Partnering with the Industry for 5G Security Assurance

HUAWEI

Contents

1 Executive Summary

This 5G security white paper focuses on the following:

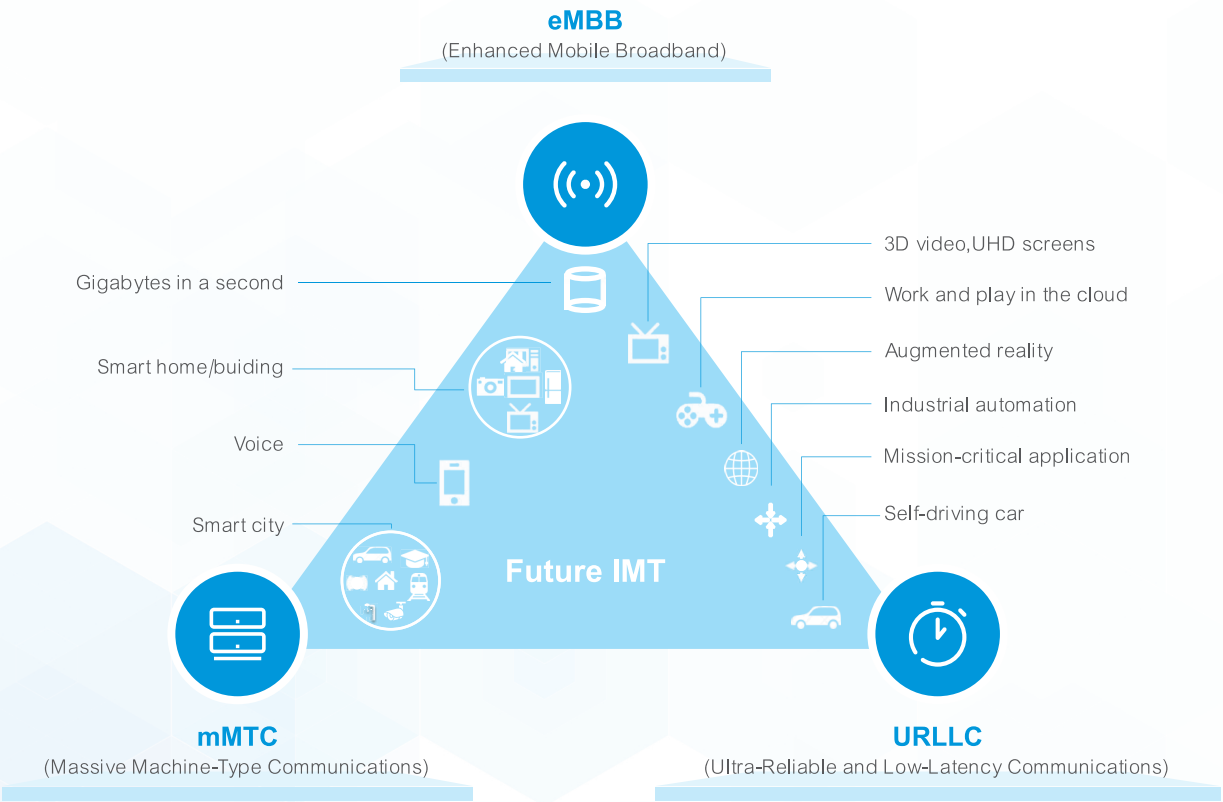
- Why is 5G secure? How do experts from industry and standards organizations ensure that 5G security risks can be effectively managed in terms of security protocols and standards as well as security assurance mechanisms?
- Why is Huawei 5G secure? What technical approaches has Huawei adopted to ensure cyber security of Huawei equipment?
- How to ensure 5G cyber security, including Huawei's support for cyber resilience and recommendations on how to deploy and operate 5G networks in a secure manner.
- How to continuously improve the 5G security level from the perspectives of different stakeholders in order to address future challenges.
- Call for stakeholders to work together to ensure that 5G security risks are controllable.

This white paper will describe industry standards, Huawei's approaches, and joint efforts of industry partners.

2 5G Is On, Bringing Both Opportunities and Challenges

2.1 5G Will Change Our Lives with Diversified Applications

As mobile broadband begins to reach every corner of the world, people's desire to unfold the blueprint of the coming fully connected world is increasing. In the era where all things will be connected over mobile broadband, 5G networks need to meet the requirements of unprecedented connectivity in Enhanced Mobile Broadband (eMBB), Massive Machine-Type Communications (mMTC), and Ultra-Reliable and Low-Latency Communications (URLLC) scenarios.



- eMBB focuses on services that require ultra-high bandwidth, such as high-definition video (4K/8K), virtual reality (VR), and augmented reality (AR), meeting user demands for a digital life.
- mMTC focuses on scenarios requiring high-density connections, such as intelligent transportation, smart grid, intelligent manufacturing (Industry 4.0), and smart logistics, meeting user demands for a digital society.
- URLLC focuses on latency-sensitive services, such as autonomous driving/assisted driving, Internet of Vehicles (IoV), and remote control, meeting user demands for a digital industry.

Towards 2020 and beyond, 5G-empowered VR/AR applications, industrial Internet, unmanned driving, IoV, and other eMBB and IoT applications will grow explosively with the maturity of 5G networks. By 2025, experts predict that there will be 100 billion connections around the world, of which 90% will be IoT connections. Mobile communication will significantly change our lives.

2.2 5G New Services, Architectures and Technologies Will Bring Security Challenges

5G faces security challenges and opportunities brought by new services, architectures, and technologies [1], as well as higher user privacy and protection requirements. The industry needs to understand the requirements of diversified scenarios and better define 5G security standards and technologies to address the associated risks. During 2018, the 3rd Generation Partnership Project (3GPP) SA3 held seven meetings. 74 companies (including their subsidiaries) sent technical experts to attend the meetings [2], with the key objective of formulating 5G security standards. The 3GPP SA3 has comprehensively analyzed 5G threats and risks in 17 security areas[3]:

Security architecture, authentication, security context and key management, radio access network (RAN) security, security within NG-UE, authorization, subscription privacy, network slicing security, relay security, network domain security, security visibility and configurability, credential provisioning, interworking and migration, small data, broadcast/multicast security, management security, and cryptographic algorithms.

Key assets of 5G networks include users' personal data and communication data, hardware and software assets of wireless and core networks, computing resource assets, as well as accounts, passwords, logs, configurations, and charging data records (CDRs) operated and maintained by operators. Hackers attack wireless networks in an attempt to steal and tamper with users' personal data or compromise the availability of networks or computing resources. According to 3GPP specifications [4], "The SUPI should not be transferred in clear text over NG-RAN except routing information, e.g. Mobile Country Code (MCC) and Mobile Network Code (MNC)." The Packet Data Convergence Protocol (PDCP) can be used for the air interface and IPsec for transmission to guarantee the confidentiality and integrity of users' personal data. 5G gNodeBs, however, face wireless signal interference on external air interfaces and attacks on protocols to compromise service availability. Some 5G core network elements, such as UDM, process and store users' personal data. As a result, 5G core networks face breach of users' personal data as well as attacks to compromise resource

availability. Because the central equipment rooms for core network deployment generally adopt high-level security protection, the risks of malicious invasion can be effectively mitigated.

In general, most threats and challenges faced by 5G security are the same as those faced by 4G security. However, the security challenges brought by new services, architectures, and technologies to 5G networks need to be considered. For example, in terms of new services, consideration must be given to access authentication for third-party slicing service providers. 3GPP security standards are taking into account the security challenges and solutions to the new 5G architectures, such as network slicing and Service Based Architecture (SBA). Another aspect that requires consideration is the secure use of computing resource assets, especially as cloud architecture in 5G is widely adopted. In addition, as new technologies such as quantum computing develop, the impact they have on traditional cryptographic algorithms needs to be considered.

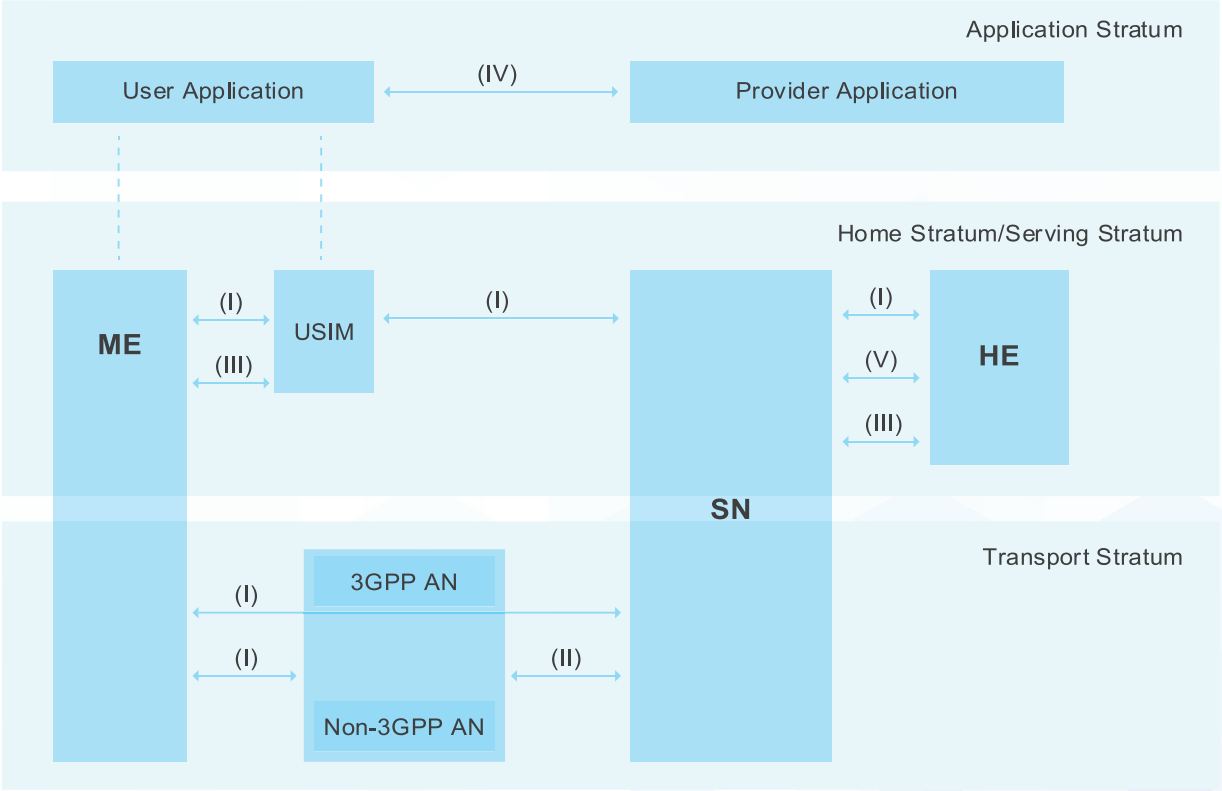
3GPP 5G security and 4G security share the same purpose, which is to ensure the confidentiality, integrity, and availability of networks and data.

3 5G Security Standards Improve on Their Predecessors

3.1 5G Security Architecture Inherits 4G Security Architecture

Currently, 3GPP SA3 has developed 5G R15 security standards and is developing 5G R16 security standards[5]. To ensure that 5G standards move ahead consistently at all technical levels, the 3GPP is developing security standards at the same pace as that of architecture and wireless standards. 5G R15 standards have defined security architectures and security standards for eMBB scenarios, covering Standalone (SA) and Non-Standalone (NSA) architectures. Based on the 5G R15 security architecture, 5G R16 and R17 standards will cover security optimization for mMTC and URLLC scenarios.

The security architecture of mobile networks is hierarchical and classified by domain in design. The 5G security architecture contains the following security domains:



Network access security (I), Network domain security (II), User domain security (III), Application domain security (IV), SBA domain security (V) [6]

- Network access security (I): the set of security features that enable a UE to authenticate and access services via the network securely, including the 3GPP access and Non-3GPP access, and in particularly, to protect against attacks on the (radio) interfaces. In addition, it includes the security context delivery from SN to AN for the access security. Specific security mechanisms include bidirectional authentication, transmission encryption, and integrity protection.

- Network domain security (II): the set of security features that enable network nodes to securely exchange signaling data and user plane data. **Network domain security defines security features for interfaces between access and core networks and between home and serving networks. The separation between access and core networks is as clear as that in 4G. For the interfaces between RAN and Core,** specific security mechanisms, such as IPsec, can be used to provide security separation and protection.

- User domain security (III): the set of security features that secure user access to mobile equipment. Mobile equipment uses internal security mechanisms, such as a PIN code, to ensure security between the mobile equipment and universal subscriber identity module (USIM).

- Application domain security (IV): the set of security features that enable applications in the user domain and in the provider domain to exchange messages securely. Security mechanisms of the application domain are transparent to the entire mobile network and are provided by application providers.

- SBA domain security (V): the set of security features that enable network functions of the SBA architecture to securely communicate within the serving network domain and with other network domains. These features include network function registration, discovery, and authorization security aspects, as well as protection for service-based interfaces. SBA domain security is a new security feature in 5G. An SBA forms the basis of the 5G core network. To ensure security between UEs in the SBA, security mechanisms such as Transport Layer Security (TLS) and Open Authorization (OAuth) are needed.

- Visibility and configurability of security (VI): the set of features that enable the user to be informed whether a security feature is in operation or not.
  Note: The visibility and configurability of security is not shown in the figure.

5G security architecture, same as 4G security architecture, consists of the transport stratum, serving stratum, home stratum, and application stratum, which are securely isolated from each other.

- Transport stratum: Located at the bottom of the architecture, the transport stratum has low security sensitivity. It includes some UE functions, all gNodeB functions, and some core network functions, such as the User Plane Function (UPF). **These functions, excluding the UE functions, do not involve sensitive data, such as subscription permanent identifiers (SUPIs) and user root keys.** They manage only low-level keys in the key hierarchy, for example, user access keys. Low-level keys can be derived,

replaced, or updated by a high-level key at the home/serving stratum. However, a low-level key cannot induce a high-level key.

- Serving stratum: It has relatively high security sensitivity and includes such core network functions of the operator's home network as the Access and Mobility Management Function (AMF), Network Repository Function (NRF), Security Edge Protection Proxy (SEPP), and Network Exposure Function (NEF). The core network functions of this stratum manage only mid-level derived keys (such as AMF keys) in the key hierarchy. A mid-level key can be derived, replaced, or updated by a high-level key at the home stratum. However, a mid-level key cannot induce a high-level key. This stratum does not involve gNodeBs.

- Home stratum: It has high security sensitivity and includes the Authentication Server Function (AUSF) and Unified Data Management (UDM) of the operator's home network, as well as the USIM in the UE, and therefore it contains sensitive data such as the SUPIs, user root keys, and high-level keys. This stratum does not involve gNodeBs or other functions of the core network.

- Application stratum: It is closely related to service providers, but hardly related to operator networks. The application stratum involves 5G applications that, similar to 4G applications, need E2E security assurance for services that require high security in addition to transport security. For example, mobile payment requires E2E security assurance at this stratum, even if transport security is guaranteed on the 4G network, to ensure the security and correctness of transactions.

The 5G network inherits the 4G network security architecture with different strata and domains. The 5G access and core networks have clear boundaries, interconnect through standard protocols, support inter-vendor interoperability, and have standards-based security protection mechanisms [7]. **In terms of cyber security risks, regulators need to monitor all four strata, service providers need to monitor the application stratum, operators need to monitor the transport, serving, and home strata, and equipment vendors need to focus on the underlying network equipment. All industries shall work together to tackle the security challenges brought by services, architectures, and technologies under the standard architecture.**

3.2 Security Enhancement of 5G Standards over 4G Standards

The 5G SA network supports more security features to tackle potential security challenges in the future 5G lifecycle. 5G NSA and 4G networks share the same security mechanisms and work in standard and practice consistently to keep improving their security levels.

- Stronger air interface security: In addition to user data encryption on 2G, 3G, and 4G networks, 5G standards provide user data integrity protection to prevent user data from being tampered with.

- Enhanced user privacy protection: In 2G, 3G, and 4G networks, users' permanent IDs (international mobile subscriber identities — IMSIs), are transmitted in plain text over the air interface. Attackers can exploit this vulnerability using IMSI catcher attacks to track users. In 5G networks, users' permanent IDs (in this case, SUPIs) are transmitted in ciphertext to defend against such attacks.

- Better roaming security: Operators usually need to set up connections via third-party operators. Attackers can forge legitimate core network nodes to initiate Signaling System 7 and other attacks by manipulating third-party operators' devices. 5G SBA defines Security Edge Protection Proxy (SEPP) to implement E2E security protection for inter-operator signaling at the transport and application strata. This prevents third-party operators' devices from tampering with sensitive data (e.g. key, user ID, and SMS) exchanged between core networks.

- Enhanced cryptographic algorithms: 5G R15 standards currently define security mechanisms such as 256-bit key transmission. Future 5G standards will support 256-bit cryptographic algorithms to ensure that such algorithms used on 5G networks are sufficiently resistant to attacks by quantum computers. The 3GPP has recommended that the ETSI Security Algorithms Group of Experts (SAGE) start to evaluate 256-bit cryptographic algorithms.

5G cyber security standards put more security features into standard to tackle potential security challenges and lead to security enhancements in the future 5G lifecycle.

3.3 5G Security Assessment Becoming Standardized

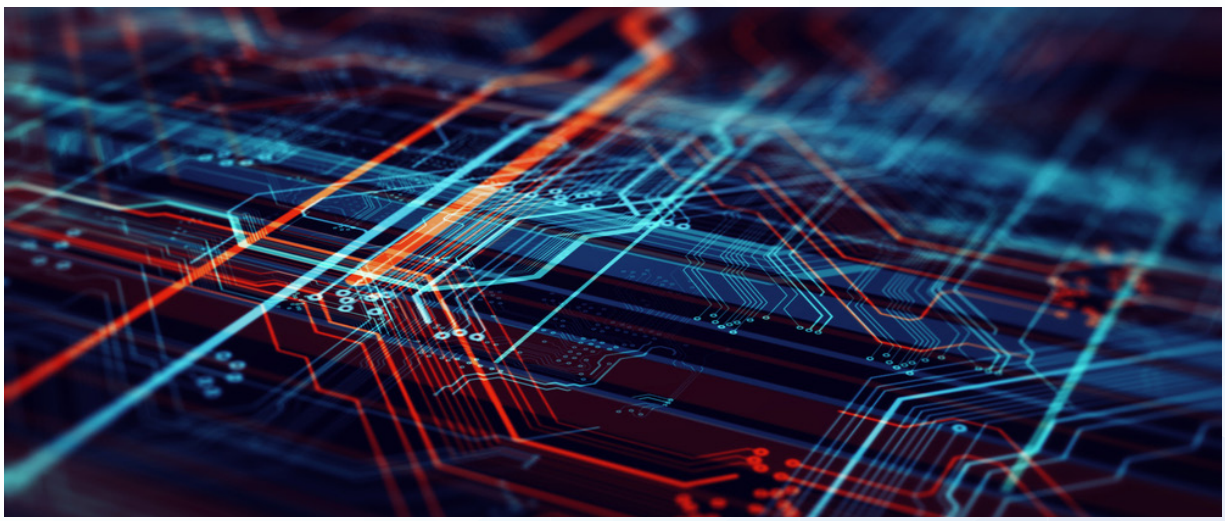
The Network Equipment Security Assurance Scheme (NESAS) is jointly defined by GSMA and 3GPP for security evaluation of mobile network equipment. **Developed according to security standard guidelines pertaining to vendors' product development and lifecycle processes, the scheme provides a security baseline to evidence that network equipment satisfies a series of security requirements.** Currently, 3GPP has initiated security evaluation of multiple 5G network equipment, and major equipment vendors and operators are actively participating in the NESAS standard formulation [8].

NESAS brings the following benefits to equipment vendors:

- Provides accreditation from the world's leading mobile industry representative body
- Delivers a world-class security review of security related processes
- Offers a uniform approach to security audits
- Avoids fragmentation and potentially conflicting security assurance requirements in different markets

NESAS brings the following benefits to mobile operators:

- Sets a rigorous security standard requiring a high level of vendor commitment
- Offers peace of mind that vendors have implemented appropriate security measures and practices
- No need to spend money and time conducting individual vendor audits



4 Huawei Is Committed to Ensuring 5G Equipment Security and Cyber Resilience

Huawei R&D focuses heavily on security throughout product development, adhering to the principle of security by design and security in process. Cyber security activities built into the process are performed in strict compliance throughout the entire product lifecycle, so that security requirements can be implemented in each phase.

Huawei R&D provides the Integrated Product Development (IPD) process to guide E2E product development. Since 2010, Huawei has started to build cyber security activities into the IPD process according to industry security practices and standards such as OWASP's Software Assurance Maturity Model (OpenSAMM), Building Security In Maturity Model (BSIMM), Microsoft Security Development Lifecycle (SDL), and National Institute of Standards and Technology Cybersecurity Framework (NIST CSF) as well as cyber security requirements of customers and governments. Such activities include security requirements, design, development, test, release, and vulnerability management. Check points are used in the process to ensure that security activities are effectively implemented in product and solution development. This practice improves the robustness of products and solutions, enhances privacy protection, and ensures Huawei provides customers with secure products and solutions.

In the design phase, Huawei has extended the Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege (STRIDE) threat model to include the attack tree and privacy impact assessment (PIA) elements, calling this new model Advanced STRIDE (ASTRIDE). Huawei has also developed security design standards to guide engineers in security design, with reference to the best practices in the industry.

In the development phase, Huawei has developed its own secure coding standards with reference to the best practices of the industry's secure coding standards of Computer Emergency Response Team (CERT), Common Weakness Enumeration (CWE), SysAdmin, Audit, Network, Security (SANS), and Open Web

Application Security Project (OWASP), and continuously carried out security training and exams for coding personnel.

In the test phase, Huawei has designed test cases based on the threat modeling to verify the effectiveness of the threat mitigation measures designed. Huawei has adopted a "many eyes and many hands" security verification mechanism. In addition to security tests of product lines, Huawei established the Independent Cyber Security Lab (ICSL), which is independent of the R&D system, to be responsible for the final verification of products. Test results are directly reported to the Global Cyber Security & Privacy Officer (GSPO), who has veto power over product launch. Third-party testing and verification schemas are supported with the cooperation of customers and industry regulators.

In addition, measures are taken to enhance software security, for example, compiler security options are used in the build process, and security scanning is implemented before version release. The digital signature center grants each software program a digital signature, which can be used by customer engineers to verify the software integrity before software loading. This mechanism prevents software from being tampered with or replaced.

Huawei R&D has systematically made good progress in live network operations. The secure operation of hundreds of LTE networks over the past 10 years is evidence for product security assurance. The BSIMM assessments over the past 5 years show continuous improvements in Huawei's security practices, ranking top among 120 ICT companies.

Huawei is committed to not only building confidentiality, integrity, availability, traceability and user privacy protection in 5G equipment based on the 3GPP security standards, but also collaborating with operators to build high cyber resilience in networks from the O&M perspective. Looking to the future, as cloud, digitization, and software-defined everything become more and more prevalent and networks become more and more open, Huawei R&D has initiated the transformation for enhancing software engineering capabilities to continuously build trustworthy, high-quality products and solutions.

4.1 Industry-leading Security Measures for the Access Network

5G security standards bring enhancements to air interface and transport security mechanisms used in 4G.

- 5G inherits security protection mechanisms in 4G, and adds data integrity protection for the user plane to prevent data tampering on the user plane. In addition, 3GPP R16 standards may include protection for broadcast messages and rogue base station detection schemes based on messages reported by devices to **enhance confidentiality, integrity, and availability.**

- In terms of transport security, the N2/N3 interfaces connecting the access and core networks and Xn interfaces connecting base stations use IPsec in 4G for transport security. 5G additionally supports

Datagram Transport Layer Security (DTLS) over Stream Control Transmission Protocol (SCTP) to secure signaling transmission on the control plane, ensuring transport security between RANs and core networks. Operators can select a transport security protection scheme based on security requirements to **prevent data breach and attacks on the transport network.**

- 3GPP R15 standards define a reference architecture, known as the central unit/distributed unit (CU/DU) split architecture, for 5G gNodeBs. This architecture is not mandatory, and the standards continue to support the CU/DU integrated architecture. In 3GPP standards, the CU is responsible for processing 3GPP Radio Resource Control (RRC), Service Data Adaptation Protocol (SDAP), and PDCP layers, and the DU is responsible for processing Radio Link Control (RLC), Media Access Control (MAC), and PHY layers. **In CU/DU split deployment mode, 3GPP defines physical security isolation between 5G gNodeBs and the core network. Specifically, IPsec can be used to protect the F1 interfaces connecting the CU and DU.** The CU processing capability is required to be less than 5% of the access network capability. CU/DU split deployment does not significantly improve performance or bring any clear value. Instead, it requires extra investment. As such, industry consensus is to favor the CU/DU integrated deployment mode.

- In terms of privacy protection, 5G security standards include encryption schemes for concealing the SUPI to tackle the risk of user information leakage through messages sent for the initial UE access, thereby **enhancing privacy protection.**

- The 3GPP will research mMTC standards in R17. Because mMTC devices have limited resources, low transmission data volume, and low transmission rate, the 3GPP will consider the security of functions such as identity authentication, confidentiality, and integrity and reduce the overhead of security-related bits.

On the basis of 5G security standards for network equipment, Huawei further provides the following air interface and system security hardening measures:

Base stations can identify DDoS attacks launched at them through the air interface from malicious UEs and mitigate the attacks using specific control mechanisms, ensuring the availability of base stations.

4.2 Security Assurance Above Standards for the Core Network

Security Standards

5G security standards bring enhancements to key hierarchy, roaming security, and transport security mechanisms for 5G core networks used in 4G.

- In terms of key hierarchy, the UE access authentication and key derivation framework and NAS signaling encryption and integrity protection for UE access are inherited in 5G. 5G enhances access authentication by defining a unified authentication framework for both 3GPP and non-3GPP access and supporting EAP Authentication and Key Agreement (EAP-AKA) and 5G AKA for **enhanced security flexibility.**

- Roaming networks may access to core networks. To address this risk, the SEPP can be deployed on 5G networks to provide the following security protection functions for signaling messages at the roaming boundaries: topology hiding, message filtering, TLS channels, and application-layer security protection for roaming messages through the IPX networks. This prevents data breach and unauthorized tampering at the transport and application strata, thereby **enhancing transport and data confidentiality and integrity.**

- 5G also provides security requirements and functions for user access authentication on the home operator networks to **address the threat of home network spoofing by roaming networks.**

Cloud Security

Compared with legacy architecture, the cloud architecture introduces universal hardware and runs network functions in a virtual environment, facilitating low-cost network deployment and quick service provisioning. Globally, there are already a large number of 4G core networks deployed in the cloud. Huawei has obtained abundant experience in cloud core network solutions and deployments together with operators.

Huawei complies with security protocols and architectures defined by industry-recognized virtualization standards. The European Telecommunications Standards Institute (ETSI) is responsible for standards formulation for network functions virtualization (NFV) technologies used in the cloud architecture. Huawei adheres to NFV security standards, such as SEC009 (multi-tenant hosting management security) and SEC002 (security feature management of open source software), defined by the ETSI.

Huawei believes that NFV security isolation is an end-to-end solution. From the data center (DC) data interface to the VM on the core server, NFV security requires a complete security solution that covers both the external and internal layers and everything in between. The NFV security isolation solution includes intra-DC security zone isolation, security isolation of different service domains in a zone, isolation of different host groups in a zone, isolation of VMs in a host, and a series of security hardening measures, implementing outside-in NFV security isolation.

Huawei has mature virtualization security applications in 4G. In terms of 5G network equipment security, Huawei provides the following standards-based security hardening measures:

In an operator network, intra-DC zones with different security levels are designed based on services. Each zone is isolated by a firewall. Users cannot directly access zones with higher security levels. Instead, they can access only through specific servers.

In a security zone, domains are usually used to further classify and isolate services. For example, operator network services are generally classified into O&M domain, gateway domain, control domain, and data domain. Different service types are aggregated into different domains. Domains are isolated from each other by firewalls and only authorized access is allowed.

In a multi-vendor environment, intra-domain host isolation is also needed. In the same host, VMs, virtualization layer, and even CPU, storage, and network security isolation schemes can be used for further isolation.

To improve system attack detection and response capabilities, security hardening measures can be taken for systems (such as the OS, container, and database), thereby implementing security isolation and system security monitoring and audit on the management, signaling, and data planes.

MEC Security

In the Mobile Edge Computing (MEC) architecture, the computing capabilities of cloud data centers are moved to the edge of the core network. The existing cloud and virtualization security technologies can be leveraged together with the enhanced third-party authentication and authorization management and user data protection to build security for edge networks. MEC security domains must be strictly defined based on services and deployments. If third-party applications are deployed in MEC, security isolation and security measures must be implemented for software, resources, systems, and Application Programming Interfaces (APIs).

Slicing Security

Network slicing is introduced in 5G networks so that a network can support multiple types of services. On the basis of security features of 5G networks, network slicing provides more security assurance measures, including:

- Slice isolation: Mature cloud and virtualization isolation measures, such as physical isolation, VM resource isolation, virtual extensible local area network (VXLAN), virtual private network (VPN), and virtual firewall, are available to implement precise and flexible slice isolation, ensuring effective isolation of CPU, storage, and I/O resources among tenants.

- Slice access security: On the basis of existing user authentication and authorization mechanisms on the 5G network, network slicing allows slice access authentication and authorization for users by operators and vertical industries collaborating together. This ensures authorized access to slices and controllable application of slice networks and resources by vertical industries.

- Slice management security: The slice management service uses the bidirectional authentication and authorization mechanisms. Security protocols can be used for slice management and between slices to ensure communication integrity, confidentiality, and anti-replay. In the slice lifecycle management, the slice templates and configurations have a check and verification mechanism to prevent slice access failures caused by incorrect configurations or security risks of data transmission and storage. The 3GPP is researching the security of vertical industries in R16 to further develop slice-level user authentication and privacy protection mechanisms.

4.3 Build High Resilience for Network Deployment and Operations Through Collaboration

In terms of business operations, it is imperative to follow the security design principles of attack and defense. Specifically, enhanced cyber resilience based on confidentiality, integrity, and availability is critical in the design of cyber security. To speed up service recovery if a security incident occurs, the design must realize continuous monitoring and response to security incidents so that their impact scope and resulting service loss can be minimized. Huawei, as a vendor, uses the Identify, Protect, Detect, Respond and Recover (IPDRR) methodology of the NIST CSF to identify and control key risks in live-network services and build cyber resilience with operators. By using IPDRR, Huawei can help operators that provide critical information infrastructure to better meet the regulatory requirements for cyber resilience.

- The equipment supports system security monitoring and auditing, as well as **system traceability.**

- The equipment supports secure boot to prevent tampering during the system boot and integrity check on important software files and running code to prevent tampering at runtime, **enhancing system integrity protection.**

- Huawei provides the HiSec security solution to **support E2E cyber resilience, covering security management, threat detection and analysis, and response and recovery.** With reference to the NIST CSF, HiSec builds cyber resilience using six key technologies: efficient vulnerability management, chip-based full-stack system protection, adaptive data security, intelligent threat detection, automated response orchestration, and open security ecosystem enablement.

4.4 End-to-End Privacy Protection Measures

5G systems require E2E measures for privacy protection based on the EU's General Data Protection Regulation (GDPR) requirements.

- 3GPP 5G standards define that user IDs are encrypted during transmission over the air interface, and encryption and integrity protection are performed on the end-to-end transmission channel to prevent personal data from being stolen or tampered with.
- User plane data protection: Both the air interface and transmission channel support encryption and integrity protection according to 3GPP standards.
- The following measures need to be taken when user identity data is collected during network O&M:

  (1) All user operations must be authorized before collection.

  (2) Collected data is encrypted during storage and processing to prevent data breach. The data is automatically deleted upon expiry of the personal data storage period.

  (3) For boards returned to the manufacturer, a secure deletion mechanism is provided to avoid data breach during repair.
- Documentation must be provided to describe how network equipment handles personal data in compliance with privacy requirements.

5 Recommendations for Operators' Security Best Practices for 5G

On top of the 3GPP security standards endorsement, operators need to develop a consistent end-to-end security framework that addresses both their network equipment and their network management. It should encompass more than just an operator's backhaul and core networks and base stations. Other network elements, such as interconnection gateways, firewalls, and IT servers (such as DHCP, DNS, and RADIUS servers) must also be considered in the overall security framework. By taking a holistic approach in designing such a framework, operators can ensure that there are no single points of failure within the network or at the border with other networks. The security of 5G networks has to be developed as an end-to-end logical layer addressing the specificities of each of the following aspects:

- Network security architecture, as described in section 3.1 of this white paper
- OAM
- Border interfaces to external networks (e.g. Internet) and intranets

A comprehensive and secure set of rules is required, in addition to the network security architecture, with which operators must follow to operate the O&M management layer. O&M is crucial in controlling the risk of entire network. Strict security rules should therefore be applied for each O&M task, with zero tolerance for how O&M data flows are processed. This should include traditional procedures, such as equipment configuration management and fault management, as well as the more advanced features such as slicing. Strict admin control is clearly a legitimate baseline for granting access rights (among options such as read only/write/copy/full control) to filter access to sensitive information.

In order to provide network resilience on top of the OAM system, new technologies such as Artificial Intelligence (AI) / Machine Learning (ML) great potential to detect and analysis the security threats to the network operation. An alternative is NIST CSF, which could be a best practice for operators to build end-to-end network resilience management.

Network security needs to continuously evolve in order to address new potential security risks coming from the open Internet and the development of new services. In-house or third-party security audit, or both, should be encouraged as a best practice for empowering mobile networks (not limited to 5G only). Operators need to be alert and always one step ahead of possible security threats.

6 Suggestions for Regulators on 5G Security

Security is part of cellular networks definition for 5G. Compared to previous wireless technologies, **5G standards include more security features to tackle potential security challenges and lead to security enhancements in the future 5G lifecycle.** Governments can be part of these efforts in controlling risks to operate 5G services in line with country regulations. A recommended win-win strategy to address 5G security is to deliver a plan described as follows:

- Formulation of regulations and laws, involving cross-discussion with all public and private partners, to guarantee a consistent security framework. Governments should take a key role here to define the requirements of their respective countries in terms of security and **encourage the development of new technologies with risk control mechanisms to address both their economic objectives and security needs.** This can be achieved through collaboration with all stakeholders, based on a common goal to define world standards. Governments play a major role in providing incentives to deliver a positive economic output for their respective countries, in terms of both leveraging innovations (5G in the context of this report) and guaranteeing that regulations are available for defining key aspects such as the security agenda, security assurance mechanism, certification program, and policies.

- Operators should be the major responsible body for the operation of network infrastructure and implementation of risk management according to the country's security regulations and official standards bodies. In addition to this, governments can implement specific policies to obtain oversight on the security level of each network operating in the country.

The time is now for government regulators to work closely with all relevant industries and partners. In this way, governments can deliver a consistent set of regulations to address 5G security while at the same time allowing operators to take responsibility for the overall implementation. It is also important to obtain the support of network equipment suppliers and relevant verticals.

7 Build Security Through Collaboration to Tackle Future Security Challenges

5G is becoming a reality and the lifecycle for 5G is going to be lasting for a while. Based on successful experience for 4G security, controlling 5G security risks is achieved through joint efforts of all industries. To control risks in the 5G lifecycle, we need to continuously enhance security solutions through technological innovation and build secure systems and networks through standards and ecosystem cooperation

- **Equipment vendors:** Vendors should contribute industry security standard work, comply with standards, and integrate security technologies to build secure equipment. Together with customers and other stakeholders, vendors should provide capability to support the operators to assure secure operation and cyber resilience.
- **Operators:** Operators are responsible for the secure operations and cyber resilience of their own networks. 5G networks are private networks. The boundaries between different networks are clear. Operators can prevent external attacks with firewalls and security gateways. For internal threats, operators can manage, monitor, and audit all vendors and partners to make sure their network elements are secure.
- **Industry and government regulators:** As an industry, we all need to work together on standards. This is our shared responsibility. In terms of technologies, we need to continuously contextualize 5G security risks (in slicing, MEC, mMTC and other scenarios) and enhance protocol-based security. In terms of security assurance, we need to standardize cyber security requirements and ensure that these standards are applicable to and verifiable for all vendors and operators.

To build a system that we all can trust, we need aligned responsibilities, unified standards, and clear regulation.

References

[1][3] 3GPP TR 33.899: "Study on the security aspects of the next generation system", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3045

[2] 5G Security Transparency: http://www.circleid.com/posts/20181209_5g_security_transparency/

[4] 3GPP TS 33.501: "Security architecture and procedures for 5G System - 5.2.5 Subscriber privacy", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[5][6] 3GPP TS 33.501: "Security architecture and procedures for 5G System", https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3169

[7] 3GPP 5G Security: http://www.3gpp.org/news-events/3gpp-news/1975-sec_5g?from=timeline

[8] Network Equipment Security Assurance Scheme: https://www.gsma.com/aboutus/workinggroups/working-groups/fraud-security-group/network-equipment-security-assurance-scheme

Trademark Notice

NO WARRANTY

HUAWEI TECHNOLOGIES CO., LTD.
Bantian, Longgang District
Shenzhen518129, P. R. China
Tel:+86-755-28780808

www.huawei.com