

IoT Security

Prepared by Dr. Abdelrhman Ahmed

Lecture 2



جامعة الجميع الذكية
EVERYONE'S SMART UNIVERSITY

IoT Security Technologies

- In today's human-centered network era, security has become the biggest concern for network development. It also will be a more trending topic in the coming Internet of Things (IoT) era where everything can be connected.
- IoT security involves four layers: application, platform, network, and device. A comprehensive security protection mechanism must be designed to ensure collaborative protection at each layer.

- Upon completion of this course, you will have an understanding of:
 - ☐ Problems faced by IoT
 - ☐ Huawei IoT security technologies
 - ☐ Typical Huawei IoT security cases

Chapter 02

Tesla Incident

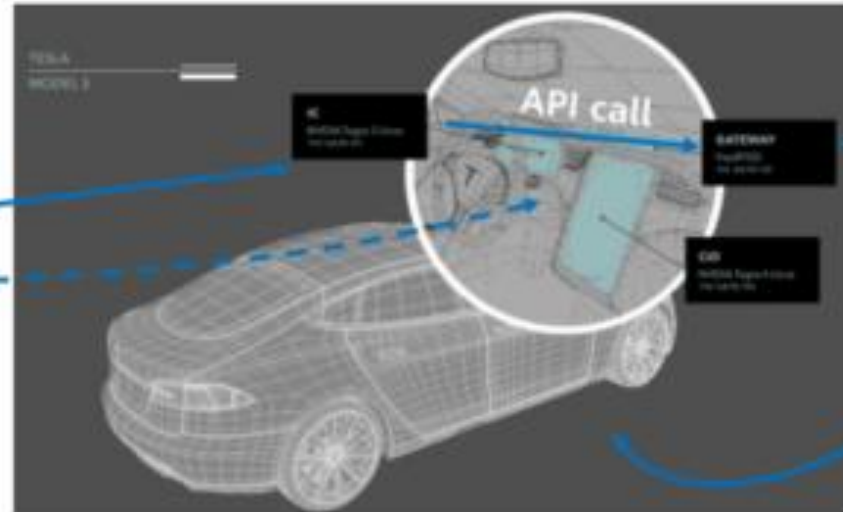
- The in-vehicle system is intruded, causing a vehicle to be remotely started or stopped.

- ② Forge a connection to communicate with the background and obtain the password for the in-vehicle system.



- ③ Log in to the system and deliver commands to the CAN bus through the gateway.

- ① Analyze the hardware and find the removable storage card that contains the background remote communication certificate and password stored in plaintext.



Attacks can cut off power during the driving process.

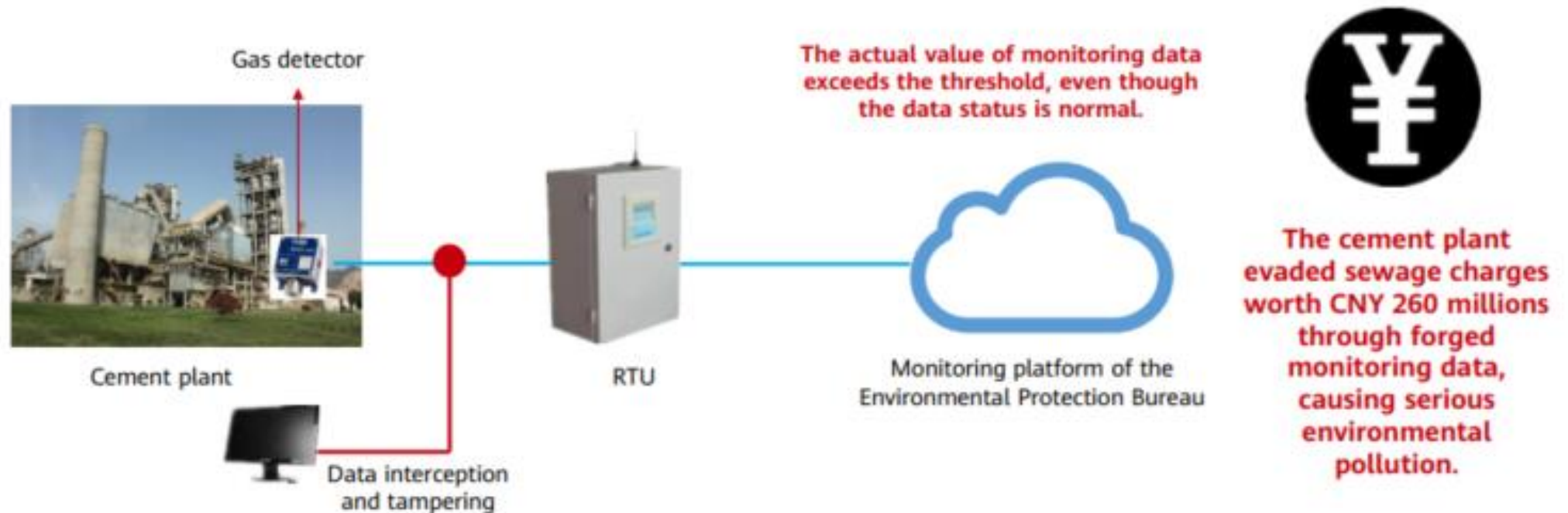
- ④ Deliver commands to the CAN bus to control the vehicle's behavior, including vehicle startup and shutdown, as well as door opening and closing.

No protection measures are taken for local key information causes this incident.

Chapter 02

Nanjing Environmental Protection Bureau Incident

- The local network was intruded, and environmental monitoring data was tampered with.



- Encryption and integrity protection are not carried out during data transmission, which allows the violation to be possible.

- The large-scale DDoS (Distributed Denial of Service) attack was launched by botnets composed of IoT devices that were infected with Mirai malware.
- "Zombies" refer to network cameras, digital video recorders and intelligent routers.
- Mirai botnets infected millions of devices, and only one tenth of them were involved in this DDoS attack.



From 11:00 to 17:00 (UTC time) on October 21, 2016, Internet services were unavailable in several cities in the U.S., and **nearly half of the network was disconnected.**

Chapter 02

Summary of Threats in Key IoT Security Fields

- The threats cover device, communications, cloud/platform and lifecycle management.

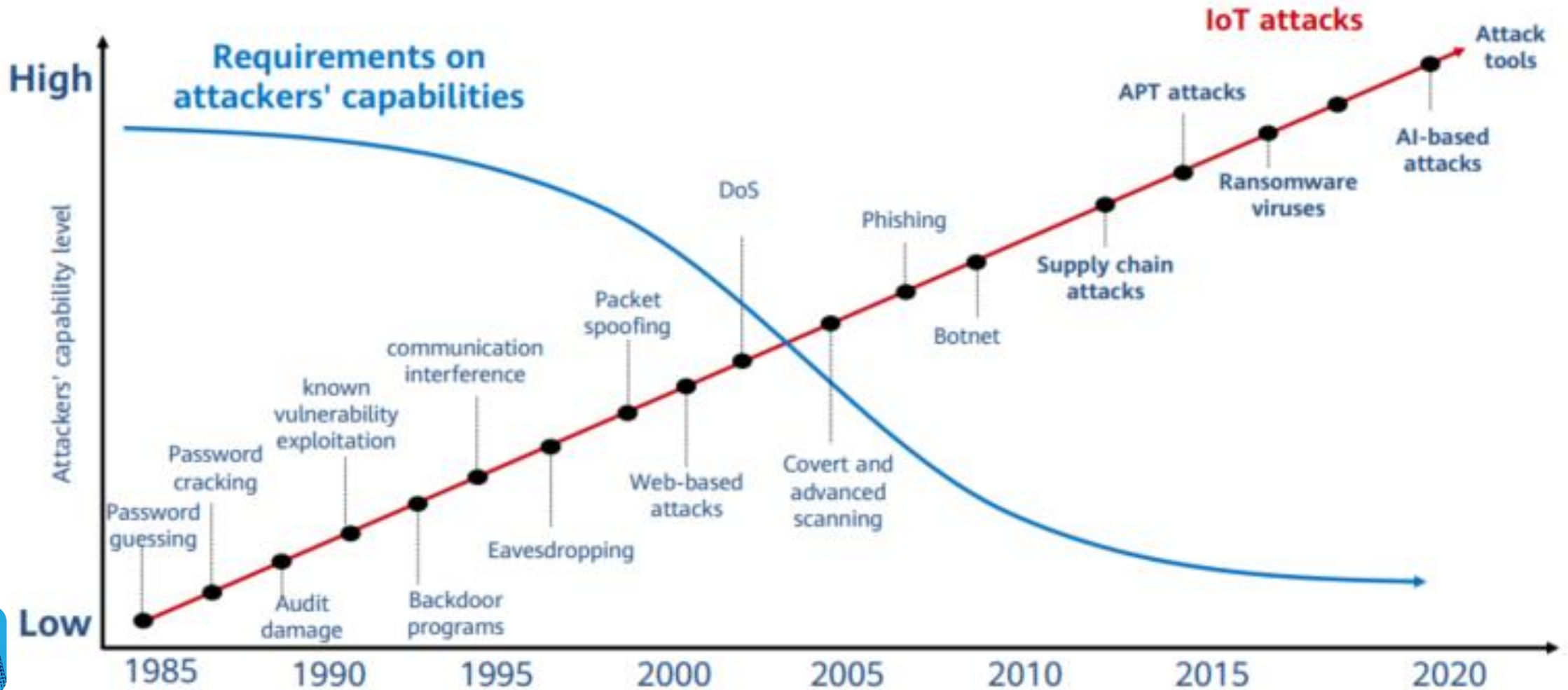


Category	LPWA Security Threat	IoV Security Threat
Application	- Sensitive information leakage - Invalid security access control - Incorrect security configurations	- Bluetooth vulnerabilities - Malicious in-vehicle infotainment (IVI) apps - API attacks
Cloud/Platform	- Unauthorized access - Tenant intrusion - Data leakage and hijacking	- Trajectory privacy leakage - Data tampering and audit - No awareness of abnormal vehicle behavior
Pipe	- DDoS attacks/signaling storms - Gateway vulnerability or improper configurations - Improper identity authentication measures - Unencrypted transmission	- Identity spoofing - Protocol attacks - PKI/CA certificate spoofing
Device	- Device identity simulation - Trust key attacks - Software and firmware interference - Remote security management - Checking of damaged devices - Brute-force device breakdown	- CAN bus authentication and encryption - T-Box communication security threats - OBU/RSU vulnerability threats - Vehicle-mounted certificate security

- IoT security threats are in the negative triangle model, and most of them are from devices. Pipe detection, cloud-cloud synergy, and trusted device authentication are effective means to resolve threats.

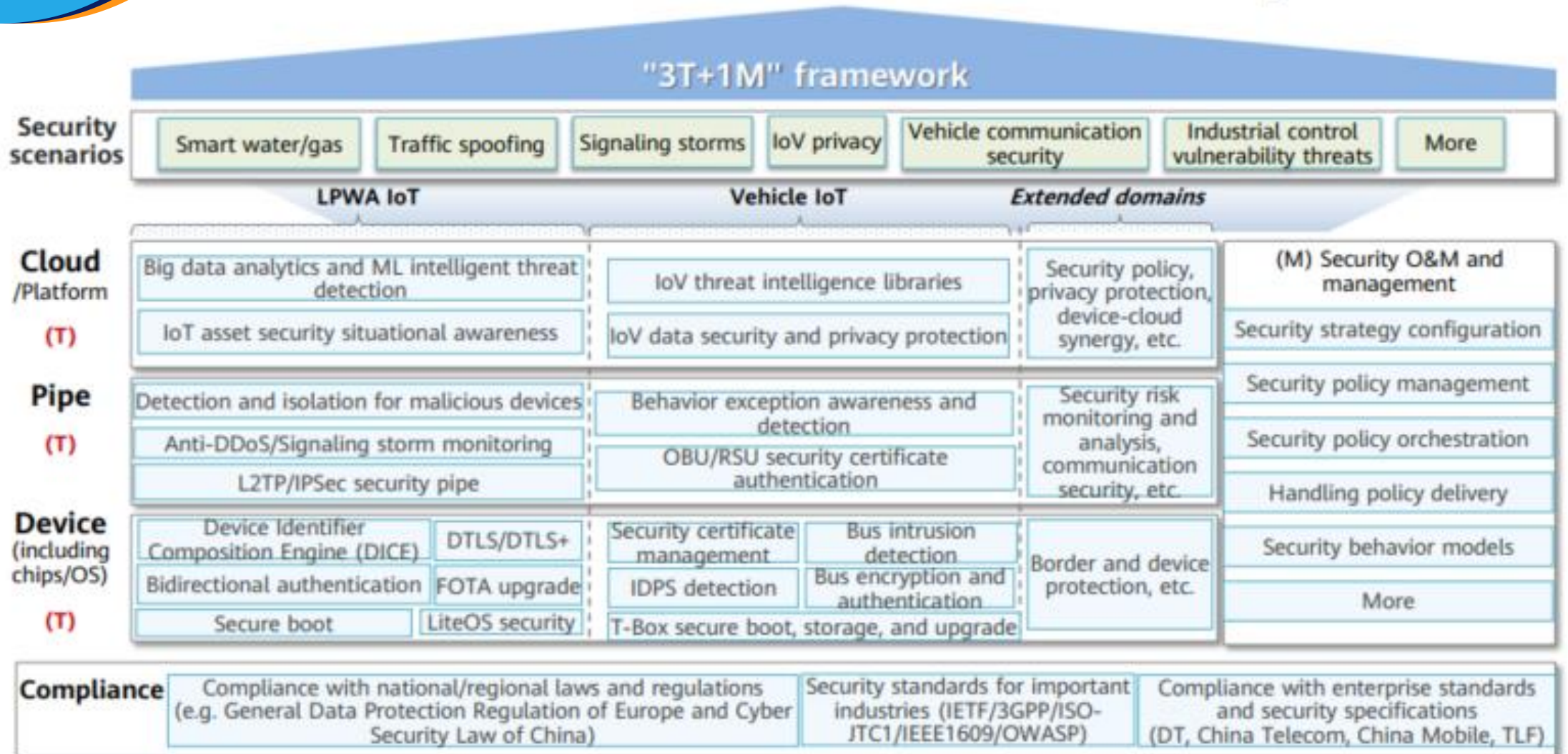
Chapter 02

Trend of Network Attack Technologies



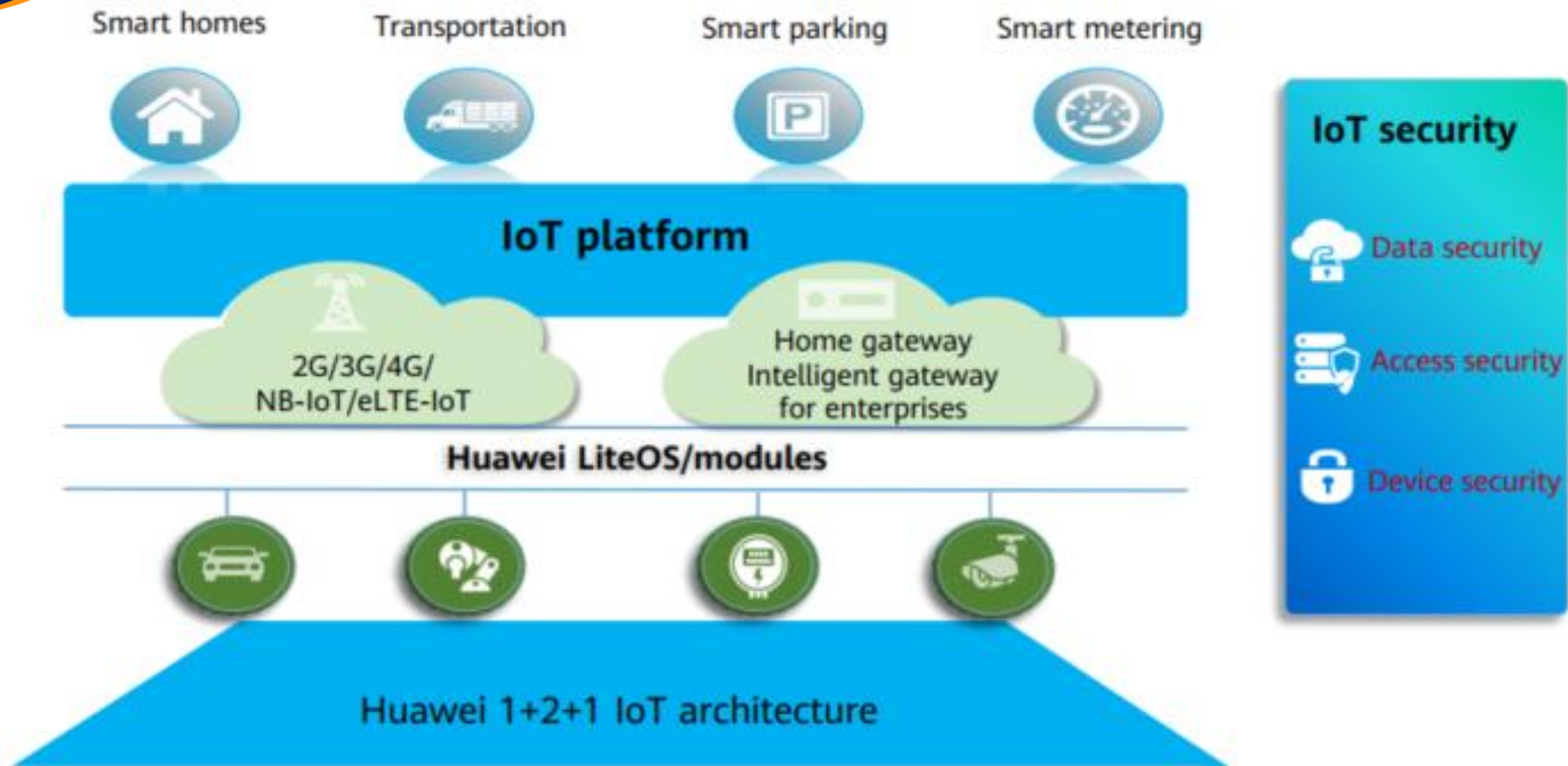
Chapter 02

"3T+1M" Framework of the Huawei IoT Security Solution



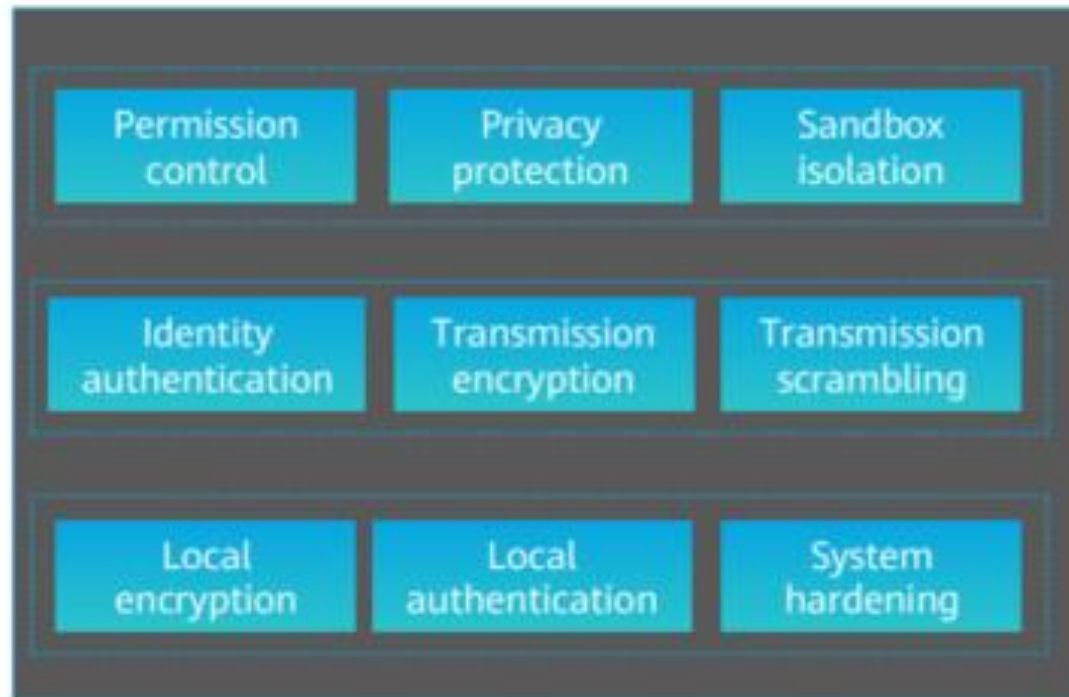
Chapter 02

Huawei IoT Security System - Cloud-Pipe-Device

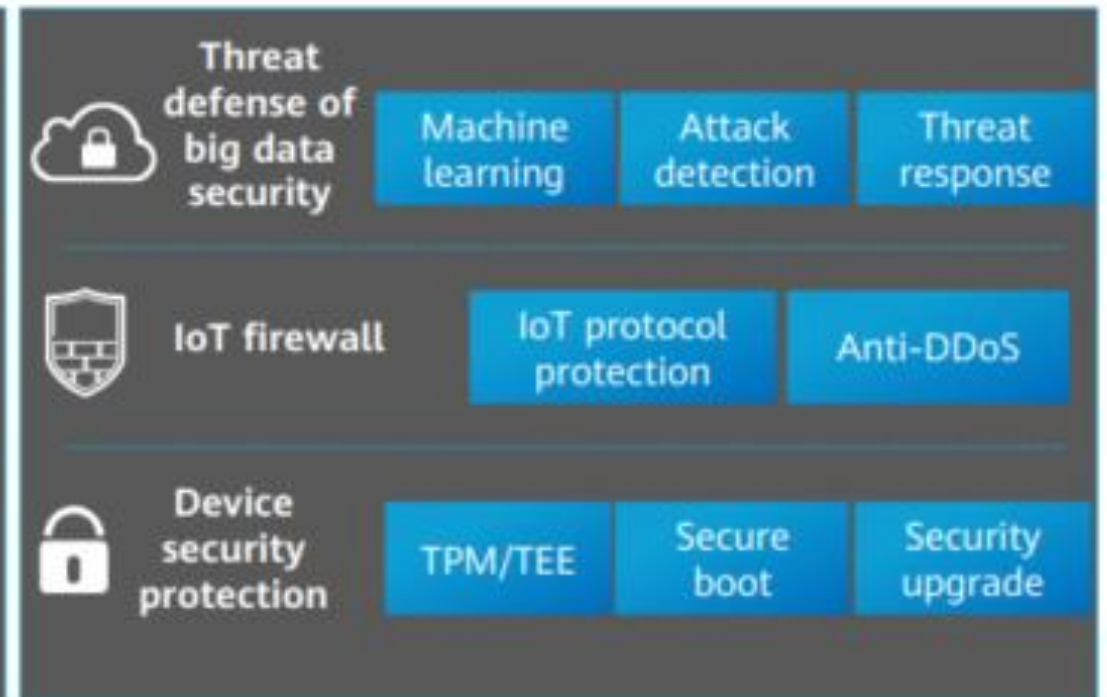


- Leveraging extensive experience in security technologies, Huawei launched a comprehensive IoT security solution.

IoT Product Security



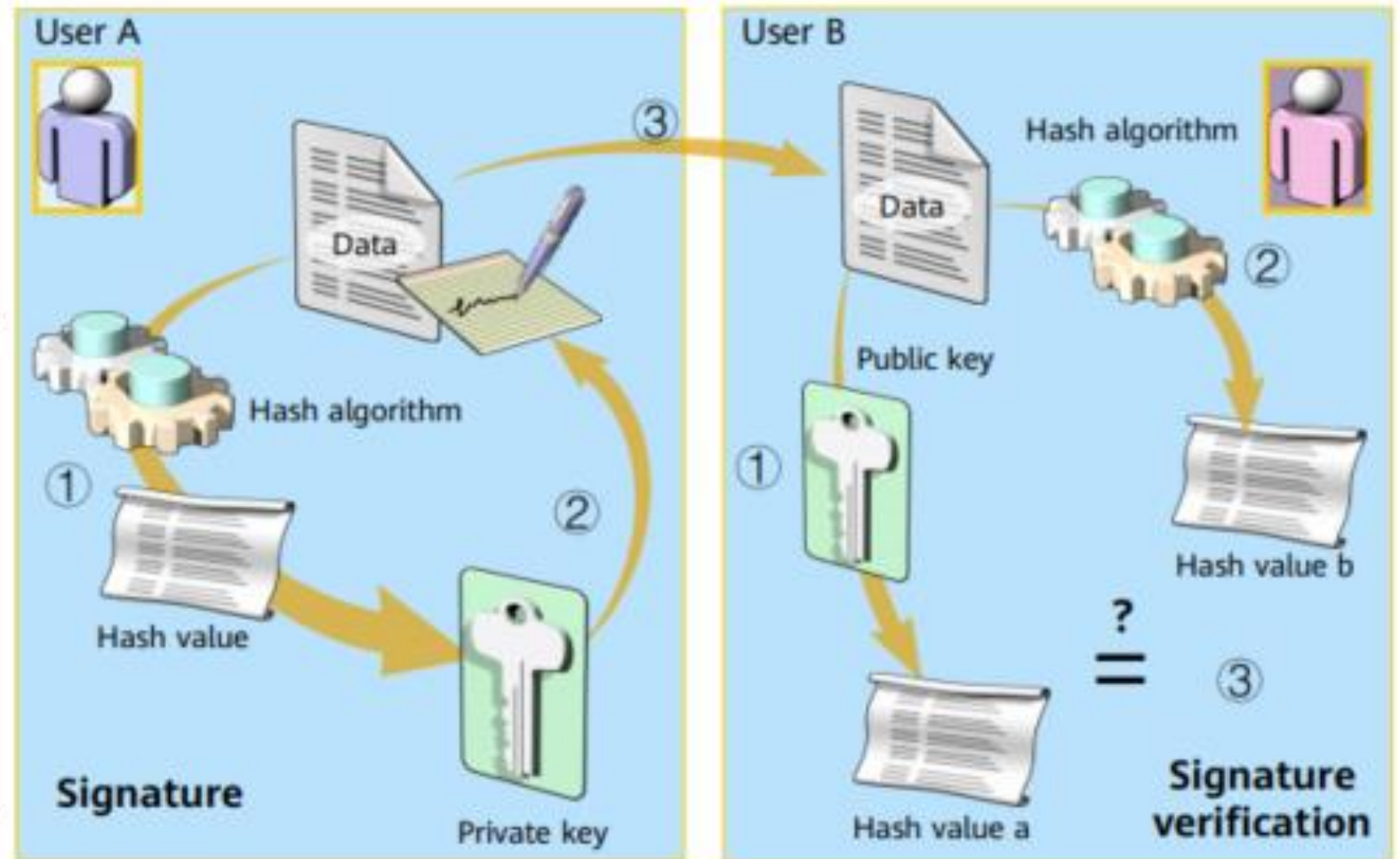
IoT Security Products



Chapter 02

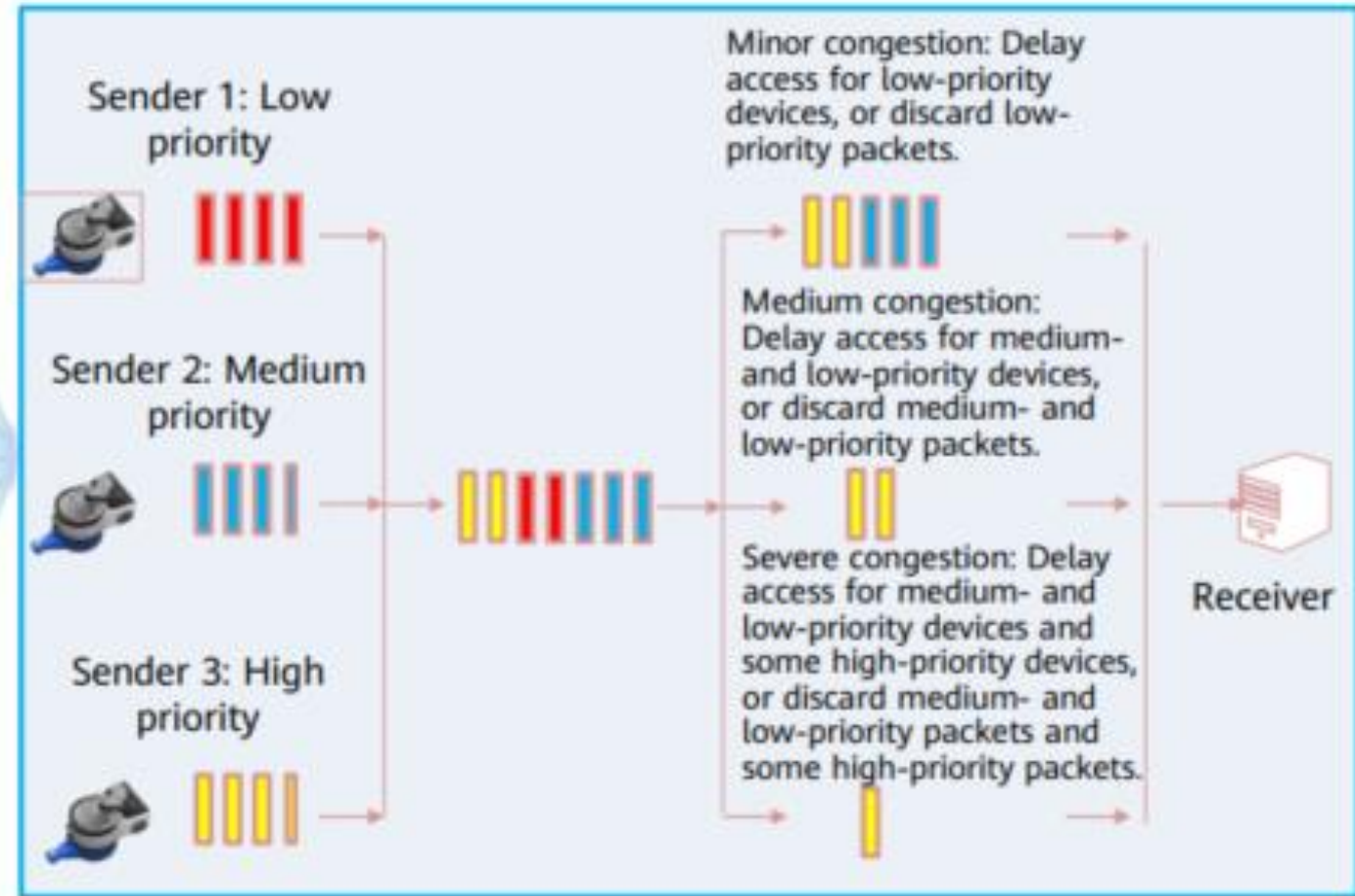
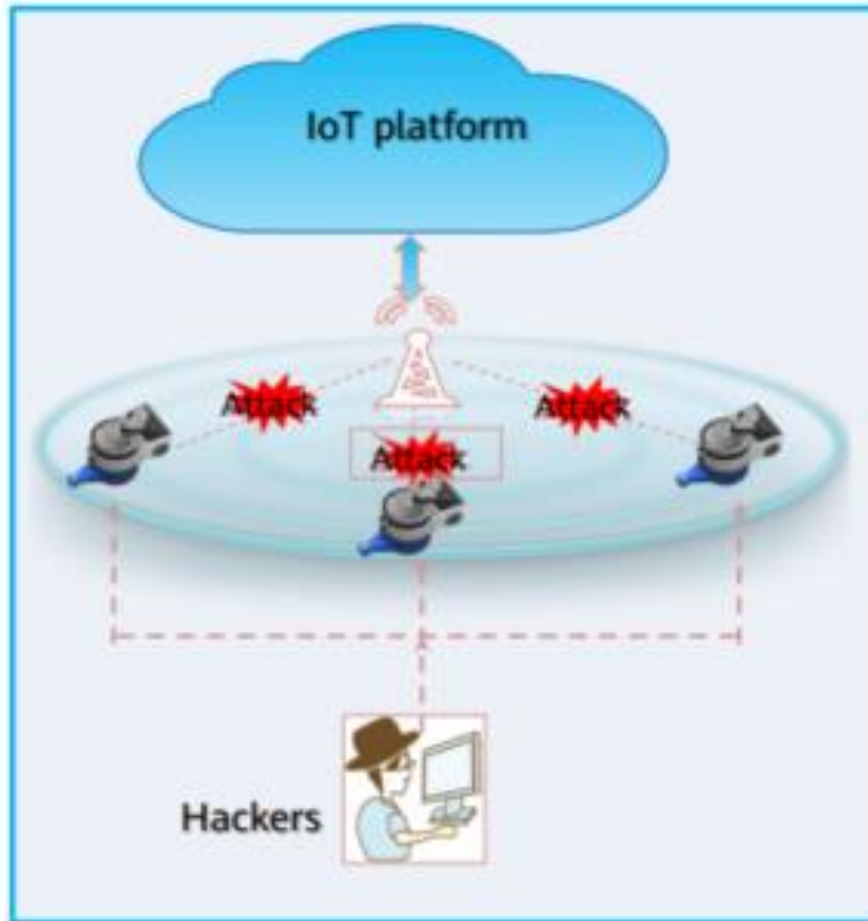
Device Security: Firmware Validity and Integrity Achieved by the FOTA Digital Signature

- Benefits: Integrity check is performed on the upgrade package (downloaded in the flash memory of the device) to ensure that the current firmware is valid and complete (not tampered with).
- Implementation: RSA2048 + SHA256
- **Algorithm**
 - Generation of public and private keys
 - Signature (encryption on the device)
 - Signature verification (decryption) - provided by Huawei



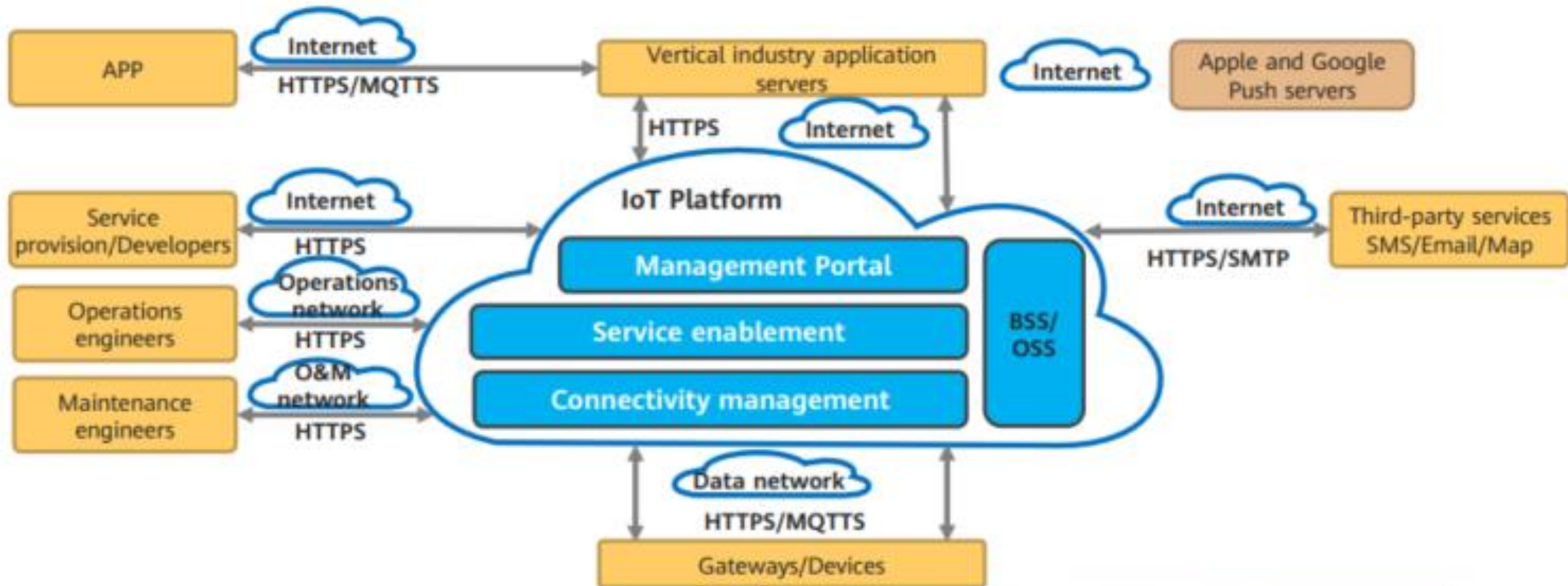
Chapter 02

Pipe Security: Anti-DDoS and Signaling Storms



Chapter 02

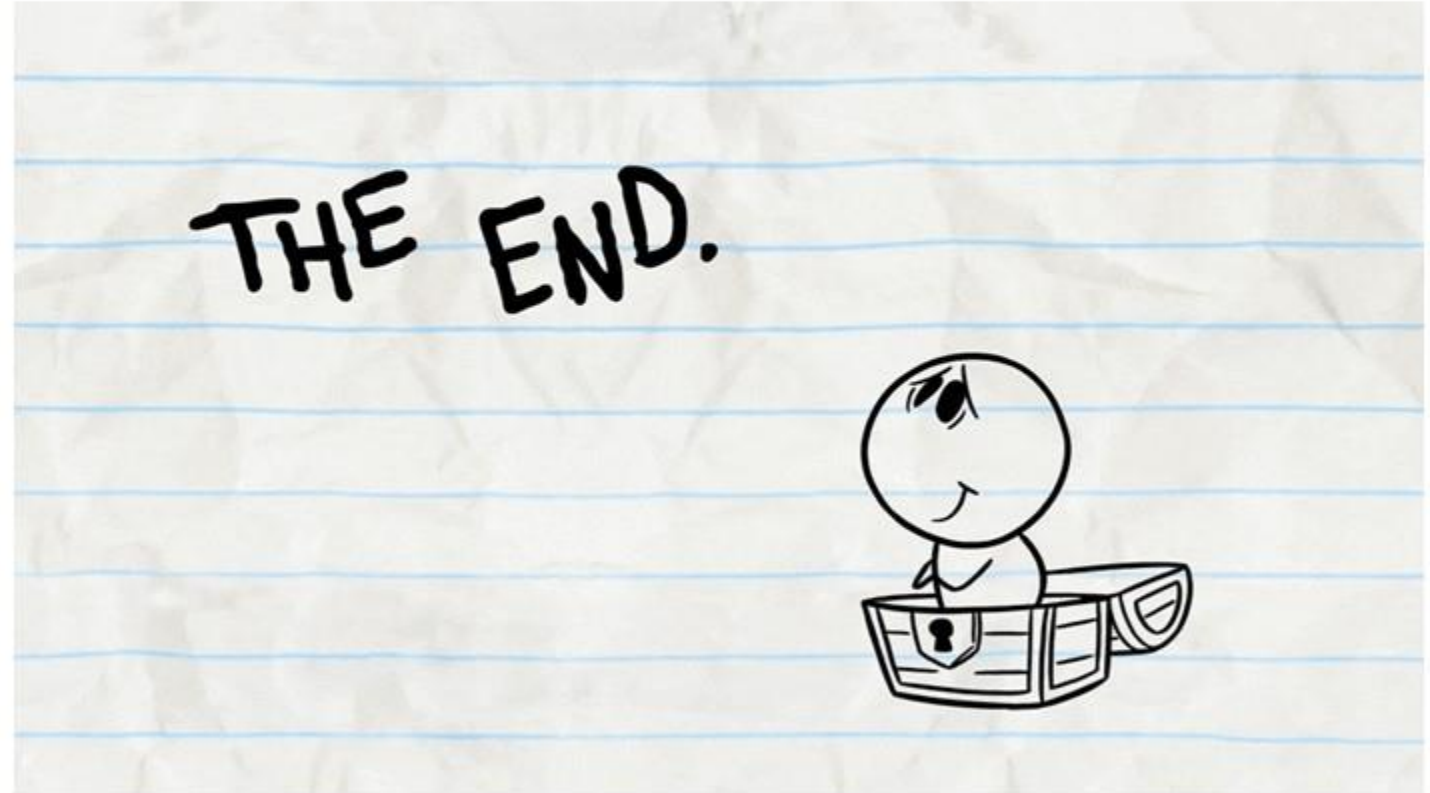
Cloud Security: E2E Authentication, Access, and Transmission Security on the IoT Platform



The IoT security solution provides secure transmission channels and trusted access. It also provides two-factor authentication (certificate + password or SMS + password) for key interfaces to ensure communication security. E2E security authentication management ensures transmission security of APIs.

The End

Please feel free to contact me anytime if you have any questions



جامعة القادسية
EVERYONE'S SMART UNIVERSITY