2019
2020
2021
2022
2023
2024
2025
2026
2027
2028
2029
2030
ITU-T
FG NET-2030,SG13/11/17
usecase,requirements,...
standardization
ITU-R
WP 5D
Trends,roles, Usage scenarios, capabilities
3GPP
R17
R18 / R19 ...
6G study
6G standardazation
NGMN
6G DRIVERS AND VISION, USE CASES AND ANALYSIS

中国移动
China Mobile

6G Scenarios


Manufacturing


Agriculture


Transportation


Intelligent Interaction


Digital Twin

Intellectual Manufacture

Intellectual Society

Intellectual Life


Healthcare


Depopulated Zone


Synaesthesia interconnection


Virtual Reality


Holographic Interaction

Ubiquitous Intellegence

Security for 6G scenarios

The new type and new scenarios of 6G network have put forward new requirements for security and also provided more security enablement.

- R 1: Heterogeneous network convergence authentication;
- R 2: Different levels of network interworking security guarantee mechanism and customizable security service capability;
- R 3: Lightweight security to ensure secure access under resource constraints

Air-space-ground

- R 4: Twin network security, security trust interaction system between digital systems, protection measures for policy delivery interface, etc
- E 1: security deduction, which helps security from qualitative to quantitative (deterministic).

Digital twin

- R 5: Perceived data security and privacy protection
- R 6: Fine-grained and flexible configuration and scheduling of security measure

Integration of perceptual communication

- R 7: Computing security, massive data distributed secure storage and secure computing

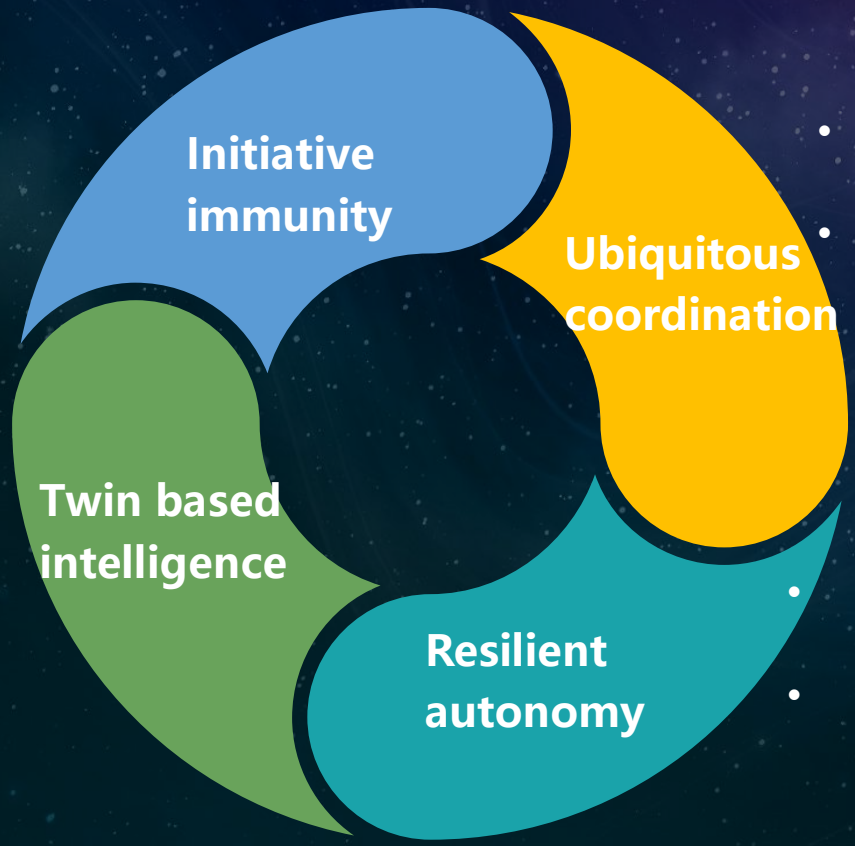
Computing convergence

- R 8 & e 4: Encryption and authentication mechanism integrated with communication
- R 9: lightweight security

Ultra high speed, ultra large connection and ultra-low delay

6G Security Vision

- Systematized builtin security to form an immune ability against internal attacks
- Enhanced security design e.g.,wireless physical layer security



- Secure interoperability of heterogeneous network(air-space-ground) convergence
- Coordination of computing and network security
- End, edge, network and cloud security capabilities collaboration

- AI bring intelligence to security
- DTN bring certainty to security intelligence
- From passive protection to active perception

- Dynamic and flexible security capability deployed on demand
- Integrated response and recovery capabilities to improve network resilience

中国移动 China Mobile

Views on 6G security

China Telcom: Trust and active immunity
《Potential impact of emerging technologies on 6G network architecture》

China Unicom: Security design is integrated within network design
《China Unicom 6G whitepaper》

NTT DOCOMO: autonomously detect network attacks
《5G Evolution and 6G》

Huawei: Native Trustworthiness
《6G the next horizon》

ZTE: a self-perceptive, self-adaptive, and self-evolving network immune system_x0002_
《Vision of Intrinsic Cybersecurity Beyond 2030》

Samsung: trust and privacy
《THE NEXT HYPER—CONNECTED EXPERIENCE FOR ALL 》

Vivo: Active security to achieve system-level privacy and security mechanism
《6Gvision、requirements and challenges》

Bell Labs: authentication, confidentiality and key exchange
《COMMUNICATIONS IN THE 6G ERA 》

University of Oulu: data protection
《Key Drivers and Research Challenges for 6G Ubiquitous Wireless Intelligence 》

Lenovo: trust, security and privacy
《Lenovo 5G/6G Whitepaper》


Thanks