GTI
5G Network Security Consideration

5G Network Security Consideration

Version:	V1.1
Deliverable Type	□ **Procedural Document** □ **Working Document**
Confidential Level	□ **Open to GTI Operator Members** □ **Open to GTI Partners** □ **Open to Public**
Working Group	5G eMBB-Architecture-Network group
Task	Task-N-PM2-PJ4-4: 5G Security White Paper
Source members	China Mobile, ZTE Corporation
Support members	Huawei, Sprint, ViVo
Editor	Minpeng Qi, Xincheng Yan
Last Edit Date	12-02-2019
Approval Date	DD-MM-YYYY

Document History

Date	Meeting #	Version #	Revision Contents
12-02-2019		1.0	First version
20-03-2019		1.1	Adding information on cover page
DD-MM-YYYY			
DD-MM-YYYY			
DD-MM-YYYY			

Table of Contents

1 Executive Summary

It's time for 5G deployment and operation worldwide. In 5G era, requirements about communication, service and network management are quite different from the requirements of 2/3/4G systems. What is more, 5G network will suffer more attacks as new attacking skills and tools are increased constantly. This document tries to study the typical characteristics of 5G service system security, figure out differences on new systems and new environments, and propose new management and operation solution to deal with them. With these recommendations, operators can provide 5G communication services secure and robust.

2 Abbreviations

Abbreviation	Explanation
AI	Artificial Intelligence
AKA	Authentication and Key Agreement
ARPF	Authentication credential Repository and Processing Function
BOSS	Business and Operation Support System
CE	Custom Edge
DDoS	Distributed Denial of Service
DNS	Domain Name Service
eMBB	Enhanced Mobile Broadband
IDS	Intrusion Detection Systems
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
Ipsec	IP layer Security (protocol)
IPX	Internetwork Packet Exchange
IT	Information Technology
MEC	Multi-access Edge Computing
mMTC	Massive Machine Type Communications
NF	Network Function
NFV	Network Function Virtualization
NFVI	Network Function Virtualization Infrastructure
NRF	NF Repository Function
O&M	Operation and Management
OS	Operating System
PTN	Packet Transport Network
SBA	Service Based Architecture
SEPP	Security Edge Protection Proxy
SPN	Slicing Packet Network
SUCI	Subscription Concealed Identifier
SUPI	Subscription Permanent Identifier
TLS	Transport Layer Security (Protocol)
UDM	Unified Data Management
UE	User Equipment
UP	User Plane

USIM	Universal Subscriber Identity Module
uRLLC	Ultra Reliable Low Latency Communications
WLAN	Wireless Local Area Network

3 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

[1] ITU-R M.2083-0: “IMT Vision – Framework and Overall Objectives of the Future Development of IMT for 2020 and Beyond”

[2] 3GPP TS 22.261: “Technical Specification Group Services and System Aspects; Service Requirements for the 5G system; Stage 1”

[3] ETSI GS MEC-002: “MEC Technical Requirements”

4 Background

As a new generation of mobile communication technology, 5G network supports higher bandwidth, lower latency, and greater connection density. This would bring deeper convergence of communications technologies into all industries. Thus it will effectively promote the development of the world's digital economy, bring new changes to society, and give continuously power to the global economic and social development. ITU-T has defined three categories of scenarios for 5G, as Enhanced Mobile Broadband (eMBB), Ultra- Reliable and Low-latency Communications (uRLLC) and Massive Machine Type Communications (mMTC) [1].

In order to meet the different network and communication requirements of different vertical industries, 5G introduced innovative technologies such as network slicing[2] and multi-access edge computing[3]. 5G network is not only able to be used for communication between people, but also for communication between people and Internet-of-things(IoT), and among IoTs, which will greatly expand the business scope of mobile networks and enrich the ecosystem for communication networks.

At present, some countries and regions have begun to provide 5G commercial services. On October 1, 2018, Verizon launched 5G commercial service in residential area such as Houston, Indianapolis, Los Angeles and Sacramento, etc. Another US operator AT&T also announced the launch of 5G mobile networks by the end of 2018. On December 1, 2018, South Korea's three major operators SKT, KT and LG U+, jointly announced to commercially launch their 5G network service in South Korea, and covers all of South Korea in 2020. Japan's mobile communications operators announced that they will provide 5G services to enterprise users in 2019, and to normal users in 2020.

In China, three major operators have basically determined to deploy 5G network with three steps: having 5G pilot in some cities in 2018, making 5G trial in 2019, and officially launch large-scale commercial 5G network in 2020. At present, China mobile makes "5+12" program to prepare for the formal commercialization of 5G system: It will have 5G trail in 5 cities simultaneously, including Hangzhou, Guangzhou, Wuhan, Shanghai and Suzhou. And some practical applications based on 5G network are running in another 12 cities including Beijing and Chongqing.

In 5G era, the three different services needs have different communication requirement, access methods and service models and the supported service delivery are also different. What is more, the difference in security is also obvious. This requires the operator to ensure the security of 5G service operations by analyzing security in all aspect of 5G network, through gap analysis from the perspective of system and environment between 5G and legacy networks.

5G network is more open than others, which needs to ensure the security of network, providing flexible security capabilities for vertical industries and applications. For network operator, the goals of 5G security should be: **completed security architecture, adequate privacy protection, flexible security capability exposure, and robust security management.**

5 5G Security Enhancement

Compared to existed network protocol, 5G networks has been defined more security features, including improved authentication function, more well-defined data protection mechanism and enhanced privacy protection, as following.

5.1 Authentication and Authorization

When network is more and more open, the trust is less and less. Thus, authentication becomes more and more important for 5G networks. It is the basis of 5G network security. As a result, both user authentication and authentication between network entities are improved.

In the 2/3/4G network, when the user authentication is performed, home network is just providing authentication vector rather than involving authentication process compared to visited network. It means home network trust visited network and relies on the result of authentication made by visited network. However, this trust relationship is not reliable. Visited network may cheat home network. In 5G, the 5G-AKA mechanism is improved. UDM/ARPF generates an authentication vector and then sends it to AUSF, which are both in home network. AUSF derives visited authentication vector through one-way derivation function and sends it to visited network instead of original authentication vector. Visited network can verify UE by deriving related information based on UE's response but it couldn't get such response by its own. This can guarantee visited network has no ability to cheat home network. As a result, it enhances home network control in authentication process.

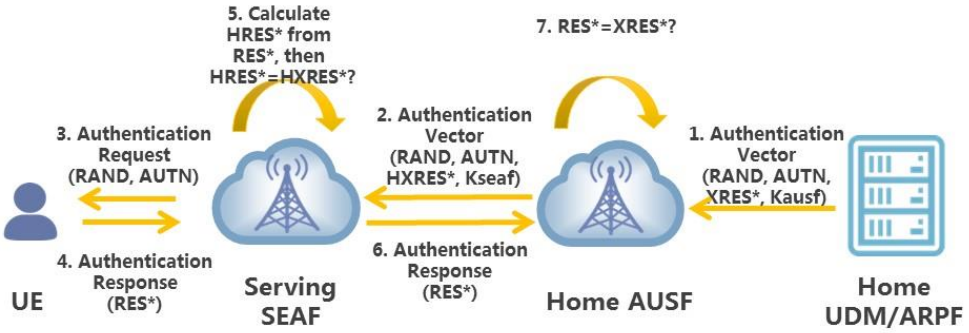

Figure 5.1 5G-AKA security mechanism

The traditional network architecture is based on the reference interface. 5G introduces Service Based Architecture (SBA). In the 5G core network, signaling communication between Network Functions (NF) shall be authenticated and authorized. In the process of NF registration and discovery, mutual authentication between NRF and NF is required and can be implemented through TLS, IPsec or physical protection method. During the service request/response process between NF, the authentication between the NFs can be implicitly achieved through authorized token check or explicitly made by mutual authentication mechanism. For authorization, there are two scenario needs to be considered: internal

authorization of one operator, and cross-operator authorization.

5.2 Data Security Protection

There is no integrity protection mechanism for user plane data in the 2/3/4g network. There is risk to modify UP data, such as tampering with user DNS requests in order to spoofing. Even the message content is encrypted, it also can be modified to result an error, and impact service eventually. In another aspect, the operators trust each other by default currently, and signaling across operator border can be handled without verification. However, the link/path between operator networks is more and more open. Signaling may be tampered with during transmission. Therefore, in 5G network, it considers interconnection security for signaling transferring.

In 5G air interface, an optional integrity protection mechanism is provided for user plane data. In security algorithm negotiation procedure, it only negotiates the integrity algorithm and not start protection compared to 4G network. Such protection will be triggered only when the user needs to create a new bearer, and be determined whether to have real protection based on configuration policy which is coming from core network.

5G introduces a new network function called Security Edge Protection Proxy (SEPP) for interconnection security protection. It has defines two security protection mechanisms: one is based on transport layer protocol, mainly relying on TLS. This mechanism is end-to-end encrypted and integrated that will cause the intermediate switcher IPX has no ability to adjust signaling. The other one is an application layer protocol, which can be named as ALS. This mechanism can protect message on data object granularity in application level. This brings flexibility for each data object protection based one different security policies. Thus it leaves freedom for IPX to obtain or modify relevant information.

5.3 Privacy Protection Enhancement

In the 2/3/4G network, permanent user identity IMSI can be retrieved as plaintext on the air interface. It will cause the issue that IMSI can be obtained over air interface.

In order to protect user's identity, a pair of public/private key can be generated by the home operator in 5G network. Such public key can be installed in user's USIM, while the private key is stored in UDM. When the user needs to send the SUPI (Subscription Permanent Identifier) over the air, the UE encrypts its SUPI with the public key and sends the encrypted result SUCI (Subscription Concealed Identifier) to visited network. The home network decrypts SUCI transferred from visited network by using private key to get real SUPI, and send it back to the visited network. Under this way, SUPI can be securely transferred over the air.

6 5G Security Requirement

Although 5G has a series of security enhancement features, more and more security requirements are raised due to the development of network, service and IT technology, as

following.

6.1 Enhanced capabilities to mitigate Internet attacks

5G network is more open compared with 2/3/4G networks. 5G network can provide more capabilities through its exposure interfaces and supports multiple access technologies like Internet, WLAN, etc. Meanwhile, introducing MEC makes core network extends near to user. So 5G networks has more interfaces with others, thus suffers more attack through such interfaces. Therefore, 5G network shall be securely enhanced to cope with Internet attacks.

6.2 More flexible security requirements

In 2/3/4G networks, a unified network policy and security mechanism can be used. However, the applications of various vertical industries supported by 5G network. This requires more refined and differentiated security capabilities. For example, different vertical industries need different security protection on authentication, isolation, data security protection and so on. In another aspect, new technologies such as network slicing, software-defined network, and network function virtualization, cloud computing and artificial intelligence makes it possible for operators to provide more flexible and adaptable security services in 5G network. This can meet the different security requirements of various vertical industries rapidly and intelligently mentioned above.

6.3 New Security Requirements introduced by virtualization

Network virtualization technology is involved into 5G core network, thus telecom functional node can be implemented as tailored software based on common hardware. As a result, telecommunication network is evolved from network entity based system to a combined system containing NFV infrastructure, communication service sub-system and management sub-system. With the introduction of core network virtualization technology, 5G networks could not be secured based physical isolation only, as the previous network, nor can it deploy a large number of security devices on the network to improve protection, as before. When 5G is deployed with virtualization technology, virtualized core network interfaces, such as interfaces with management sub-system, with BOSS and with Internet, shall be at the same or higher security level as traditional physical device-based networks.

6.4 Requirements of Security Capabilities exposure

5G network has comprehensive security capabilities, such as key generation and management, authentication, access control, security management, etc. Some kinds of security capabilities can be exposed to vertical industries for effectiveness and flexibility to build secure 5G ecosystem.

7 5G Security Solution

It has defined enhanced security solution for 5G network. However, it still need to improve security configuration during 5G deployment. Additional security protection system is also necessary to be built in order to protect network operation in order to take advantage of 5G.

7.1 Network Security Architecture

It is still a basic way forward for network deployment designing and security mechanism construction according to the concept of defense in depth, which is as following:

- To separate 5G network into different sections, and deploy security equipment at the border;
- To define security domain as access network domain, core network domain, BOSS domain, O&M domain in one section, and utilizing security mechanism like logical isolation, access control, etc.;
- To isolate access network and core network by using PTN/SPN transport system which is physically isolated with Internet and independent CE between access network and core network;
- To deploy firewalls and intrusion detection systems (IDS) at the interfaces connected with the Internet and third-party services for monitoring and blocking attacks from the Internet.

7.2 Provides Flexible Security Capabilities Based on Slicing

The 5G network slicing integrates network virtualization technology in nature. It can provides basic security capabilities for vertical industries including security authentication, privacy protection, transmission encryption, etc. in virtualized and flexible way. As a result, 5G network slicing can own tailored security capability based on specific security requirement from vertical industry.

A common slicing using shared infrastructure has basic security capabilities such as user authentication, data encryption, security isolation, which can meet basic security requirements of most applications. When vertical industry users have specific security requirements (such as encryption algorithm, encryption strength, security isolation), it can order enhanced network slicing with higher security level customized by the operator.

7.3 Improve NFV Security System

In order to ensure the security of NFV system, following solutions can be considered to

protect NFVI, communication service sub-system and management sub-system: Involving trusted computing techniques to ensure credibility; Reinforcing virtualization software, host machine and virtual machine OS; Isolating virtual machines; Using standardized protocols with encryption, integrity and anti-replay protection for the communication data; Security reinforcement for management elements; Applying encryption, integrity and anti-replay protection for the data transferred on internal interface inside management sub-system between management sub-system and other sub-systems.

7.4 Build Security Capabilities Exposure Platform

In 5G, network operator can expose network security capabilities to the applications of vertical industries, allowing the vertical industry service providers pay more time and attention on specific service development. In this way, new services can be deployed quickly and flexibly to meet users' changing requirements. Same security capabilities in the network can be shared with the applications of multiple vertical industries by instantiation, while the isolation of security-related data can be maintained. Thus improve the efficiency of operators' network security capabilities.

7.5 Secure O&M for Internet of Things Services

In the 5G era, massive Internet of Things terminals will be deployed. The security shall be made followed minimal, necessary and controllable principle: The communication shall be minimized. Only necessary service functions are available. When security incident occurs, the communication shall be able under operator’s control in order to mitigate attacks from such IoT terminals.

7.6 AI and Big Data Application

In 5G era, all kinds of services are complex and diverse. Service data have massive characteristics. As a result, traditional security method which based on data schema matching is not sufficient, and hardly to find out abnormal data. A novel method should be considered to enhance data security by using AI and big data analysis mechanism, in following aspect.

- Malicious website identification. Users may visit phishing websites or the websites contains malicious hyperlinks or virus. In order to protect users' information security, analysis based on artificial intelligence technology can be used to analyze website URLs and web content automatically. A warning message can be sent to users when malicious websites are detected.

- Network security monitoring and situational awareness. In 5G era, there is big challenge how to detect network attacks from massive data. AI can be used efficiently to analyze the characteristics of network data packets like attacking sources, vulnerable destinations, services, impact, etc. which can be used to set up attacking model. AI also can be used to discover the origin of attack actively, to detect attacks accurately and to

perform specific protection against attack. For example, AI can discover the main controller of botnet, update protection policy and/or profile of security equipment, etc.

- Security management for Internet of Things terminal. A main reason for the issue caused by IoT terminals is the large scale of IoT. What is more, the fragmentation of Internet of Things applications leads to complex and diverse systems and protocols. Many terminals have vulnerabilities even when they leave the factory. Therefore, in 5G era, security solutions shall be made to monitor the large number IoT terminals status and mitigate DDoS attacks caused by such IoT terminals. Thus, AI-based monitoring solution can identify service risk, classify and manage potential vulnerable IoT terminals by analyzing location data, log data, billing data. This can reduce the security impact of Internet of Things terminals on communication networks.

8 Conclusion

As next generation of telecommunication technology, 5G will bring big impact for social development and human life. It also expand new space for information and communication technology industry. Facing security challenge, 5G security protocols are enhanced and 5G security capability are exposed. The security enhancement on access network and core network are made by considering adequately the change on service requirement, network architecture, trust model, and progress of attacking. The security capability exposure can improve the security level of whole 5G ecosystem by exposing security capability to service used to ignore security feature and extending security protection for them. At the same time, the development of AI and big data technology also provides a better technical solution to deal with security challenges.

In the future, GTI is willing to work with all partners to promote 5G ecosystem healthy and continuously, to promote 5G network and service security simultaneously, and to provide secure and reliable infrastructure services for society to enter new era of intelligence.