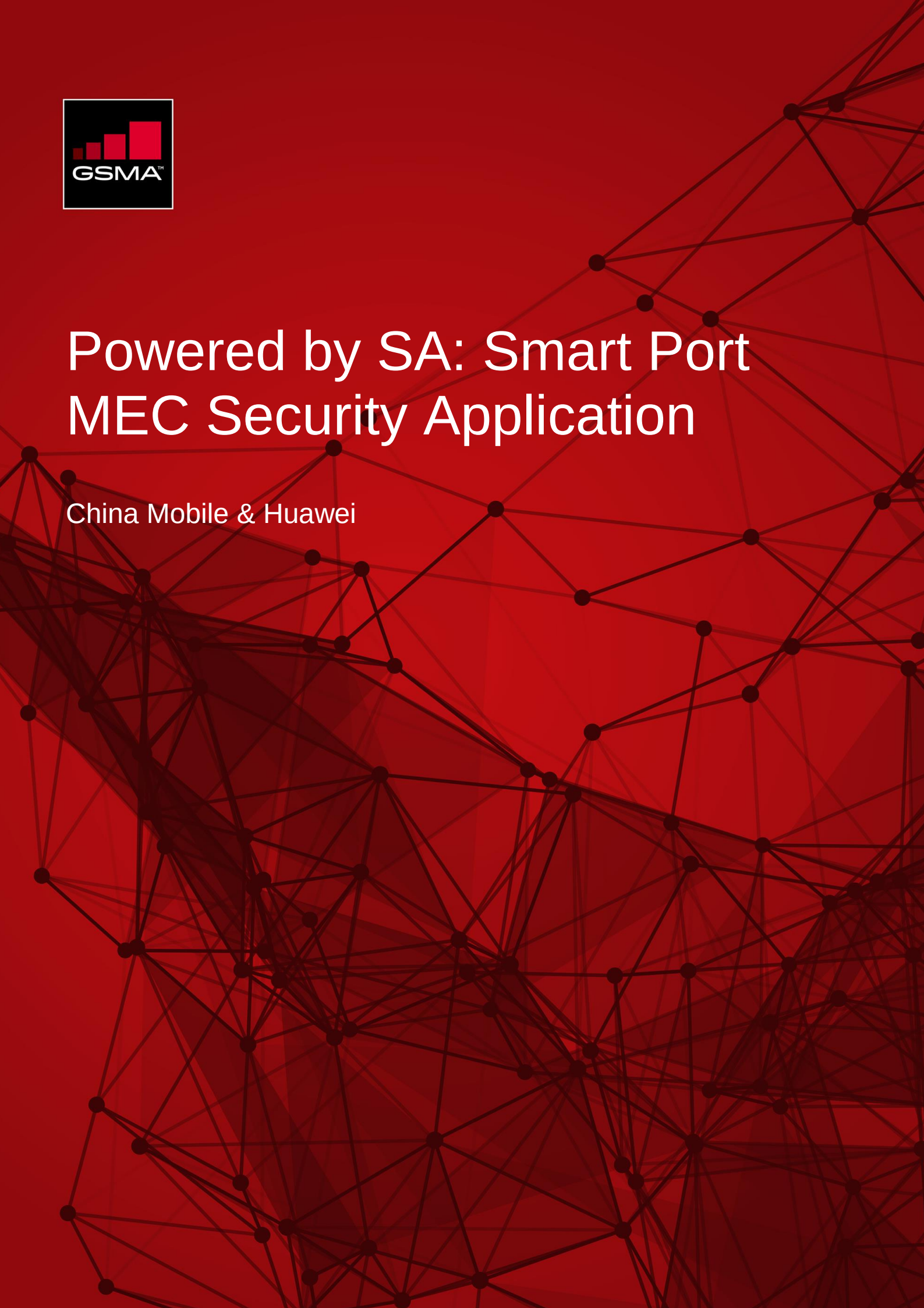

Powered by SA: Smart Port MEC Security Application

China Mobile & Huawei

Table of Contents

Introduction

5G is a key enabling technology that will drive the development of the industrial internet, which in turn, will be critical to accelerating the commercial deployment of 5G. In addition, the requirement of the industrial internet for low latency makes it important to introduce MEC (Multi-access Edge Computing) at the edge of the 5G network. As an example of a typical industrial operation environment, a port is usually densely deployed with heavy mechanical equipment such as gantry cranes etc. Therefore, the deep integration of 5G and MEC technology with ports will have a profound impact on the port infrastructure, transportation organization, and business governance. In this scenario, it is also important to ensure high security and reliability.

In October 2019, China Mobile, Ningbo Port, and Huawei jointly launched the "5G SA Smart Port MEC Security Application" innovation project, focusing on 5G network security protection, MEC security risk elimination, industrial internet application risk control, slicing security assurance, and data security protection. This document outlines typical risks and security solutions for smart port service scenarios, providing practical guidance for large-scale 5G+[1] industrial internet security assessment and security operation and maintenance (O&M). The project has made major breakthroughs in verifying technical feasibility, exploring business expansion opportunities, and fostering the industry ecosystem. It highlights the benefits of the 5G SA network and MEC to enable industrial internet applications, while providing a valuable reference for cooperation between global operators and 5G industry ecosystem.

5G Enables Smart Port Development

Operational efficiency and automation levels of the port are crucial in determining future competitiveness and economic benefits. With the maturity of remote control technology of container cranes, as well as the increase in labor cost and market tension, the need for separating human, machine and intelligent remote control has been increasing.

5G provides ultra-low latency and high bandwidth access capabilities to meet the requirements of remote control, automatic guided vehicle (AGV) driving, and campus security monitoring. In addition, MEC technology implements local traffic processing and logical calculation, saves bandwidth and delay, and further meets the requirements of remote low latency control of heavy machinery equipment and high bandwidth transmission of on-site HD video. Therefore, 5G and MEC can enable the efficient development of smart ports while reducing operation costs.

In particular, 5G NR is directly connected to the 5G core network without relying on 4G network when applying the 5G SA (Standalone) networking mode. With network slicing and MEC technologies, a complete and independent 5G network has the advantages of convenient interconnection, flexible and reliable service, etc., which can be innovatively applied across all industries. Meanwhile, many 5G application innovations will be limited with 5G Non-Standalone (NSA), when considering that the 5G NSA networking mode has limited capabilities in the 5G core network, uplink bandwidth, delay, etc.

[1] 5G+ is the trade mark of China Mobile for 5G services

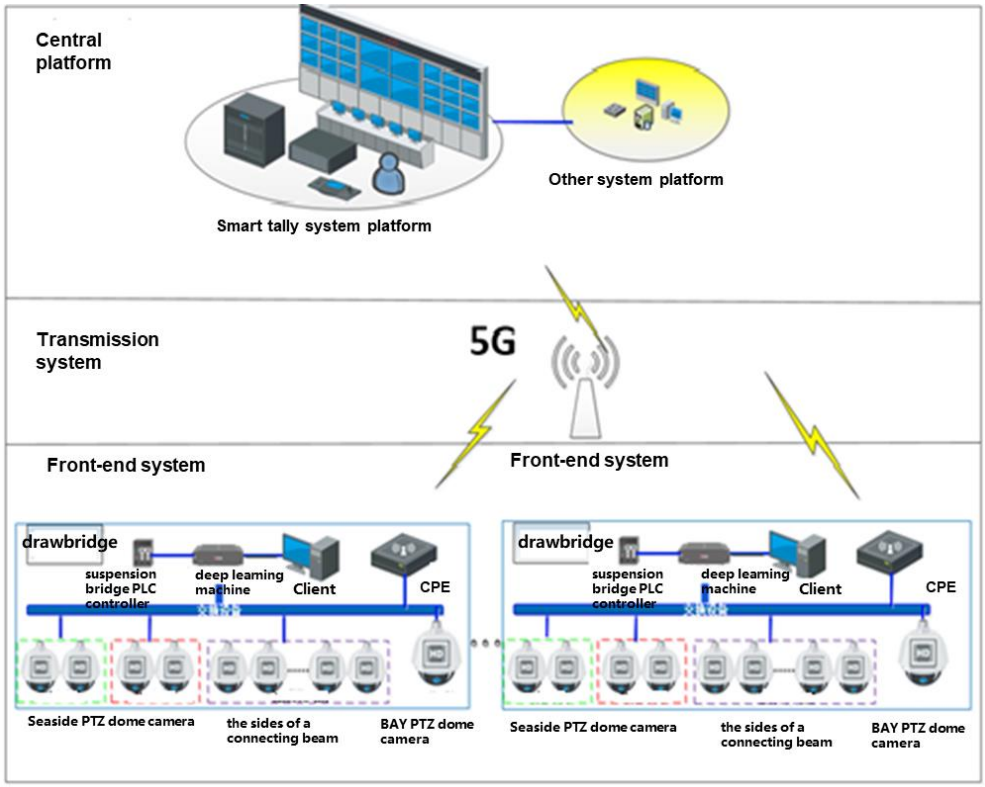

Figure 1. Port remote tally system based on 5G network

Security Challenges and Assurance Requirements for 5G Smart Ports

Smart ports can be a major application of 5G within vertical industries. They are closely related to the Information and Communications Technology (ICT) infrastructure of the port and enable the enterprise distributed intranets to communicate with one another through a carrier's 5G network. In addition, MEC puts the core network elements of the 5G network to reside in the port making it dependent on the requirements of the port's application security. Therefore, the 5G smart port application scenario not only needs to ensure 5G network security and MEC security, but also needs to address new security capabilities for port applications. This poses higher requirements on network security assurance, including the following five aspects:

1. **5G cyber security risks**: New risks are arising from CU (Central Unit)/DU (Distributed Unit) separation, air interface, core network, and interconnection. In addition, the actual security assurance capabilities for SDN (Software-defined Networking), NFV (Network Function Virtualisation), and slicing technologies need to be verified.

2. **MEC security risks**: The MEC facility is deployed at the edge of the network. As a result, the number of edge nodes and security borders increase. In addition, core network elements reside locally and are more open. The unified MEC management is complex and prone to exposure attacks.

3. **Industrial internet application risks**: As a typical edge cloud computing environment, the 5G MEC platform may be subject to data leakage, software tampering, unavailability, and attacks from 5G Core. Industrial internet applications require a more trusted MEC environment.

4. **Standalone (SA) slicing security risks**: SA slicing does not implement security isolation, resulting in competition and abuse of CPU, storage, and I/O resources. In addition, security authentication for slicing access to 5G networks needs to be considered to ensure access

to valid slices and the controllability of applications to slice the networks and resource usage.

5. **Data security risks**: The traditional closed industrial network becomes more open with 5G and MEC. As a result, public network users may be able to access private network users. Carrier networks and enterprise networks can be accessed from each other. Data centers are more vulnerable to attacks and sensitive data leakage.

5G Smart Port Security Solution

5G Network Security Protection

The smart port enterprise network and carrier network are both trusted domains. Protection measures must be deployed at the border of the network to prevent attacks from the other domain.

The N6 interface on the 5G network is located at the border between the MEC and the enterprise network. Security devices, such as firewalls, anti-DDoS (Distributed Denial-of-Service) devices, and IDS (Intrusion Detection System) devices, need to be deployed. The security device on the MEC side is used to defend against attacks from the enterprise network to the carrier network. The security device on the enterprise network is used to defend against attacks from the carrier network to the enterprise network.

In real application, there are several construction modes for the MEC platform. The MEC platform can be constructed and provided by carriers or it is constructed and provided by users, while basic resources are provided by carriers. The APP may be constructed by users and security protection in different modes may vary. The 5G network must consider different levels of protection requirements due to different MEC homing. For example, a firewall is deployed between the 5G core network and radio access network to prevent attacks from the enterprise network to the carrier network by using the user MEC platform as a springboard.

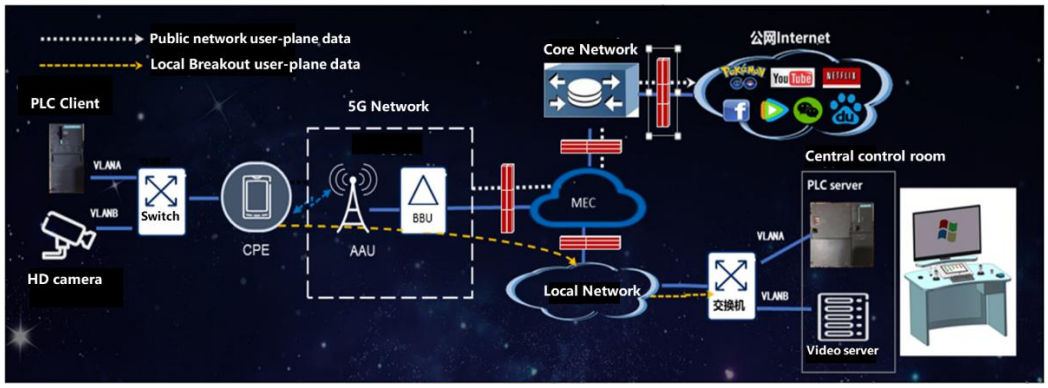

Figure 2. MEC network architecture

MEC Security Risk Elimination

1. **Physical security**: According to the service scenario in Hong Kong, MEC physical security involves the equipment room of the MEC node campus and the site close to the user. In a relatively open environment, MEC devices are more vulnerable to physical damage. To ensure the physical security of the infrastructure, security measures such as access control and environment monitoring need to be implemented. In addition, the structure design for anti-theft and anti-damage of the MEC must be enhanced, and the input/output and debugging interfaces of the device must be controlled.
2. **Platform security**: To prevent software tampering of the MEC platform, it is necessary to enhance platform security, platform management security, data storage, and transmission

security, as well as introduce trusted computing technologies, start the system to upper-layer applications, verify the system level by level, and build a trusted MEC platform. In addition, Virtual Machine (VM) isolation is required to improve virtualization security. For VMs deployed on MEC, micro segmentation is used to strictly isolate VMs and applications. In addition, the VM running status can be monitored in real time to effectively detect malicious VM behaviors and prevent MEC from being infected by malicious VM migration.

3. **Cyber security:** MEC connects to multiple external networks and therefore needs to implement isolation protection based on traditional defense technologies such as border defense, internal and external authentication, isolation, and encryption. From the perspective of the MEC platform, the MEC is divided into different functional domains, such as the management domain, core network domain, basic service domain (capability openness), and third-party application domain. The MEC is divided into different security domains to implement isolation and access control. In addition, the built-in intrusion detection function detects malicious software and malicious attacks to prevent horizontal expansion of threats.

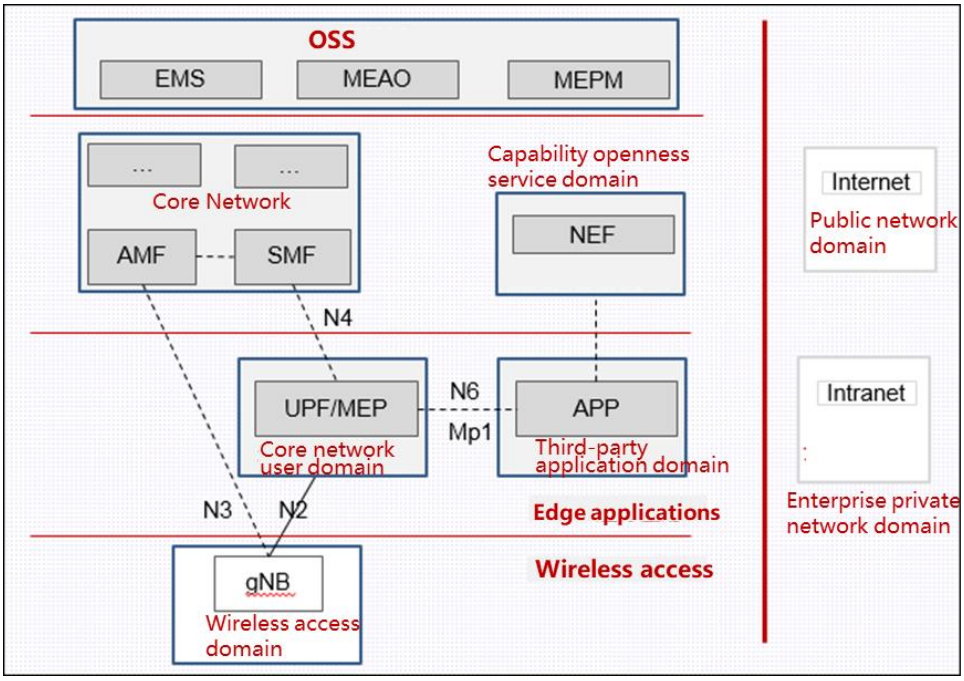

Figure 3. MEC internal network security domain isolation

4. **MEC interface security**: The MEC is connected to the N4 interface on the control plane of the core network. The N9/N6 interface on the user plane can provide the IPSec security transmission channel. An Access Control List (ACL) can be provided for packet filtering to detect malformed packets.

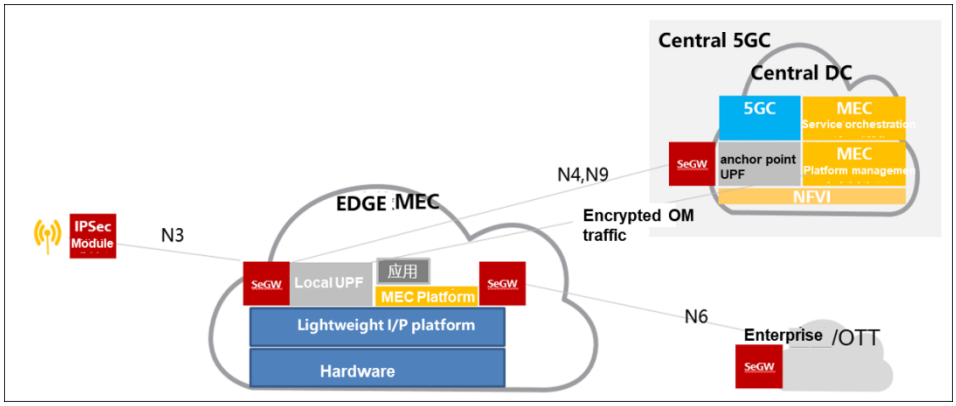

Figure 4. MEC interface security protection

5. **O&M security**: First, authentication and authorization management is required. To ensure the security of assets and data on the MEC node, the user needs to perform authentication, authorization, and audit on the behaviors of the parties that use the MEC. Secondly, the ownership, right to use, and O&M rights of data assets are managed by rights- and domain-based management at the platform, network, and service levels. When key communications such as management and charging are carried out between the MEC and the core domain, the Public Key Infrastructure (PKI) and Transport Layer Security (TLS)/IPSec protocols are fully used to implement authentication authorization and transmission encryption. Virtual Network Function (VNF) version verification is also necessary. To ensure the security of the running version and prevent viruses, the MEC needs to support both the release party and receiver signature of the VNF version package in the different delivery phases. In addition, the MEC needs to verify the signature of the released version package. Thirdly, a security assessment is required. To prevent security vulnerabilities from affecting other functional domains on the MEC node, a strict control process must be performed before other applications on the campus network are introduced, in order to perform comprehensive security evaluation and detection. At the same time, the application registration process is used to control the application rights, and the audit method is used to standardize the execution of the application.

Slice security assurance

Sectional access security

First, authentication of the user access slice should be provided. When a terminal accesses the network, the 5G network access authentication is used to ensure the validity of the user, that the access legal slice is valid, and that the campus application can control the slice network and resource usage. Secondly, protection should be provided for slicing selection auxiliary information. The slice selection auxiliary information Network Slice Selection Assistance Information (NSSAI) can distinguish slices of different types. When the campus terminal initially accesses the network, the NSSAI instructs the base station and the core network element to route the network element to the correct network slice element. Slice selection auxiliary information is sensitive information for smart ports, therefore 5G networks need to protect NSSAI privacy.

Slice isolation

Network slicing is a logically independent private network. However, network slices share physical resources and IT infrastructure, and each slice is a tenant on them. The slice manager Network Slice Management Function (NSMF) allocates a corresponding server resource to each slice according to the slice Quality of Service (QoS) and security policy. NSMF uses multiple means, such as resource allocation policy and virtualization isolation, to ensure that no competition and abuse of Central Processing Unit (CPU) , storage, and I/O resources occur among different tenants. A three-level, three-dimensional security isolation system is required for slicing, as shown in the following figure.

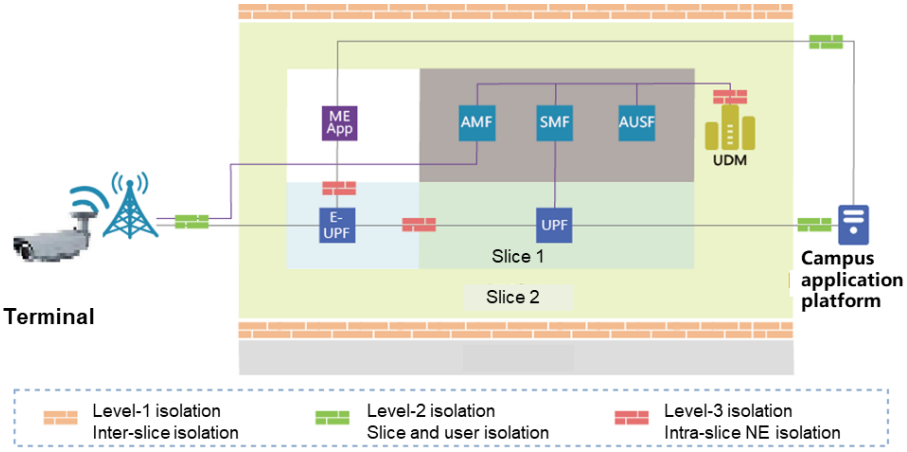

Figure 5. Three-level three-dimensional isolation system for network slicing

The slicing isolation system includes:

1. **Slicing isolation:** Slicing isolation is effectively carried out based on the service application scenario and the importance of data assets, so as to ensure that each slice has the corresponding security level.

2. **Slicing network and user isolation:** To ensure secure and reliable 5G network slices, an isolation mechanism is configured on both the end-user and campus application sides during network slicing design to provide high-reliability slicing services for different applications based on Service Level Agreement (SLA). This ensures clear security boundaries of the slicing as well as the security and controllability of the slice itself.

3. **Isolation between network elements in a slice:** Security zones are divided on the slicing network to provide security isolation between network elements.

In the three-hierarchical security isolation system, the isolation solution at each level can be implemented at three layers: network element, network, and data. When the mature virtualization isolation solution is used, the NFV and SDN technologies are used to collaborate with the VM orchestration and slicing orchestration functions, leading to precise and flexible slicing isolation.

Security issues when the app is co-deployed with the MEC

To accommodate more low-latency and high-bandwidth services in ports, smart ports deploy industry apps on the MEC platform. The co-deployment of industry apps and carriers' MEC brings more security challenges such as the issue of trust between an operator’s app and industry apps on the same MEC platform. If an untrusted app is running on the MEC platform, it will bring security threats to MEC and even 5GC through MEC. Industry apps are also concerned that MEC platform vulnerabilities will cause intrusion into industry apps and even into enterprise private networks through the industry apps. Therefore, the security of the carrier's MEC platform and the isolation between carriers and industry apps must be ensured to prevent attacks from spreading.

1. **APP security:** The MEC verifies the digital signature of the integrated industry app to prevent the app from being illegal or tampered with. The MEC platform provides various security services, such as data encryption services, for apps.

2. **Capability openness security:** Access authentication and authentication are provided for access to API interfaces provided by industry apps to prevent DDoS attacks.

3. **Security situational awareness:** Deploy the security management system to quickly analyze user behaviors, logs, and traffic. It also performs policy orchestration and response processing for detection events. Situational awareness visualization also improves security O&M efficiency.

Data transmission security

The base station is connected to public users and smart ports at the same time. Smart ports use industry terminals and access enterprise private networks through 5G networks. It is necessary to ensure transmission security and transmission isolation of 5G networks as private networks, preventing personal data and enterprise data from being disclosed.

1. **Transmission isolation:** The smart port Data Network Name (DNN) and other common public network DNNs are divided into different Virtual Local Area Network (VLAN) / Virtual Private Networks (VPNs) so that they cannot communicate with each other. That is, terminals authorized by the non-smart port DNN cannot access the enterprise private network or access the industry terminals authorized by the smart port DNN.

2. **Transmission security**: 5G provides air interface data confidentiality and integrity protection capabilities to ensure air interface security from industry terminals to base stations. From the industry terminal to the 5G control plane core network, NAS signaling confidentiality and integrity protection is implemented. The N3 interface between the base station and the MEC provides the IPSec security transmission channel to ensure confidentiality and integrity of data transmission. The VPN tunnel from the MEC to the enterprise network is established through the IPSec tunnel between the MEC and the enterprise network. The data transmission security of the entire campus network is ensured.

3. **E2E (End-to-end) data security**: Enterprise networks can also establish VPN transmission tunnels from terminals to enterprise private networks to ensure industry data security at the application layer.

Smart Port Security Practices Based on 5G SA Slices

Ningbo Port is a large port with an annual cargo throughput of over 1 billion tons. It has more than 550 gantry cranes and is responsible for the shipment of 70% of goods to Hong Kong. As the working environment of the gantry crane is poor, remote automatic reconstruction to improve the working environment of the driver and work efficiency is a trend in the industry. China Mobile has completed the informatization reconstruction of the No.58 gantry crane at the International Container Terminal No. 4 in Meishan Island, Ningbo Port, and successfully implemented remote operation control based on 5G, marking the first formal implementation of the first smart port project based on 5G SA slicing and MEC.

In August 2019, China Mobile, Ningbo Port, and Huawei completed the world's first MEC security pilot that complies with the latest 5G SA specifications of 3rd Generation Partnership Project (3GPP). It is also the first MEC security test in the industry in a real industrial internet environment such as Ningbo Port. The pilot proves that the 5G SA slicing technology and MEC technology can be used to implement remote control of heavy equipment such as gantry cranes, access of public network users to port private networks, access of public network users to port terminals, and internet access to port enterprise networks. The SLA also addressed network reliability, delay jitter, and security isolation, with E2E latency of 10.5ms, jitter less than 2ms, and upstream average bandwidth up to 175Mbps. This enabled the 18ms latency requirement of the Programmable Logic Controller (PLC) control signaling of the gantry crane, smooth transmission of 18 HD videos, and meeting the stringent requirements of network security and data security. This is a profound milestone in the exploration of 5G+ industrial internet security applications.

Additional technical achievements

1. Released the 5G Security White Paper, 5G Network Capability Openness Security Consideration, Vertical Industry 5G Network Slicing Security White Paper, and 5G Security White Paper for the Medical Industry in MWC (Mobile World Congress), NGMN (Next Generation Mobile Network), and GTI (Global TD-LTE Initiative).

2. The Guidelines for 5G Security Risk Prevention and Control of China Mobile and China Mobile 5G Network and Service Security Benchmarking Standards have been developed to guide the entire group to ensure the security of 5G networks and services.

3. Three 5G security-related projects have been initiated in 3GPP, and one of them has been completed.

4. Initiate the research on the Cyber Security Risk and Standard System of the Fifth Generation Mobile Communications (5G) in TC260, and initiate the 5G Data Security Technical Requirements in CCSA (China Communications Standards Association) to promote the standardization of 5 data security in China.

Ecological construction

1. China attaches great importance to the development of the 5G industry and the participation of industrial Internet industry partners, such as shipping ports, to jointly promote the integrated application and innovative development of the 5G+ industrial Internet. Partners include basic telecom enterprises (China Mobile), port industries (Zhejiang Port of Ningbo-Zhoushan, Shanghai Yangshan Port), security platform providers (Huawei), and government regulators (Zhejiang Communications Regulatory Authority of the Ministry of Industry and Information Technology), which is important for promoting the maturity of the 5G industry chain.

2. Standards organizations and industry alliances, e.g., the GSMA (GSM Association), 3GPP, ISO (International Organization for Standardization), ITU (International Telecommunications), 5G-ACIA (5G Alliance for Connected Industries and Automation), and IMT2020 (International Mobile Telecommunications), need to actively promote and guide the industry to reach an important consensus to ensure that 5G SA and MEC security is the fundamental prerequisite for operation of 5G smart ports. This will play an important role in promoting global competitiveness.

Summary

The smart port security practice based on 5G SA and MEC is an innovative and secure application of the 5G+ industrial internet environment. The 5G SA slicing technology and MEC technology improves the informatization level of the port, enhances operation and maintenance efficiency, reduces reconstruction costs, as well as reducing human-machine contact. This helps port enterprises to significantly reduce the TCO (Total Cost of Ownership), especially labor network construction costs of original port operations, and enables satisfactory ROI (Return on Investment) for carriers. At the same time, its successful deployment provides an application environment for the research and practice of 5G+ industrial internet applications and opens up new business models. It is a useful reference and practical guide for security risk assessment and assurance of the 5G+ industrial Internet environment. This case study indicates that global operators should cooperate with all parties in the industry chain in 5G security ecosystem cooperation.

GSMA HEAD OFFICE
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom
www.gsma.com