ITU KALEIDOSCOPE
ONLINE 2021

6-10 December 2021

Collaborative 5G multiaccess computing security: Threats, protection requirements and scenario

Hongyang Zhang
China Mobile, China

Session 4: Policies and ontology for security management

Paper S4.1: Collaborative 5G multiaccess computing security: Threats, protection requirements and scenarios

Authors: Gang Zhao, Feng Zhang, Le Yu, Hongyang Zhang, Qin Qiu, Sijia Xu (China Mobile)

Abstract

Definition

- 5G MEC is a new model for 5G network architecture that moves cloud computing capabilities and IT service environments to the edge of mobile communications networks, providing nearby services for users.

Function

- 5G MEC establishes a carrier-class service environment with high performance, low latency, and high bandwidth. 5G MEC enables new applications by moving core network functions to the network edge.

Challenge & Protection

- 5G MEC brings new security challenges and increases security supervision difficulty. This paper proposes 5G MEC security protection policies for operators and 5G industry customers by drawing on successful industry practices.

Goal

- Help industry customers implement the three sync security requirements (synchronous planning, synchronous construction, and synchronous maintenance) while developing 5G MEC applications, as well as guiding the industry to improve MEC security capabilities.

5G MEC Introduction

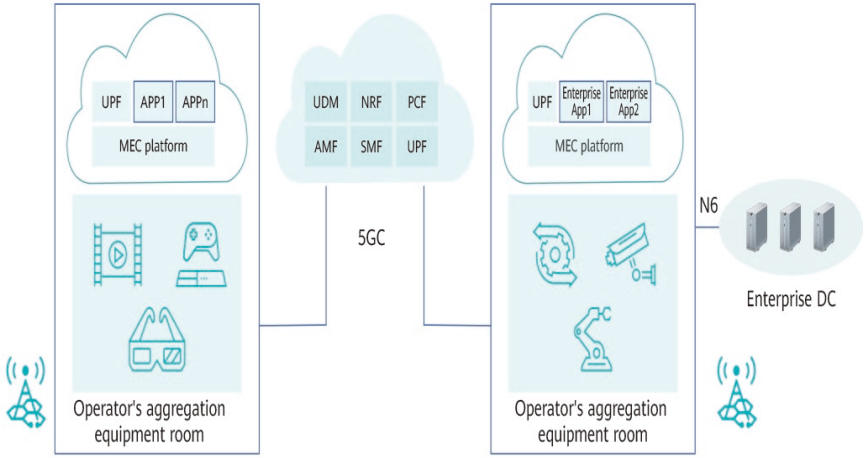
Deployment Scenario

- MEC is mainly deployed in aggregation equipment rooms and on campuses due to the latency, cost, and enterprise data security requirements of different services.

- There are two typical MEC deployment scenarios: wide area network (WAN) MEC and local area network (LAN) MEC.

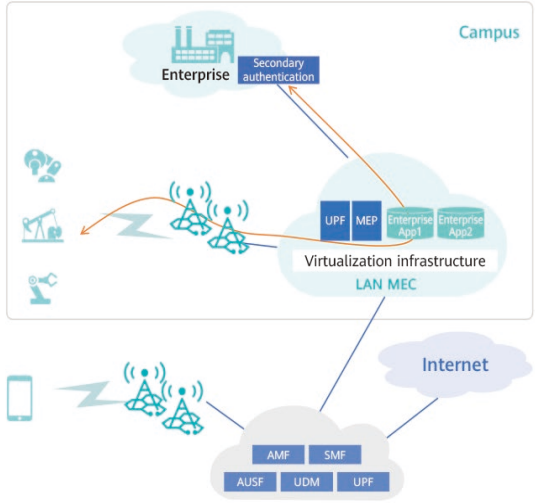
WAN MEC

- To ensure low latency services through two-way latency below 1 millisecond over 100 km of transmission.



LAN MEC

- Is for industries that are highly sensitive to security and privacy protection.



5G MEC Security Threats

1.Threats to Network Service Security

- Threats of UPF deployment model
- Threats of posed by mobile edge architecture
- Threats of illegal access
- Traditional cyber attack threats

2.Threats to Hardware Environment Security

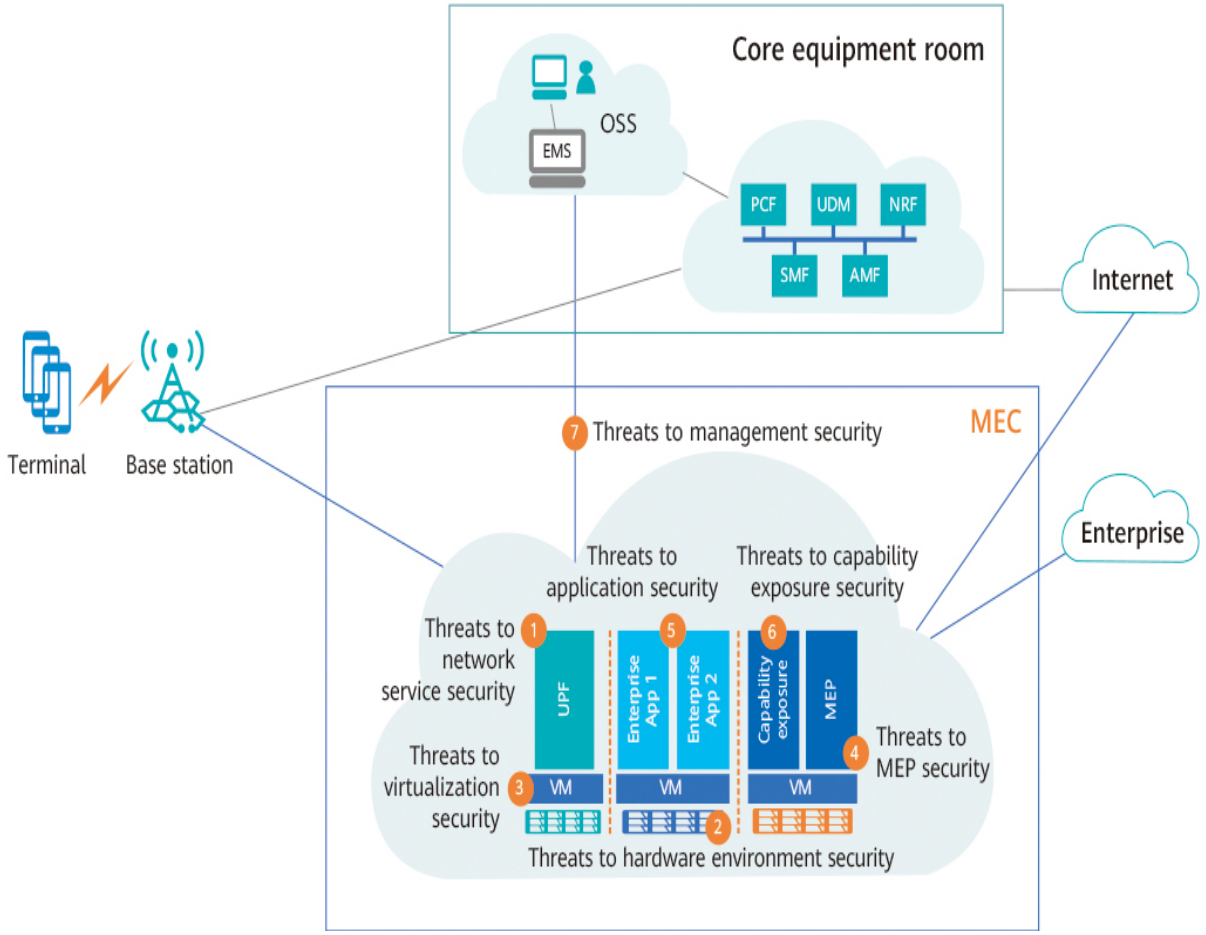
- Weak security measures threats
- Threats of illegal access

3.Threats to Virtualization Security

- Threats of tampering with container or virtual machine image
- Rights Escalation threats
- Resource abuse threats

4.Threats to MEP Security

- Threats of illegal access
- Traditional cyber attack threats



5G MEC security threats

5.Threats to Application Security

- Information security control threats
- Threats of communication protocol vulnerabilities

6.Threats to Capability Exposure Security

- Privacy disclosure threats
- Rights Escalation threats
- Service manipulation threats

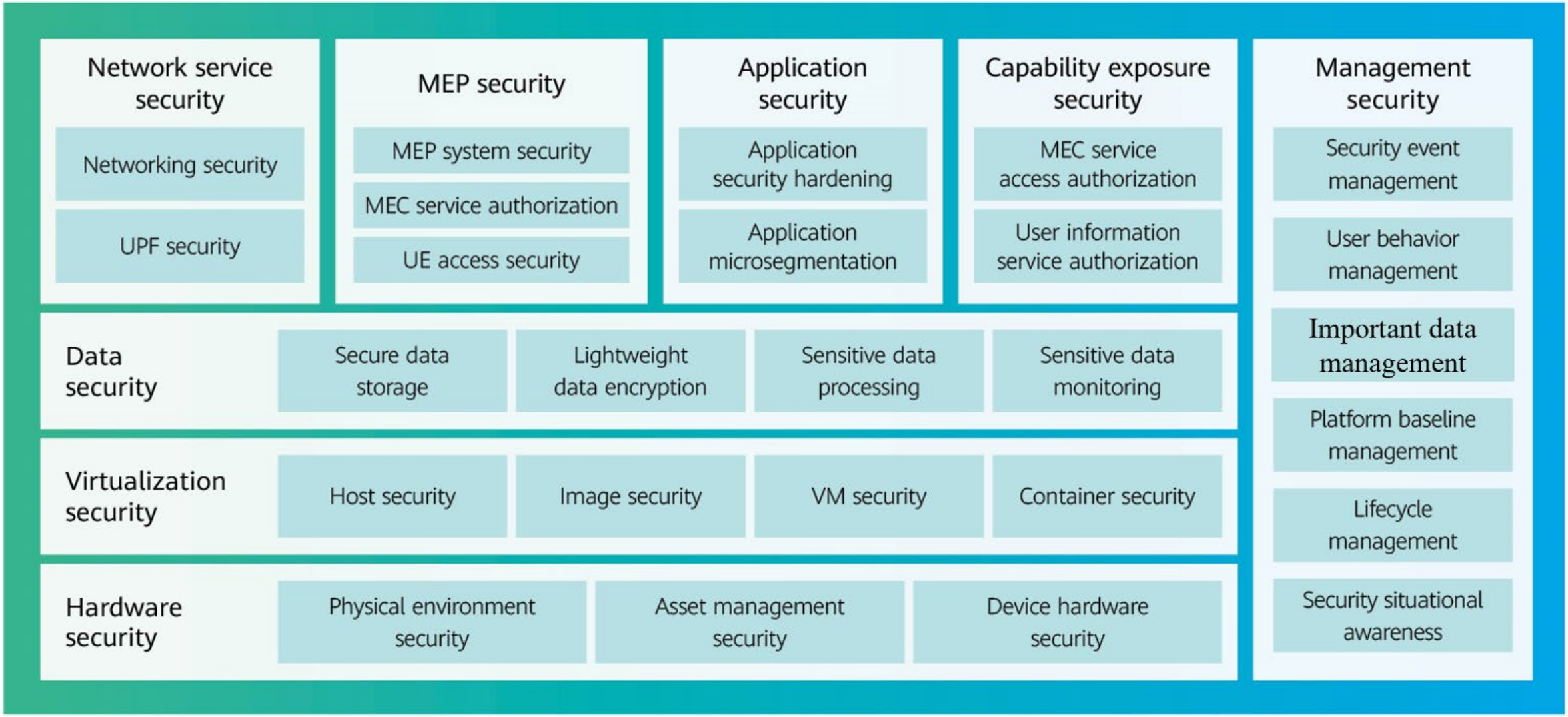
7.Threats to Management Security

- Threats of illegal access
- Threats of untimely operation and maintenance
- Weak password threats

8.Threats to Data Security

- Threats of not backing up important data
- Threats of malicious access to user's sensitive privacy data

5G MEC Security Protection

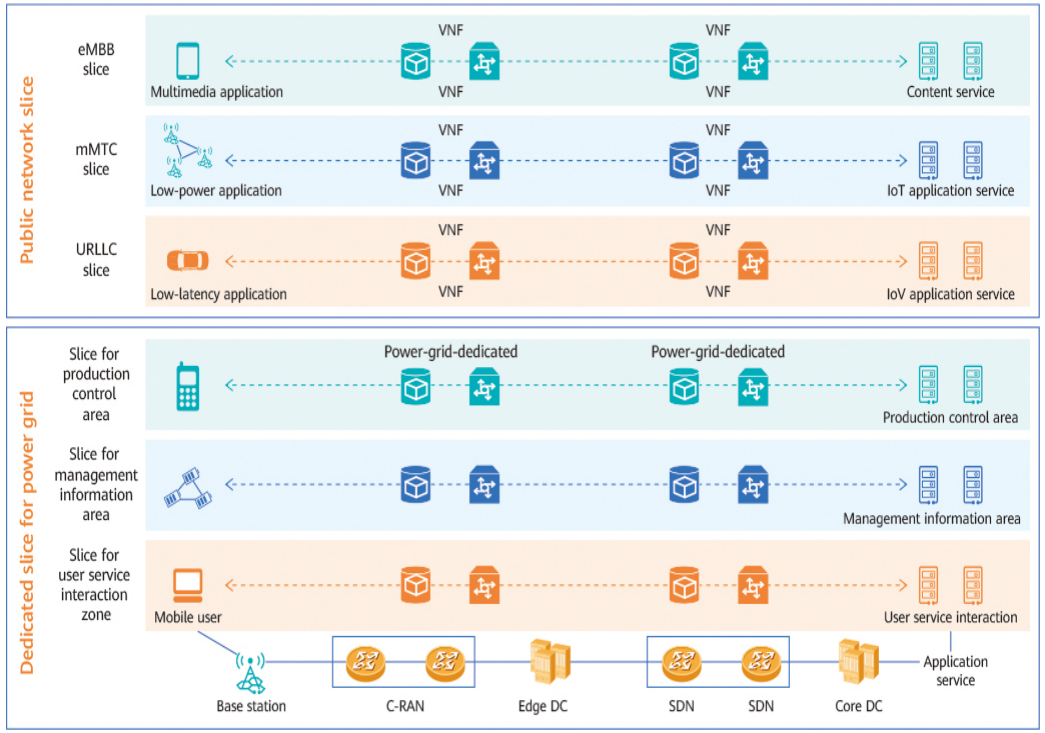


5G MEC security protection architecture

Case 1: WAN MEC Scenario---Smart Grid

Deployment Requirement

- Need to match the traffic direction of power services
- Satisfying service latency and isolation requirements
- Based on the characteristics of power grid services



Overall framework of the 5G slices for power grid

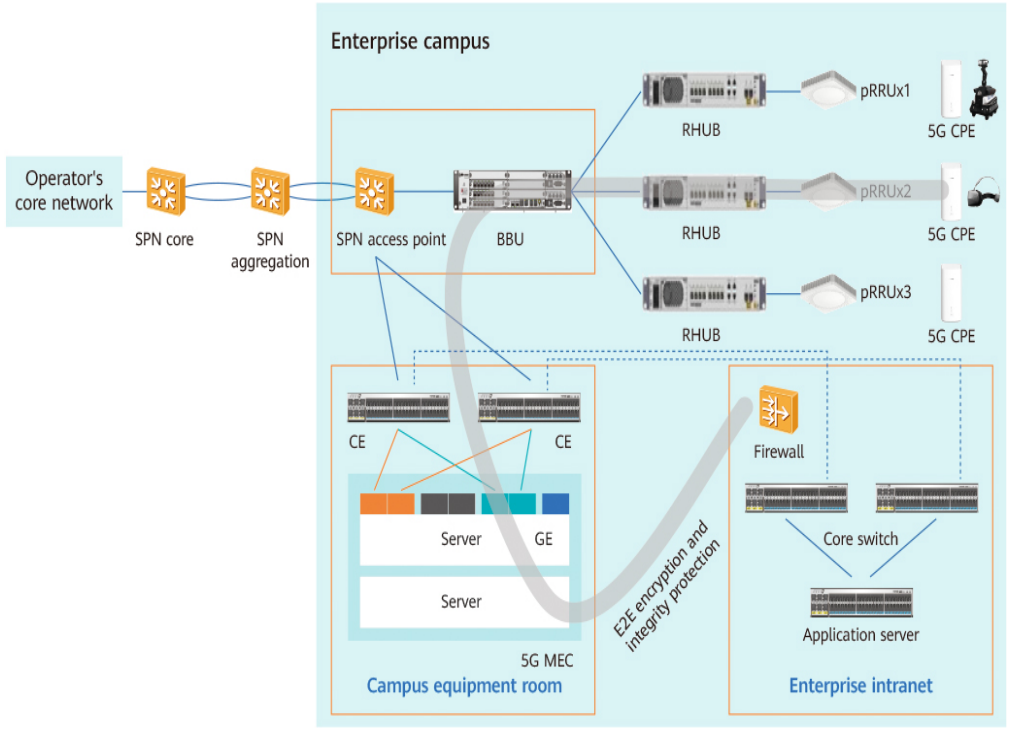
Security Protection

- **Security Zoning**
  - Production control area: high security isolation
  - Management information area: local data processing
- **Dedicated Network**
  - Physical isolation: between production control area service and other services
  - Logical isolation: among different services in an area
- **Horizontal Isolation**
  - Isolation production control area and management information area: a horizontal unidirectional security isolation device which is certified by national department , must be deployed.
- **Vertical Authentication**
  - Special protection: bidirectional identity authentication, data encryption and access control.

Case 2: LAN MEC Scenario---Smart Factory

Deployment Requirement

- The smart factory network architecture consists of 5G UEs, 5G base stations, 5G transport network, and 5G core network.
- Deploy MEC LBO mode to implement low-latency and high-bandwidth access to local network resources and ensure that data is not transmitted out of the factory.



End-to-end encryption and integrity protection

Security Protection

- **UE Access Security**
  - Identity authentication of SIM card : 5G AKA mutual authentication Independent authenticate and manage enterprise UEs: deploy AAA services
- **Confidentiality and Integrity Protection**
  - Confidentiality: 128-bit encryption algorithms, creating a dedicated tunnel
  - Integrity: use integrity algorithms
- **Enterprise Network Border Isolation**
  - Deploy firewall : between the UPF and the core switch on the enterprise network. The firewall provides refined access control policies to reduce the attack surface, traffic and behavior analysis capabilities.
- **Security Management and Audit**
  - Log audit system: deploy at security management center collects system security events, user access records, system run logs, system operating status, and other information.

Outlook

- In future, as MEC continues to gain popularity, we shall ensure a secure 5G MEC environment.
- On the one hand, we need to collect and analyze these threats of 5G MEC and take the security protections to deal with them.
- On the other hand, we will make greater contributions to 5G MEC applications in each area such as smart city, smart transportation and so on.

ITU KALEIDOSCOPE
ONLINE 2021

Thank you!