ZTE

5G Security White Paper

Security Makes 5G Go Further

May, 2019

Introduction

Following the concepts of network business convergence and on-demand services, 5G introduces a wide variety of access capabilities, a flexible network architecture and higher security, changes the plain mobile communication service model, provides enhanced bandwidth and higher cost performance for the Consumer Internet, and provides a highly customizable network and ICT services for the Industrial Internet.

The wide diversity of vertical industries that can be supported is a prominent feature of the Industrial Internet. The differences in security level requirements, network architecture, traffic characteristics, and protocol types creates complexities in adopting a unified 5G network security architecture for vertical industries. A 5G network security architecture needs to be customized for a specific network based on its social and economic background, regulations and business scenarios.

The stability and health of the Industrial Internet affect the future of the Internet. With the development of 5G standards and applications, large-scale commercialization of 5G is imminent. To make 5G go further, we need to do more to ensure network security.

Content

Chapter One

01 Building a More Secure and Flexible 5G Network

First Choice for Industrial Internet

As a commercial telecommunications network, the mobile network takes into account the mobility, reliability and security of network access from the outset of standards development. Communication is secured by means of SIM/USIM identification, authentication, transport encryption, and access authorization. After decades of refinement by telecommunication operators, standards organizations and vendors, its security architecture has been significantly improved, which makes the mobile network the first choice of the future Industrial Internet.

Inheriting the security features of 4G, the 5G network enhances network architecture, authentication, privacy protection, data transmission security and interconnection security. Compared with non-3GPP access networks, such as WiFi, and enterprise private networks, 5G provides a wider range of mobility, more robust service security, tighter data protection, and better user privacy.

5G provides a bidirectional authentication capability based on a Unified Authentication Framework, which enables terminals and the network to mutually confirm their validity. In this way, 5G not only prevents fake base stations or hot spots from information leakage, but also prevents unauthorized access. By user authentication, the network can trace the user behaviors, increase the legal risks to the attacker, and effectively reduce attacks.

The 5G network provides an end-to-end secure channel for each terminal to isolate from each other effectively. Even if a terminal is infected, it is difficult for the malware to spread to the others throughout the 5G network.

The traditional Consumer Interne was originally designed to be open, which has proved to be a source of network security problems. As the future Industrial Internet will connect high-value assets in important fields such as finance, energy, industry, and transportation, a semi-closed or closed network will be a better choice. 5G network slicing can provide not only network customization for different SLA services, but also secure network isolation capabilities.

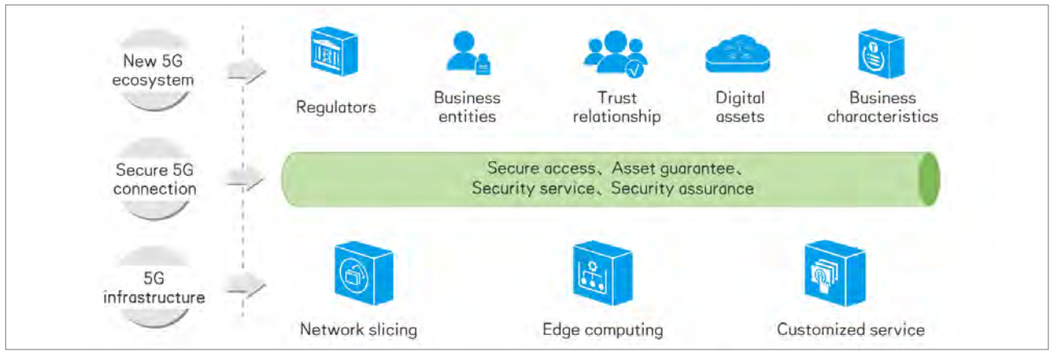
To enhance the security capabilities of a 5G network for different service scenarios and provide users with more comprehensive and flexible network security options, 3GPP is researching and formulating security standards for Enhanced SBA (Service-Based Architecture) security, wireless & wireline convergence, non-public network (NPN), NPN-PLMN interaction, enhanced cellular IoT, uRLLC services, authentication and key management for applications based on 3GPP credentials, and V2X Services.

ZTE believes that 5G will become the cornerstone of the entire society. Assuming that the security of traditional mobile networks has considerable impact on the Internet economy, then 5G network security will have major influence on the security of social and economic fields. So we need to analyze 5G security challenges in a more comprehensive and systematic way based on the security framework defined by 3GPP.

New Security Challenges

Redefined 5G infrastructure

The 5G business ecosystem introduces new regulators and business entities. It also brings more trust relationships and digital assets. In order to build a diversified and trustworthy 5G ecosystem, enable 5G to bear digital assets with different service characteristics, and achieve the 5G business objectives defined by the ITU-T, the network infrastructure is not merely traffic bearer. It is also redefined by new technologies such as SDN/NFV and MEC to provide on-demand network services through slice customization.



5G Capability Architecture and Security Guarantee

Secure access capability of 5G private networks

With the continuous evolution of the Internet from consumption to industry, involving critical infrastructures such as energy, industry and transportation, 5G bears higher business value and more social influence than traditional consumer services. Therefore, the network characteristics are no longer limited to bandwidth and traffic rate but include security and reliability. In the future, 5G will profoundly penetrate our lifestyles, and affect the whole of society, industrial innovation and economic growth. To carry high-value services, a 5G network must be able to provide higher security and reliability than traditional high-grade private networks, and needs to provide further security reinforcement capabilities based on network slicing.

In 5G private networks with security requirements for critical infrastructure, the business system can be divided into different regions according to the service value and SLA characteristics. Different regions use different network slices with different security attributes.

Secure guarantee capability for cross-industry assets

5G connects key infrastructures in IoT and vertical industries, and enables the mobile network to evolve from person-to-person connections to machine-to-machine connections, resulting in potential mutual penetration of security threats between the IT domain and the OT (Operation Technology) domain. The consequences of attacks are exacerbated by the fact that such attacks are often targeted at people, assets and critical infrastructures that connect the physical world. Because the infrastructures are located at the network edge, MEC will be an important choice and barrier for vertical industries. Operators need to take necessary security measures to protect MEC nodes and the customer data assets.

Continuous innovation in security capabilities

On one hand, with the in-depth integration between networks and businesses, 5G network security capabilities need to be innovated. Based on the business characteristics and security situations of specific industries, new intelligent detection technologies and new defense mechanisms need to be introduced to provide continuous innovative 5G network security solutions. On the other hand, 5G can expose its own security capabilities to the vertical industries, reducing their security development and deployment costs, and improving the efficiency of business innovation.

Diversified security assurance

The integration of the Industrial Internet and the 5G network will also have an impact on the security assurance system. Firstly, the security regulations are diversified. In comparison with telecommunications networks, the financial, energy, and industrial networks have different security regulations and standards, data protection norms, and security evaluation standards. Secondly, the assets are diversified. The equipment, platforms and applications in MEC have different owners and users, and may also require an operation and maintenance system across multiple organizations. How 5G adapt to a diversified security assurance system, or whether it is possible to build a unified security assurance system remains to be explored.

Chapter Two

02 Customizable Slice Security

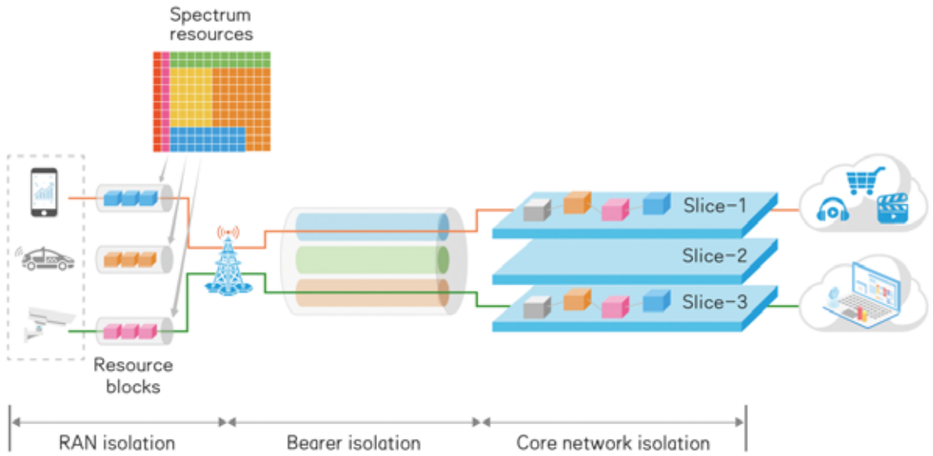
Network Slicing and Slice Security

A 5G network slice is a logical network constructed on the cloud core, bearer and RAN network infrastructure by using the network virtualization technologies in accordance with application requirements. Operators can orchestrate separate 5G network slices for multiple industry applications on a shared network infrastructure through capability exposure, intelligent scheduling, and secure isolation, to provide differentiated network services.

Network slicing helps to build an open network ecosystem around operators, to fully exert the potential of the network infrastructure and to exploit new revenue sources. For vertical industries, network slices can greatly reduce the TCO of private networks and meet the dynamic network demands using network slice scaling. Network slicing greatly changes a telecommunications network, which lays a solid foundation for the deep integration of telecommunications networks and industry applications. Compared with privacy and closeness of traditional networks, a network slice is a virtualized private network which is built on the common infrastructure. Therefore, security is the key precondition for vertical industries when using network slicing. In addition to providing the traditional mobile network security mechanisms (such as access authentication, encryption and integrity protection of access stratum and non-access stratum signaling and data), 5G needs to provide end-to-end isolation between network slices.

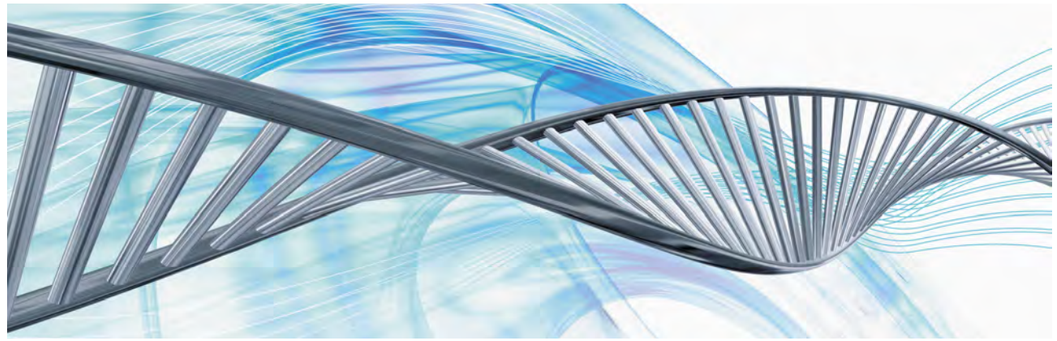
E2E Isolation for Network Slices

Network slices are logically independent dedicated networks that share a common network infrastructure. To achieve high security and availability, 5G shall support isolation between network slices by using physical or logical isolation methods. 5G can ensure end-to-end isolation in RAN, bearer network, and core network, as the following figure shows.



E2E Isolation Model for 5G Network Slicing

Isolation in the RAN



The RAN resources contain the radio spectrum resources and base station processing resources. The network slices on the RAN side need to be isolated in terms of spectrum resources and base station processing resources.

In the 5G OFDMA system, spectrum resources are divided into different resource blocks in terms of the time domain, the frequency domain and the spatial domain for bearing the data transmitted between terminals and base stations. Spectrum resources can be isolated physically and logically. Physical isolation means allocating dedicated spectrum to network slices. A network slice uses its own specific spectrum resources. In this case, the resource blocks allocated to the slice are continuous. Logical isolation means that resource blocks are allocated as required by different slices. The resource blocks allocated to each slice are not continuous, and several slices share the total spectrum resources. Because resource block allocation processes are orthogonal to each other and independent from each other, logical spectrum isolation is implemented through resource block isolation.

Due to the orthogonality of resource blocks, 5G provides equivalent slice isolation for network slices using shared and dedicated spectrum. However, the coverage range and quality of the dedicated spectrum are not as good as that of the shared spectrum. When a data packet is large or if the user is at the edge of the cell, a data packet cannot be transmitted using wider spectrum, which increases the transmission latency. In addition, the spectrum resource under physical isolation cannot be used flexibly, and the leasing cost of the dedicated spectrum is high. Logical isolation enables the base station scheduler to allocate resources according to the transmission requirements of different slices, and improves the utilization of spectrum resource. Therefore, logical isolation is preferred if there is no special requirements.

The traditional BBU functions are reconstructed in the form of DU and CU. The DU is used to process L1 (PHY) and L2 (MAC) layer functions, such as resource block scheduling, modulation and coding and power control, while the CU is used to process functions above L2 layer, such as packet data convergence and switching. The isolation of base station processing resources can be implemented on the DU and CU. The DU runs on dedicated hardware, while CU can run on dedicated or universal hardware. The processing resources on the DU may be shared by slices (but isolated logically) or occupied by each slice physically, for example, different DU boards or processor cores are assigned to different slices. Sharing processing resources on the DU is preferred because of cost efficiencies. If the CU also runs on dedicated hardware, sharing processing resources on the CU is also preferred. If the CU runs on universal hardware, the slice isolation on the CU can be achieved by the NFV technology, for example, assigning slices with different virtual machines or containers. Isolation on the DU and CU can be achieved individually or together, depending on isolation requirements.

Isolation in the bearer network

Network slice isolation in the bearer network can be realized by soft isolation or hard isolation.

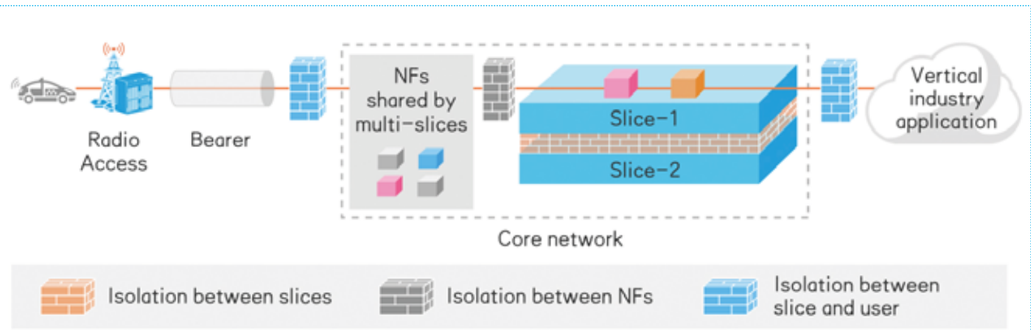
Soft isolation is achieved by mapping network slice identifiers to VLAN tags. A network slice has a unique slice identifier and encapsulates a unique VLAN tag. The slices are isolated by VLAN isolation. Although this isolation method divides the data of different slices into VLANs, data of all the slices with VLAN tags are still mixed together to be scheduled and forwarded. So soft isolation cannot be realized at the hardware or time slot level.

Based on the Ethernet technology, hard isolation uses FlexE technology to create another "cushion" between L1 (PHY) and L2 (MAC) layers. FlexE divides a physical Ethernet port into several Ethernet elastic pipes based on time slot scheduling, enabling the bearer network with not only good isolation features, same as of TDM (Time Division Multiplexing) but also statistical multiplexing and the high network efficiency features of Ethernet.

Soft isolation and hard isolation can be combined to isolate slices in the bearer network. After logical isolation by VLANs, the slices can further be isolated by FlexE at the time slot level.

Isolation in the core network

The 5G Core(5GC) is built based on a virtualized infrastructure. 5GC has many Network Functions(NFs), some of them are slice-specific while others are slices-shared. Therefore, slice isolation in core network uses the multi-level isolation methods, as the following figure shows.



5G Core Network Isolation Model

Isolation between network slices

Since slices share physical resources, the slices must be isolated to ensure that one slice exception does not affect other slices. By physical isolation, independent physical resources can be allocated to slices requiring higher security. This isolation method is costly and not flexible enough for resource allocation. By logical isolation, a mature virtualization isolation method is implemented at the network infrastructure layer. VLAN/VXLAN partitioning is used at the network layer, and role-based and domain-based management is used for orchestration, that is, tenants can orchestrate and manage their own slices only, and do not have the right to manage slices of others.

Isolation between NFs

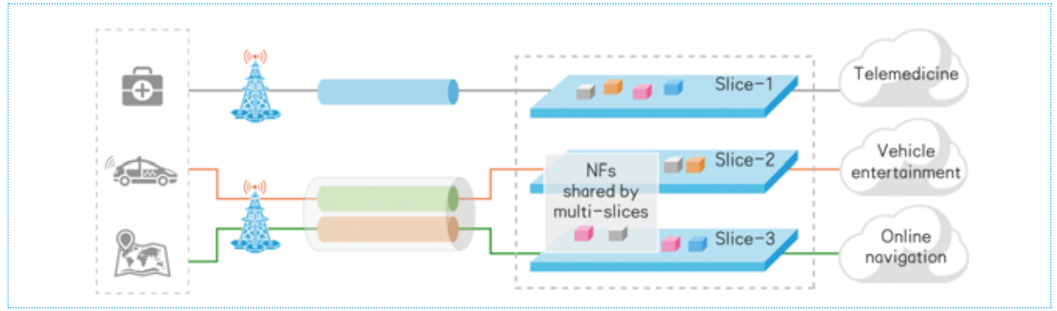
NFs having different security levels can be placed into different security domains. There are a large number of MEC applications on the 5G network. NFs such as the UPF need to be relocated from the core to the network edge and can be deployed at the same location as the base station or the DU/CU. This means that the relocated NFs and other core NFs will exist in different security domains. For the case where a slices-shared NF accesses a slice-specific NF, it is necessary to set a security protection mechanism (such as a white list) to prevent unauthorized access..

Isolation between network slices and users

In order to protect CN (Core Network) slices from attacks, it is necessary to set up security isolation between the slices and the end users, and between the slices and the industrial applications. Isolation between the slices and end users can be based on access controls. Before an end user accesses a slice, the user must be authenticated to ensure valid access. In addition, the user accesses the correct slice based on the user subscription information and the slice selection mechanism. The isolation between the slices and industrial applications is based on virtual or physical firewalls and the corresponding access policies.

Network Slice Customization

To provide differentiated network service customization capabilities, the 5G network needs to be closely integrated with the service characteristics and requirements of the vertical industries. Security is a basic factor that must be considered in the process of customizing network slices. The following figure shows an example of network slice customization.



Customized Network Slices Combined with Vertical Industries

For applications requiring low latency but high security, such as telemedicine service, 5G network services should meet the highest slice security isolation and access control requirements. Therefore, when designing, orchestrating, and deploying slices, the following security protection measures can be taken: isolating radio interfaces in the NR to assign the applications with independent cells and special frequency bands, isolating physical resources in the CN to implement physical isolation, and transmitting data over dedicated lines in the bearer network to ensure the security of data transmission.

For Internet applications which are not as demanding high security, such as vehicle entertainment and online navigation, the slices can be designed, orchestrated and deployed based on the following security mechanism: The RAN slices can be isolated in the shared-cell by resource block isolation; the CN slices can share some control plane NFs and be isolated on the user plane and partial control plane; the bearer network slices can share transmission resources and be logically isolated by policy routing, SDN, IPsec or FlexE.

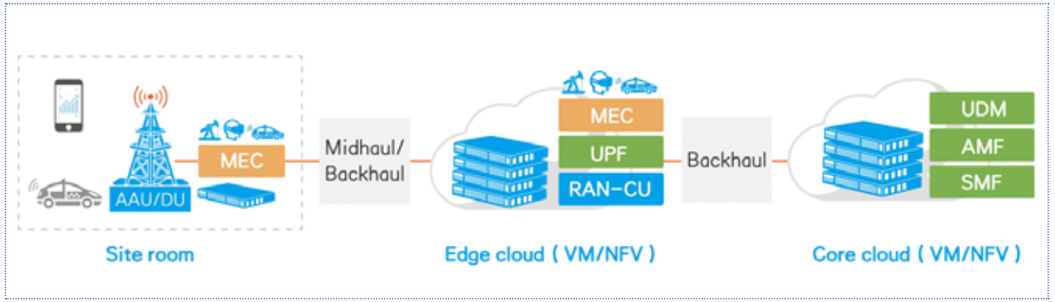
03 Chapter Three MEC Security

Application of MEC in 5G

MEC is one of the core technologies for the diversification of 5G services. With a distributed network architecture, MEC pushes the service capability and application to the edge of the network, and changes the separation of network and services. It is a representative capability of 5G.

5G supports MEC by relocating the UPF and steering traffic. MEC can expose capabilities, such as LCS and bandwidth management of mobile networks, to the upper-layer applications, so as to optimize business application, develop new business models, and enhance network value.

The MEC deploys data caching, traffic forwarding and applications close to users, it can greatly reduce the service latency in order to meet the low-latency requirements of services such as the V2X Network and the Industrial Internet, reduce the bandwidth pressure from HD video and AR/VR services on the transport network, and improve the content distribution efficiency and user experience.



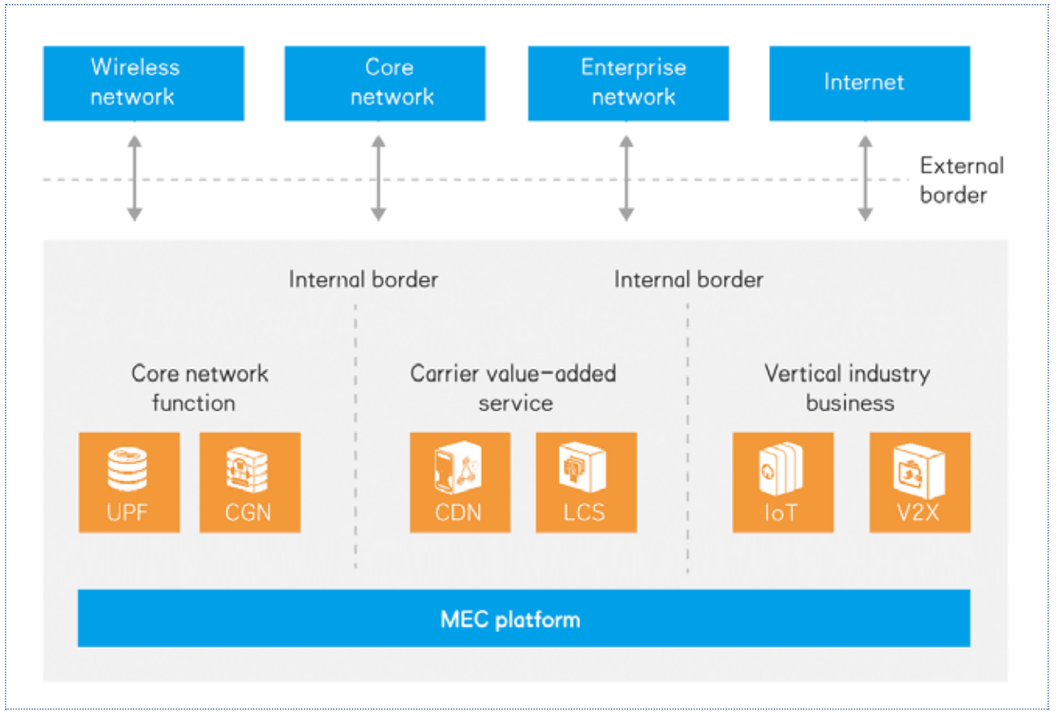
MEC in 5G Network

With the imminent commercialization of 5G and the deep integration of 5G networks and vertical industries, a number of new services requiring enhanced bandwidth and ultra-low latency will gradually emerge. Therefore, it is necessary to study the security issues faced by MEC.

For MEC, security not only protects MEC infrastructure, network functions and data assets, but also enables its deployment in enterprise campuses or designated security zones to provide more secure and reliable services.

Security as Key Element of MEC

A typical MEC carries some core network functions, operator value-added services, and vertical industry services. It interconnects with the RANs, CNs, government and enterprise networks, and the Internet, and takes advantage of edge deployment to meet the needs of 5G services. In general, MEC is an extension and enhancement of central computing, which inherits the advantages of central computing and faces the threats similar to that of central computing. Due to the changes in physical location, network boundary and customers, the security requirements faced by the MEC need to be re-evaluated.



MEC Structure

Compared with the traditional telecommunications network, MEC has undergone significant changes in terms of the network architecture and operational models, which have spawned new security threats and challenges, as described in the following sections:

Network infrastructure

Moving MEC nodes closer to the edge of the network weakens the management capability because the MEC platform and MEC applications are in a relatively insecure physical environment, which increases the risk of unauthorized access, sensitive data leakage, DoS/DDoS attacks, and physical attacks to equipment. In addition, the operator network functions are deployed on a platform together with untrusted third-party applications, which results in security issues such as network boundary ambiguity, virtual machine escape, image tampering, data leakage, all of which threaten operator assets and industry assets.

Network function

With MEC some core network functions can be deployed at the network edge, which increases the threats to NFs and enlarges the attack surface area of the core network. Traffic does not pass through the core area, so fraudulent charging attacks may exist. In the traditional telecommunications network, the core network gateways, such as GGSN and PGW, collect charging information and report it to the charging system. If 5G network's traffic charging is executed in the edge area, the UPFs are deployed at access sites, such as a stadium or a shopping center, the charging records may be tampered with. In addition, due to the limited service coverage of MEC nodes, once a user switches across nodes, for example, the user takes a high speed train, the MEC nodes may be confronted with security issues, such as mutual trust between sites and secure delivery of session contexts.

Network operation and maintenance

MEC is a comprehensive system, including the mobile communication networks, MEC capability exposure services, and vertical industry applications. New trust models need to be constructed for the integration of multiple systems, including the trust model between users, industry applications and MEC network services (such as LCS) and the trust model between mobile devices, network slices and MEC platforms. As the MEC architecture and 5G mobile network are defined in different standards, how to integrate them to meet different operation and maintenance requirements is a key topic in MEC research.

MEC Security Protection

As an extension and enhancement to central computing, MEC can inherit the security protection methods of the telecommunication cloud data centers, including cloud infrastructure hardening, and virtualized network security services. Moreover, specific security protection measures based on services need to be taken. The four aspects described below are key considerations.

Infrastructure hardening

1. **Physical security**: Depending on the application scenario, MEC nodes can be deployed in an edge data center, an unattended site room, or even in a site closer to the users. Because the MEC equipment is located in a relatively open environment, the equipment is more vulnerable to physical damage and requires physical security measures. The sites specified by industry customers need to be evaluated in terms of physical environment security. The physical environment and even the core devices need to be protected through access control and personnel management. The structure and overview design of MEC equipment needs to consider anti-theft and anti-damage measures, and strengthen I/O access controls. It is recommended that trusted computing technologies be used to secure key data. In addition, MEC nodes must support high availability in harsh physical environments.

2. **Platform security:** Based on the cloud infrastructure and NFV technology, MEC can use virtualized security solutions, such as virtual machine security and container security. In order to ensure the security of the running software, the MEC needs to support signature (publisher) and verification (receiver) for the VNF software packages between different delivery phases, and signature verification is required for software packages released by vendors. For the MEC nodes deployed in areas poorly controlled by operators, it is necessary to introduce the security reinforcement measures to strengthen the platform management security, data storage and transmission security, such as introducing trusted computing technology to construct a trusted MEC platform by step-by-step verification from the system booting to upper-level applications.

   To ensure higher availability, MEC resource pools can be established between homogeneous MECs to provide mutual remote disaster recovery. When an incident occurs, the services on MEC can be quickly switched to other MECs to ensure service continuity.

3. **Network security:** From the aspect of network boundary, MEC includes Internet interfaces, enterprise network interfaces, wireless device interfaces, capability exposure interfaces, and third-party application interfaces. Traditional security technologies such as border defense, authentication, isolation and encryption need to be retained in MEC. From the aspect of components, MEC is divided into different functional domains, such as the management domain, the core network domain, the service capability domain, and the third-party application domain. Since the MEC contains services from different providers, it is necessary to introduce various security capabilities to isolate operators, industries and Internet services, and isolate network slices. Moreover, the MEC can use the intrusion detection technology, abnormal traffic analysis, and anti-APT to detect malware. In addition, given the distribution of MEC at the network edge, the detection can be achieved by deploying multiple monitoring points and collaboration between multiple nodes.

Business and application security

The 3GPP 5GC standards support user plane relocation and solves the problem of charging. However, the risks of illegal eavesdropping and fraudulent charging attacks still need to be considered, and strict authentication, isolation or encryption methods are needed to protect the corresponding transmission channels. When the edge domain communicates with the core domain, especially the control signaling and charging services, it is necessary to make full use of TLS/IPSec, 5G protocols, and the 802.11 protocol to implement authentication and transmission encryption.

MEC provides an open platform for deploying customized services and Internet services from the vertical industries, as well as providing complete customizable security mechanisms for comprehensive security assessment and testing. By means of regional isolation, access controls, authentication, service subscriptions, trusted computing, and behavior audit, the MEC can monitor the traffic and behavior of untrusted applications and prevent malicious behaviors from weakening system robustness.

Operation and maintenance management security

MEC contains many data assets of operators and industrial customers. It is necessary to manage each party from the aspects of authentication, authorization and monitoring, and audit the security measures to secure the MEC nodes. Besides using the functions of the traditional network such as Accounting, Authentication, Authorization and Auditing, the system needs to manage the rights of ownership, using and operating data assets in different domains from the aspects of platform and service, network and application, and network slices.

To prevent security vulnerabilities or threats from affecting other functional domains on MEC nodes, the MEC needs to evaluate third-party applications to ensure its compliance and validity. In addition, the MEC regulates the third-party applications by means of application registration, virus scanning, access control, and behavior audit to avoid security problems.

Data assets protection

MEC nodes are located at the network edge where the operators have a relatively poor control, the risk of data theft and leakage is relatively high. Because some vertical industries are demanding in terms of data control, for example, enterprise data is not allowed to leave the factory, MEC has higher security requirements for data storage, transmission and processing.

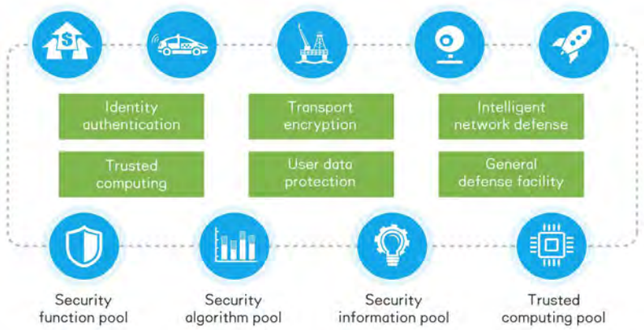
During MEC deployment and service operation, related user data assets must be identified, including but not limited to user identification and access location. The data with high security requirements needs to be encrypted. High value data in vertical industries should be transmitted over IPSec, TLS or other methods to avoid data leakage and tampering. Data processing, analysis, and usage must comply with privacy laws and regulations in combination with data operation object authentication and authorization. If data privacy is involved, personal data needs to be masked.

04 Chapter Four
Security Capability Exposure

Security Capability Exposure

The 5G network capabilities can be exposed to vertical industries through APIs, which enables customization of network services. Security capabilities along with other network capabilities can be exposed through abstraction and encapsulation. In order to meet the security requirements of different vertical industries, the 5G network provides flexible and customizable security services through security capability orchestration in combination with dynamic resource allocation and deployment.

The 5G security capability exposure model is shown in the following figure.



5G Security Capability Exposure Model

The 5G security capability exposure model can be divided into three layers: resource layer, capability layer, and application layer.

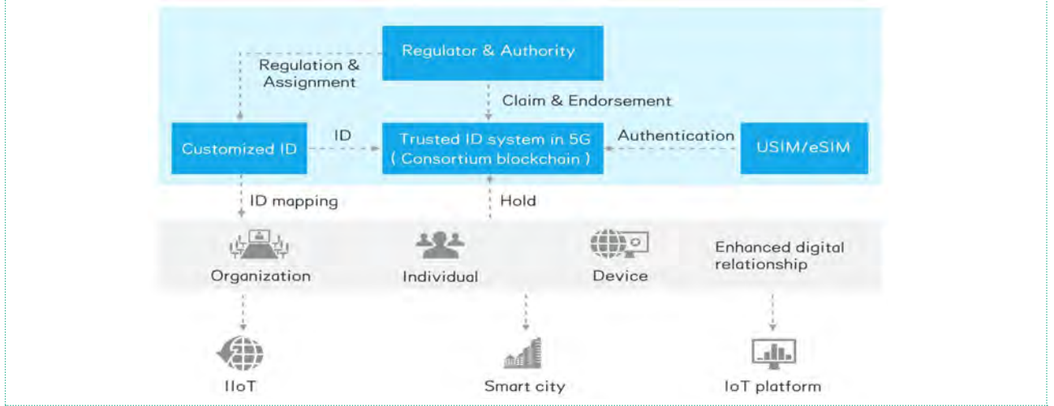
The resource layer abstracts and encapsulates basic resources. Resources can be of various types and forms, provided by resource pools, including the security function pool, security algorithm pool, security information pool and trusted computing pool. The security function pool includes virtual firewall, virtual security gateway and other virtualized security facilities. The security algorithm pool includes a series of encryption, integrity algorithms, and AI algorithms. The security information pool includes various security information resources, such as vulnerability database, virus repositories, and threat information. The trusted computing pool includes hardware modules and software platforms that support trusted computing.

The capability layer provides a variety of security capability sets that can be invoked by the application layer, such as the digital identity system, trusted computing system, and channel encryption system. These capability sets are integrated and maintained by operators in combination with the advantages of the 5G network, and provide highly available and flexible capability APIs.

The application layer orchestrates security capabilities to construct the security defense system to cope with the application security requirements. Because the resource layer has very strong scalability, the application layer can also obtain elastic security capability

Trusted Digital Identity

The Industrial Internet brings many new types of participants and business models to 5G, such as regulators, vertical industry entities, business types, and machine oriented connections. So the regulation, ownership and management, agreement, trust, and endorsement and verification in the 5G ecosystem are complicated and diversified, affecting the network layer and the application layer.



5G Trusted Digital Identity System

With the large-scale deployment of 5G and the popularization of Internet of Things (IoT), a trusted identity system that embodies the new digital relationships among the parties (operators, regulators, vertical industries, OTT, third-party service providers, and consumers) is required for establishing a more diversified digital relationship and supporting 5G business innovation and business model evolution.

The traditional Internet digital identity systems (such as DNS and PKI) are based on individual autonomy and independent third-party CA trust models. It is independent of services and applicable to the Consumer Internet. 5G oriented vertical industries have more appropriate trust subjects, closer endorsers, and more ownership to describe richer digital relationships.

A lot of studies related to digital identity are currently being conducted, including identification systems in vertical industries, IoT-oriented digital certificate systems, 5G integrated identity authentication and cross-operator collaboration. All the existing digital identity systems can be integrated into a unified trusted digital identity framework. Based on USIM/eSIM, new technologies such as blockchain and DID are introduced to rebuild a new digital trust relationship for 5G networks and Industrial Internet, enabling more parties (such as operators, regulators, Internet enterprises, etc.) to participate in a 5G digital identity ecosystem.

Intelligent Network Defense

The architecture, networking, hardware, and software of 5G networks vary with business scenarios, so 5G may be confronted with network attacks of different types and in different means.

5G Intelligent Network Defense Capability

5G networks support machine-oriented connections. In comparison with the Consumer Internet, the behavior mode of machines is simpler and the traffic model is predictable. In addition, network slicing isolates different traffic based on service features. Through rapid learning and training, AI technology can more accurately detect, backtrack, and analyze abnormal traffic and behaviors in vertical industries, provide practical security analysis and alarms for users, and prevent various APT attacks.

AI technology provides the intelligent attack detection capability for the 5G network. It analyzes network traffic and logs continuously to detect useful security events that can reflect behaviors in the network. By using preset models to analyze security events and identifying abnormal behaviors, AI can determine whether there are attacks and locate the source of the attacks.

To further analyze the attack scope and system vulnerabilities, we need to know the spreading process, source, and scope of the attacks, so the network needs to perform correlation analysis on the security incidents to shape the chain of an attack, and clearly display the whole process and scope of the attack. Based on deep-mining of network attack events and analysis on network status, we can evaluate the network security situation, predict possible network attacks, and provide preventative suggestions and measures.

05 Chapter Five
5G Cybersecurity Assurance and Evaluation

5G network security is not merely a technical issue. The integration of 5G and vertical industries, such as manufacturing, energy, and transportation, breaks the barriers of infrastructure and exposes infrastructure to more risks. This imposes more requirements on the 5G network, such as new legal frameworks and regulatory models, additional security assessment and certification requirements. As the core of the 5G ecosystem, the operators need to consult with governments and the regulatory agencies to formulate and carry out appropriate security regulation and supervision processes. Moreover, the security assurance framework and support systems of the traditional Consumer Internet is not suitable for the Industrial Internet. The operators need to construct the 5G security assurance system, operation and maintenance system, and customer service system for the Industrial Internet and provide sustainable, credible and secure network services for users.To set up multiple defense lines, 5G networks need to involve the customers (especially the vertical industries) in the security assurance system to provide customers with stronger security assurance capabilities.

Vendors are important parts of 5G supply chain, their security assurance is the foundation for 5G security. As a leading vendor of 5G, ZTE deeply understands the concerns and attention of consumers, customers, governments, and relevant organizations in relation to cybersecurity, and provides secure and credible 5G solutions and products by building a first-class cybersecurity assurance system.

Adhering to openness and transparency, ZTE launches continuous and comprehensive security audits, embeds security measures into the entire product lifecycle, and works with world class third-party security evaluation agencies and certification institutions to independently test and evaluate the products and services. ZTE is preparing cybersecurity labs across the world where customers and independent evaluation agencies can conduct source code reviews, security design audits, procedural document reviews, black box testing and penetration testing on 5G products to gain customer confidence in the security of ZTE's 5G products and services.

ZTE is looking forward to researching the open and transparent assurance mechanisms for 5G networks together with operators, governments, regulatory departments, and independent security evaluation agencies, and sharing successful security assurance ideas and practices.

06 Chapter Six
Conclusions and Outlook

As a global enterprise, ZTE always regards product and service security as one of its basic responsibilities. In the past 30 years since its foundation, ZTE has insisted on treating security as an intrinsic attribute of products, services and processes and pursuing utmost security from the company's culture, organization and security assurance structure through to product R&D, delivery, and engineering services.

With the acceleration of 5G commercialization and the integration of 5G networks and vertical industries, new service scenarios will emerge constantly, and new technologies will be put into use, which will bring new challenges to network and information security. ZTE will uphold security and compliance to continuously improve the cybersecurity assurance system and strengthen cybersecurity competitiveness. And ZTE will integrate the latest and best practices to drive the innovation of security capabilities and provide highly secure 5G products and services for global customers.

List of Abbreviations

Acronym	Definition
3GPP	3rd Generation Partnership Project
AAU	Active Antenna Unit
AI	Artificial Intelligence
API	Application Programming Interface
APT	Advanced Persistent Threat
AR	Augmented Reality
BBU	Base Band Unit
CDN	Content Delivery Network
CA	Certificate Authority
CU	Centralized Unit
DID	Decentralized IDentifier
DNS	Domain Name System
DoS/DDoS	Denial of Service/Distributed Denial of Service
DU	Distribute Unit
eSIM	electronic Subscriber Identity Module
GGSN	Gateway GPRS Support Node
HD	High Definition
IT	Information Technology
ITU-T	International Technological University-Telecommunication Standardization Sector
LCS	LoCation Service
MEC	Multi-access Edge Computing

Acronym	Definition
NFV	Network Function Virtualization
NPN	Non-Public Network
OT	Operation Technology
OTT	Over The Top
PCF	Policy Control Function
PGW	PDN Gateway
PHY/MAC	Physics/Media Access Control layer
PKI	Public Key Infrastructure
PLMN	Public Land Mobile Network
RAN	Radio Access Network
SDN	Software Defined Network
SLA	Service Level Agreement
SMF	Session Management Function
TDM	Time Division Multiplexing
TLS	Transport Layer Security
UPF	User Plane Function
uRLLC	ultra Reliable & Low Latency Communication
USIM	Universal Subscriber Identity Module
VLAN	Virtual Local Area Network
VM	Virtual Machine
VR	Virtual Reality
V2X	Vehicle to Everything

References:

[1] 3GPP TS 33.501. Security Architecture and Procedures for 5G System[S], 3GPP.

[2] 5G-ENSURE_D2.7 Security Architecture[R], 5GPPP.

[3] ETSI GS MEC-002. MEC Technical Requirements[S], ETSI.

[4] IMT-2020 5G Network Security Requirement & Architecture[R], IMT-2020.

[5] GTI 5G Network Security Consideration[R], GTI.

[6] ZHAO Fuchuan, WEN Jianzhong. Slicing Packet Network Infrastructure and Key Technologies for 5G Mobile Backaul[J], ZTE TECHNOLOGY,2018.8.

[7] Recommendation ITU-T X.rdmase: Requirements and Guidelines for Dynamic Malware Analysis in a Sandbox Environment[R], ITU-T.

[8] Data Model and Syntaxes for Decentralized Identifiers(DIDs). https://w3c-ccg.github.io/did-spec/

[9] Verifiable Credentials Data Model. https://w3c-github.io/vc-data-model

Acknowledgement:

This whitepaper is formulated by the Security Technical Expert Committee under the guidance of ZTE Chief Security Officer Mr. Zhong Hong.

Thanks for assistance from Yan Xincheng, Tang Kai, Mao Yuxin, Hao Zhenwu, Ma Su'an, Christopher Mulley, Xu Xiuli, Li Rui, Liu Jianhua, Zhou Jihua, Wang Yijun, Lin Zhaoji, You Shilin, Lu Haitao, Wei Yuanqing, Ping Li, Tian tian, Lin Jun, Li Chengyuan, and Zhang Can.

ZTE
NO. 55, Hi-tech Road South, ShenZhen, P.R.China Postcode: 518057
Tel: +86-755-26770000 Website: www.zte.com.cn