HUAWEI

IoT Security White Paper 2018

——Evolving Security Architecture

PREFACE

The Internet of Things (IoT) is comprised of billions of connected devices, collecting and sharing data. This data can be gathered, analyzed, and monetized. The changing service environment brings new security threats and challenges to various industries.

In February 2017, Huawei released the white paper *Building a Trusted and Managed IoT World* with Instituto Nacional de Ciberseguridad (INCIBE) and Red.es of Spain at the Mobile Work Congress 2017. In October 2017, Huawei proposed an innovative 3T+1M IoT security architecture to meet E2E security requirements from devices to applications. Huawei also released the *IoT Security White Paper 2017* to drive efforts for building industry security.

This white paper embodies the preceding ideas and describes the latest achievements in IoT security research and best practices. It discusses how to build IoT security ecosystems by working with governments, industries, standardization/certification organizations, and industry alliances. Huawei works with stakeholders to explore and address the security risks and privacy protection requirements brought about by new technologies and to encourage rapid and sustainable development of the IoT industry.

CONTENTS

1 IoT Trend and Threats

1.1 IoT Development Trend

The fourth industrial revolution is creating an environment in which everything will be perceptible, interconnected, and intelligent. IoT is the cornerstone of this new era. ICT powers the ability of IoT to reshape traditional industries. By integrating the physical and digital worlds, IoT shortens business processes, boosts productivity, and provides better products and services, while, at the same time, unleashing the huge potential for innovation.

In the future, everything will be connected in scenarios more diverse than simply connected people. For example, governments want to make everything intelligent. From street lighting, parking, and bicycles, to water meters, gas meters, manhole covers, fire protection, and environment monitoring, governments hope that IoT will improve quality of life and increase city management efficiency. This will bring a new wave of connectivity services, presenting great opportunities for development. At the same time, the IoT platform is used to integrate the open asset data of different industries. This data may be sourced from water, gas, and electricity meters, intelligent door locks, pet tracking, home security, luggage, vehicles, and so on. Through the unified portal, IoT can make people's lives both smarter and more convenient.

As everything becomes connected and intelligent, the IoT brings huge economic value. It is driving the digital transformation of all industries. From governments and organizations to businesses and local communities around the world, everyone is actively investing in and researching the IoT. They collect, analyze, and apply data generated through the IoT, facilitating the rapid development of all industries.

According to Huawei's Global Industry Vision (GIV) predictions, everything will be brought into a digitalized and intelligentized world where everything is both perceptible and connected. By 2025, it is predicted that 40 billion smart devices will be in use worldwide, with a total of 100 billion connections in public utilities, transportation, manufacturing, medical care, agriculture, finance, and other industries. The IoT promotes digital transformation, creating a digital economy worth US$23 trillion[1]. With the comprehensive improvement of perception and connectivity capabilities, the IoT connects huge numbers of devices to achieve breakthroughs. It not only creates value from data but is also becoming part of our everyday life.

1.2 IoT Security Threats and Challenges

One of the many values of the IoT is that it is driving the digitalization of all industries; however, the IoT brings with it new security threats due to new technology applications.

[1]GIV 2025, https://www.huawei.com/minisite/giv/en/

As the tools used in attacks become more sophisticated, Machine Learning (ML) and Artificial Intelligence (AI) will compound attack-defense confrontation. Although AI can be used to rapidly detect new security threats, it can also be used to launch attacks. The technical barriers for implementing attacks become lower. IoT devices, including refrigerators, vacuum cleaners, water meters, and street lights, will become potential targets for attack. By 2020, Gartner predicts that more than 25 percent of identified attacks in enterprises will involve the IoT[2]. In addition, devices at different physical locations and network layers are connected to each other, breaking up the boundaries of traditional network security and generating more attack vectors. Attacks can be launched at different locations to target different layers, creating a springboard effect where attackers can leverage small vulnerabilities to open up larger ones. Of note is that attackers have transformed the way in which they launch attacks. Attacks that were once launched on vulnerable devices are now being launched on legitimate devices. Attackers now use automation tools to simulate authorized operations on legitimate devices, which are then exploited as a springboard to launch attacks.

As the IoT enters a more pragmatic and operational phase, industry customers are aware of the importance of IoT security. Gartner predicts that worldwide spending on IoT security will reach US$1.506 billion in 2018, a 28 percent increase[3] over the US$1.174 billion spent in 2017. Different commercial sectors face a wide range of different threats. For example, the Internet of Vehicles (IoV) may face completely different threats and security challenges compared to those facing intelligent street lighting. IoT security needs to move from single products to end-to-end solutions and eventually to the entire security architecture. The evolving security architecture is used in future business scenarios, such as Smart City, smart energy, smart transportation, smart manufacturing/industry 4.0, smart life, and autonomous driving.

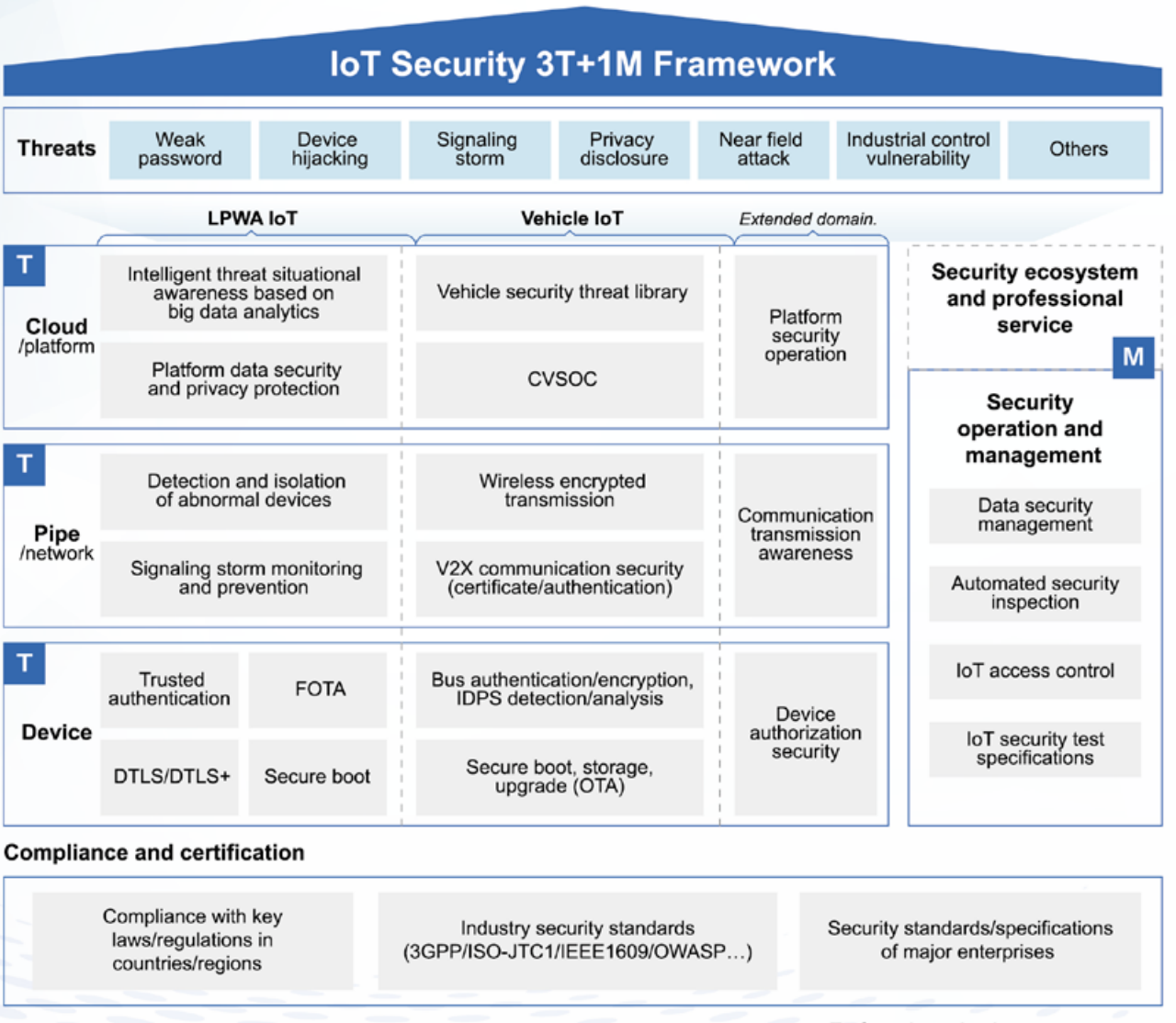
[2]Leading the IoT, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

[3]Gartner, https://www.gartner.com/newsroom/id/3869181

2 Constantly-Evolving 3T+1M Security Architecture

IoT security is involved in Low Power Wide Area (LPWA) networking, the IoV, industrial IoT, wearable devices, and other industries. In the IoT ecosystem, numerous IoT devices generate and use massive amounts of data. The pipe ensures transmission security of highly concurrent data, and the cloud and IoT platform provide support for a wide range of IoT applications. These support systems and applications may become potential targets of malicious attacks. The 3T+1M security architecture focuses on the security features of the device, pipe, cloud, and platform to address the security threats at the sensor, network, and application layers in the IoT. Based on platform and cloud security, Huawei leverages its extensive experience in telecom network security to provide IoT security situational awareness and analytics. Working together with ecosystem partners, Huawei is relentless in its pursuit of addressing IoT security threats and challenges. In its efforts to ensure continued evolution and technological innovations in the 3T+1M security architecture, Huawei considers the wide range of industry requirements for IoT cloud-pipe-device security, especially differentiated security requirements. The 3T+1M security architecture builds security in innovation and meets diverse security requirements in evolution.

Figure 2-1 IoT security 3T+1M framework



T : Security technology
M: Security operation and management

In the 3T+1M IoT security architecture, 3T refers to IoT device defense, pipe security assurance, and cloud protection technologies, and 1M refers to security operation and management. This architecture focuses on the security of IoT scenarios (such as the IoV, LPWA, and industrial IoT) to ensure compliance with national and regional laws/regulations and industry standards and build an end-to-end IoT security protection system. The 3T+1M IoT security solution consists of the following parts:

1. IoT device defense technology family (1T): provides matching security capabilities and device-cloud synergy for IoT devices with different processing capabilities in different application scenarios. Basic security capabilities, such as DTLS/DTLS+ (for Datagram Transport Layer Security), trusted DICE, FOTA upgrade, and secure boot must be provided for weak devices (including LPWA smart meters and locks for shared bicycles). For strong devices (including IoV T-Box and OBU), security certificate management, intrusion detection, encryption authentication, and Trusted Platform Module (TPM) are required.

2. IoT pipe assurance technology family (1T): provides malicious behavior detection and isolation, especially for abnormal behavior of IoT devices (such as IoV T-Box and LPWA smart street lights). Abnormal behavior includes abnormal traffic transmission and abnormal reporting frequency. Different IoT pipe security capabilities are enhanced for different scenarios. For example, anti-DDoS and signaling storm prevention capabilities are improved for NB-IoT devices. For Cooperative Intelligent Transport Systems (C-ITS) of connected vehicles, the trusted capability of Vehicle to Everything (V2X) communication needs to be improved.

3. IoT platform protection technology family (1T): focuses on how to build IoT platforms and clouds to provide security situational awareness based on big data analytics, security analysis/awareness of connected vehicles, and IoT data security and privacy protection for LPWA, and to provide configurable cloud security assurance capabilities for customers.

4. IoT security operation and management (1M): focuses on how to develop security operation and management specifications and procedures and construct E2E security O&M tools to improve operation and testing efficiency. It also focuses on improving the IoT security system in terms of threat prevention, detection and analysis, and response. This includes improving security inspection tools, periodic IoT security evaluations, and automated device and application security detection tools.

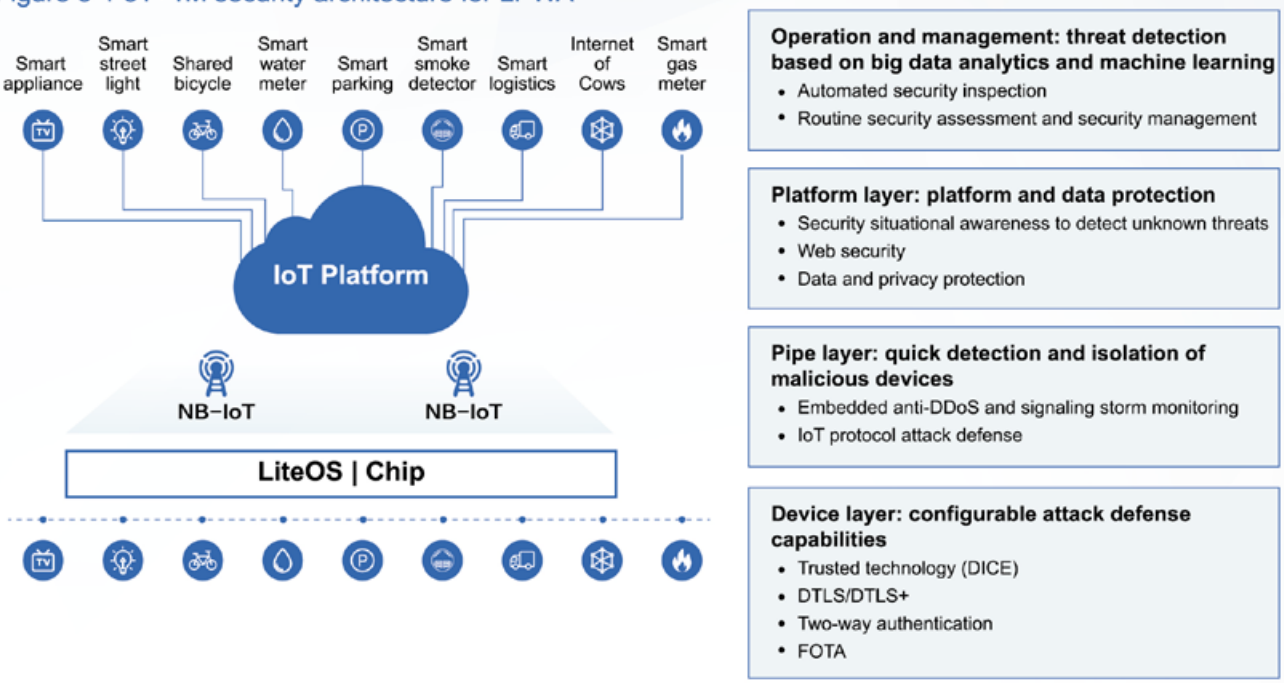
In the 3T+1M security architecture, key IoT security technologies are applied to mitigate different security risks. Some technologies focus on device security, whereas other technologies focus on pipe or cloud security. These technologies, however, are not isolated. The security system is the combination of device, pipe, cloud, and operation security technologies. If IoT devices have limited resources and application scenarios, the security system in particular requires device-cloud/pipe synergy — for example, trusted device, malicious device detection, and DTLS+.

3

3T+1M Security Architecture in LPWA

The LPWA is designed for IoT applications characterized by low bandwidth, low power consumption, long distance, and large number of connections. It is widely used in the infrastructure field, such as smart lighting, smart parking, and smart metering. The IoT 3T+1M architecture implements multi-layer security protection.

Figure 3-1 3T+1M security architecture for LPWA



Configurable device defense capabilities

The attack defense capabilities of IoT devices are configurable. For IoT devices with limited resources and sensitive to power consumption, matching security capabilities are provided: for example, FOTA for remote security upgrade management, LiteOS for lightweight security, DICE for lightweight trusted computing, and DTLS+ for lightweight secure transmission.

Malicious device detection and isolation

Abnormal behavior can be detected, and malicious IoT devices can be isolated. For example, along NB-IoT network pipes, device storm detection services are provided. Big data analytics is used to detect abnormal NB-IoT devices so that malicious devices can be isolated. In addition, network access blacklists/whitelists are supported.

Platform data security and privacy protection

The cloud platform provides data security and privacy protection capabilities, including data privacy protection and lifecycle management, data API security authorization, and tenant data isolation. Cloud security (such as WAF, firewall, and HIDS) and big data security technologies are used to protect the platform against malicious attacks.

Security Operation and Management (O&M)

Security O&M includes routine IoT security evaluation, security reporting, and automatic identification of security events based on best practice policies. The security management platform can be provided for policy configuration, policy orchestration, policy execution.

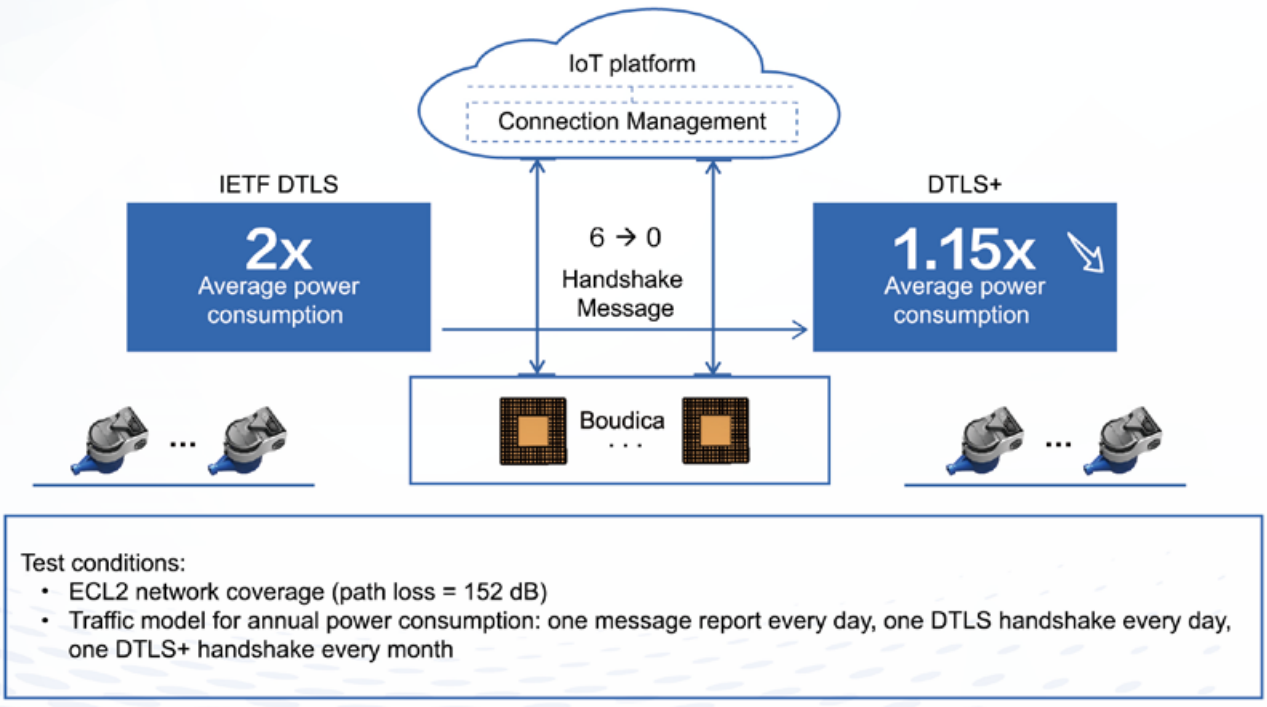
3.1 Key LPWA Security Technologies

A number of factors related to LPWA scenarios should be considered before designing the LPWA security solution. Factors such as cost and battery life play an important role in decision-making. The following describes key network security technologies in specific service scenarios:

- **DTLS+**

To reduce battery power consumption, NB-IoT devices generally spend most of the time in sleep mode. Each time a device wakes from sleep mode, if it uses DTLS for encrypted communication, the device must perform a series of handshake actions to establish a secure channel. This process consumes a significant amount of power. To address this issue, DTLS+ introduces connection ID to reuse previously established secure channels. This innovative feature removes the need to establish a new secure channel each time a device wakes from sleep mode. By allowing previously established secure channels to be reused, DTLS+ provides significant power savings by 40% for NB-IoT devices. DTLS+ has been incorporated by IETF TLS as the DTLS Connection Identifier draft and will be released officially.

Figure 3-2 General comparison between DTLS and DTLS+



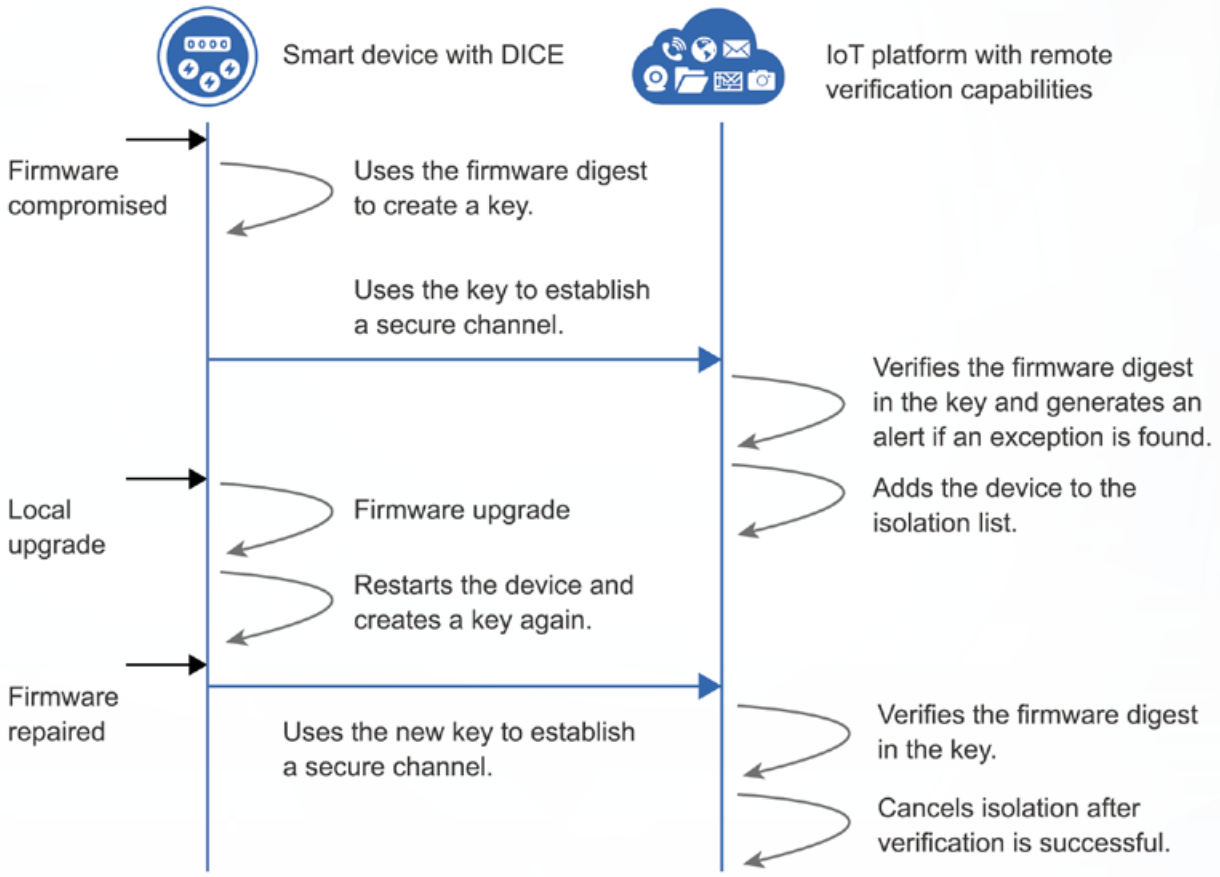
DICE

Many NB-IoT devices are deployed outdoors and are vulnerable to attacks and tampering. In addition, these devices often have limited resources (for example, limited battery capacity) with low performance. To address the resource limitation issues faced by NB-IoT devices, the Boudica chip introduces lightweight trusted computing capabilities, in accordance with the Device Identifier Composition Engine (DICE) specifications formulated by the Trusted Computing Group (TCG).

After IoT devices establish their identity authentication identifiers using DICE, the IoT platform remotely verifies the device firmware. If an exception is detected, the platform generates an alert and isolates the device. The DICE brings the following benefits:

- Device forgery prevention, providing hardware-based identity identification
- Remote attestation of device integrity
- Secure zero-touch provisioning of devices

Figure 3-3 DICE working process



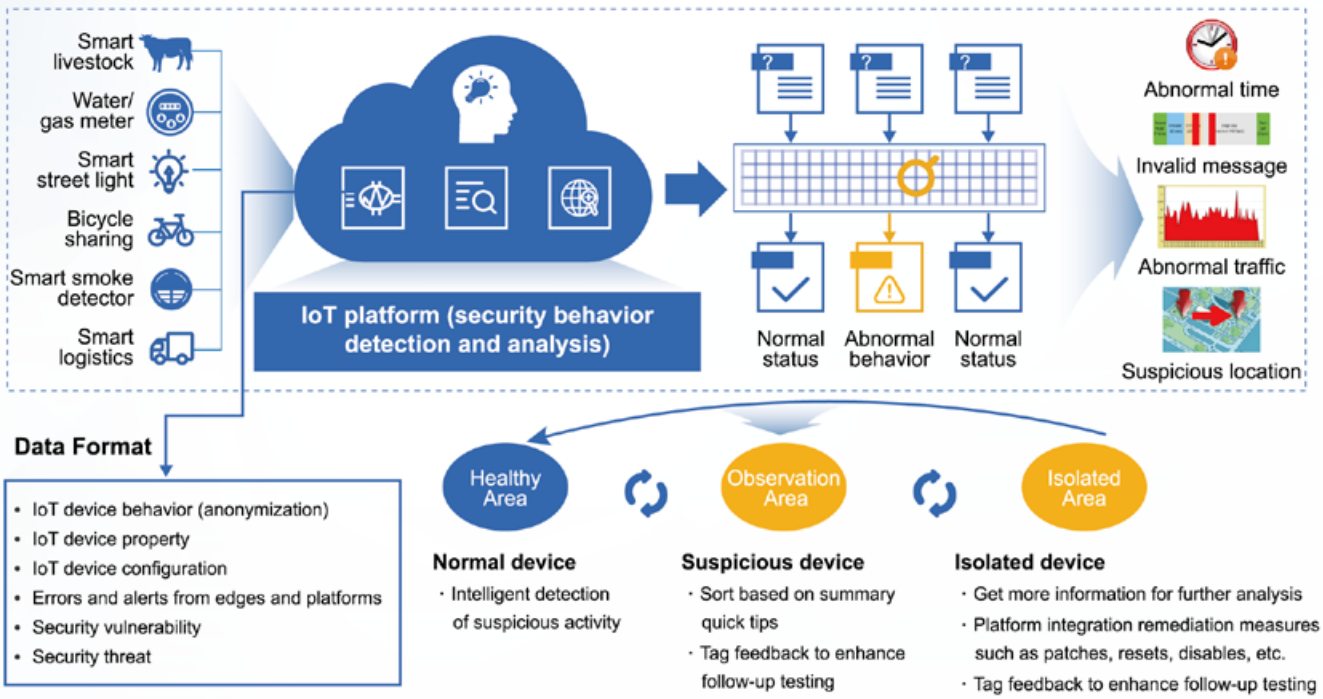
Device behavior detection and isolation

Even though diverse types of IoT devices already exist, more types of IoT devices continue to emerge; however, the way in which different vendors implement the wide range of functions provided by these IoT devices may differ significantly. Therefore, these devices may pose security risks. Under malicious control, these devices might be used to negatively impact business operation, attack the platform and network, or even affect Internet users. The IoT solution must, therefore, be able to rapidly identify abnormal devices from vast numbers of legitimate devices and then isolate them. This is a technically challenging feat to accomplish.

The abnormal device detection feature brings the following benefits:

- Visualized device security status
- Improved security management efficiency
- Mitigated security risks
- Graded management to balance between efficiency and security

With privacy protection, IoT device properties, configurations, alerts, and behavior are used for IoT modeling and big data analytics. The IoT platform works with the external threat information to identify and isolate malicious IoT devices. The normal, suspicious, and abnormal devices can be detected in a visualized manner.

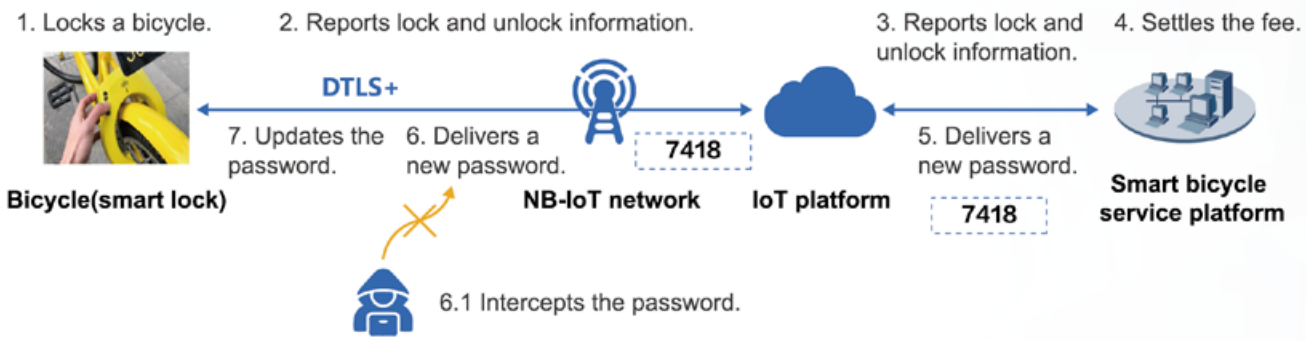


3.2 Bicycle-Sharing Service

Bicycle sharing uses wireless technology to help locate, lock, and unlock bicycles. This service is an environmentally friendly way for people to travel an average of 3 kilometers.

Users interact with the bicycle service platform to obtain passwords to unlock the smart locks on bicycles. Attackers can launch Man-in-the-Middle (MITM) attacks to steal these passwords and obtain free use of bicycles. To prevent such attacks, data transmitted over networks must be encrypted. Smart locks establish transient connections with the platform only when messages need to be reported or received. DTLS, used for network communication encryption, requires high power consumption and, therefore, reduces the battery lifespan of battery-powered smart locks. DTLS+ provides the same secure communication between smart locks and the IoT platform but significantly reduces the power consumption of smart locks.

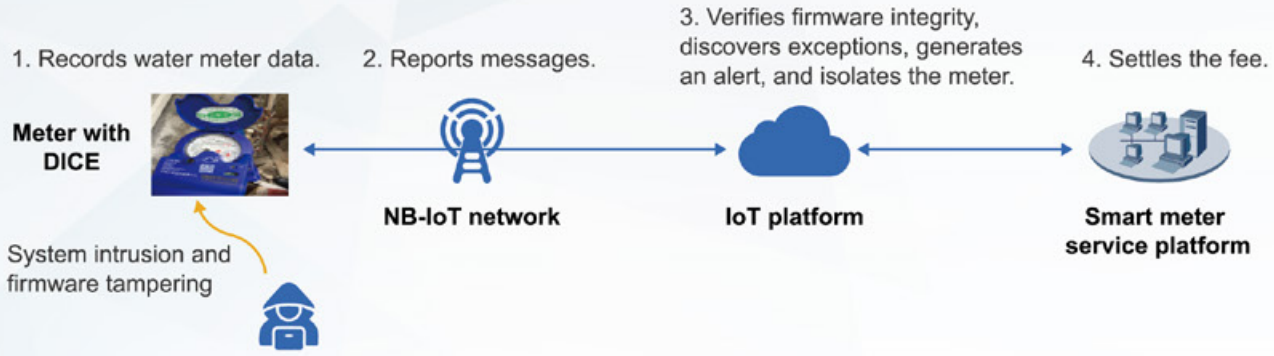
Figure 3-4 Attack and defense in the bicycle-sharing service



3.3 Smart Water Meters

Smart water meters require low power consumption and wide coverage. The platform allows water meters from different vendors to access the platform and provides unified data management capabilities for water companies to achieve intelligent metering.

Smart meters automatically send metering data to the water company for billing. Fraudulent users may attack the firmware or software running on smart water meters through wireless or serial port access to obtain water at a cheaper rate or even free. To prevent this issue, the Boudica chip with built-in lightweight trusted computing capabilities (DICE) is provided. If the firmware of a water meter using the Boudica chip is tampered with, the IoT platform uses DICE to detect firmware tampering, isolates the water meter, and generates an alert. The water company can then take appropriate action and repair the firmware. After the repaired water meter accesses the IoT platform, the platform authenticates the water meter and allows the water meter to report service data.



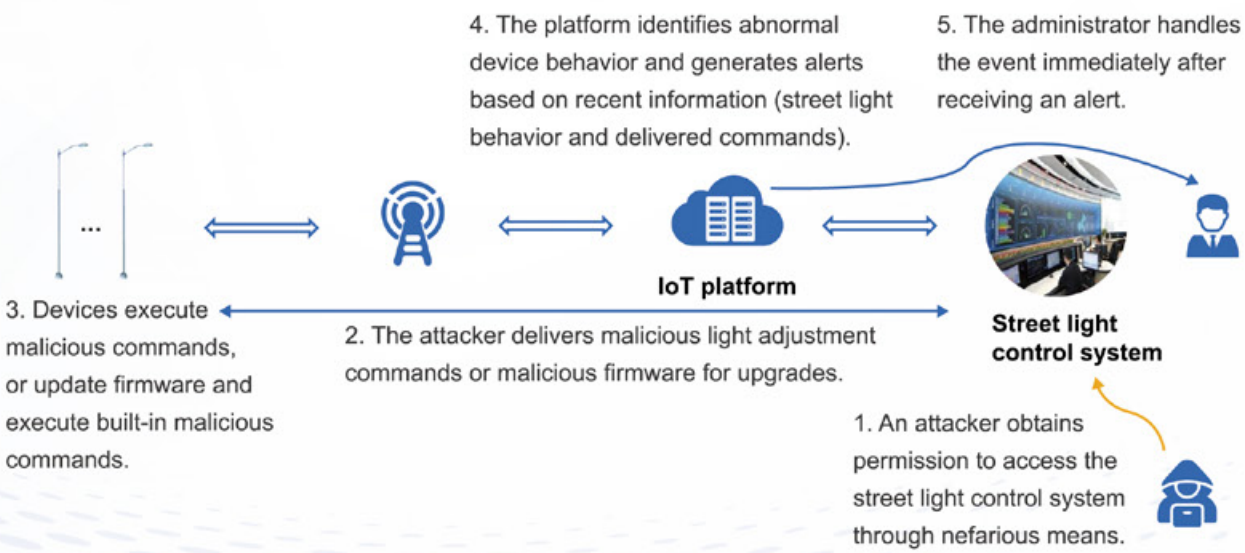
3.4 Smart Street Lights

The Smart Street Light solution provides intelligent control and detection functions, such as timing control, remote real-time control, and single-light detection.

Street lights are part of the public infrastructure that facilitate nighttime travel and safety. The street light control system or application can be exploited to affect lighting in certain blocks or even an entire city, causing panic and security risks. Administrators will learn of the event only after people call in to report malfunctioning lighting.

Unauthorized users deliver malicious commands through the street light control system or perform unauthorized operations through malware, and these behaviors differ from the normal ones. The IoT platform collects and analyzes device behavior, identifies abnormal behavior, and generates alerts.

Figure 3-5 Attack and defense in the smart street light service



3T+1M Security Architecture in Connected Vehicle

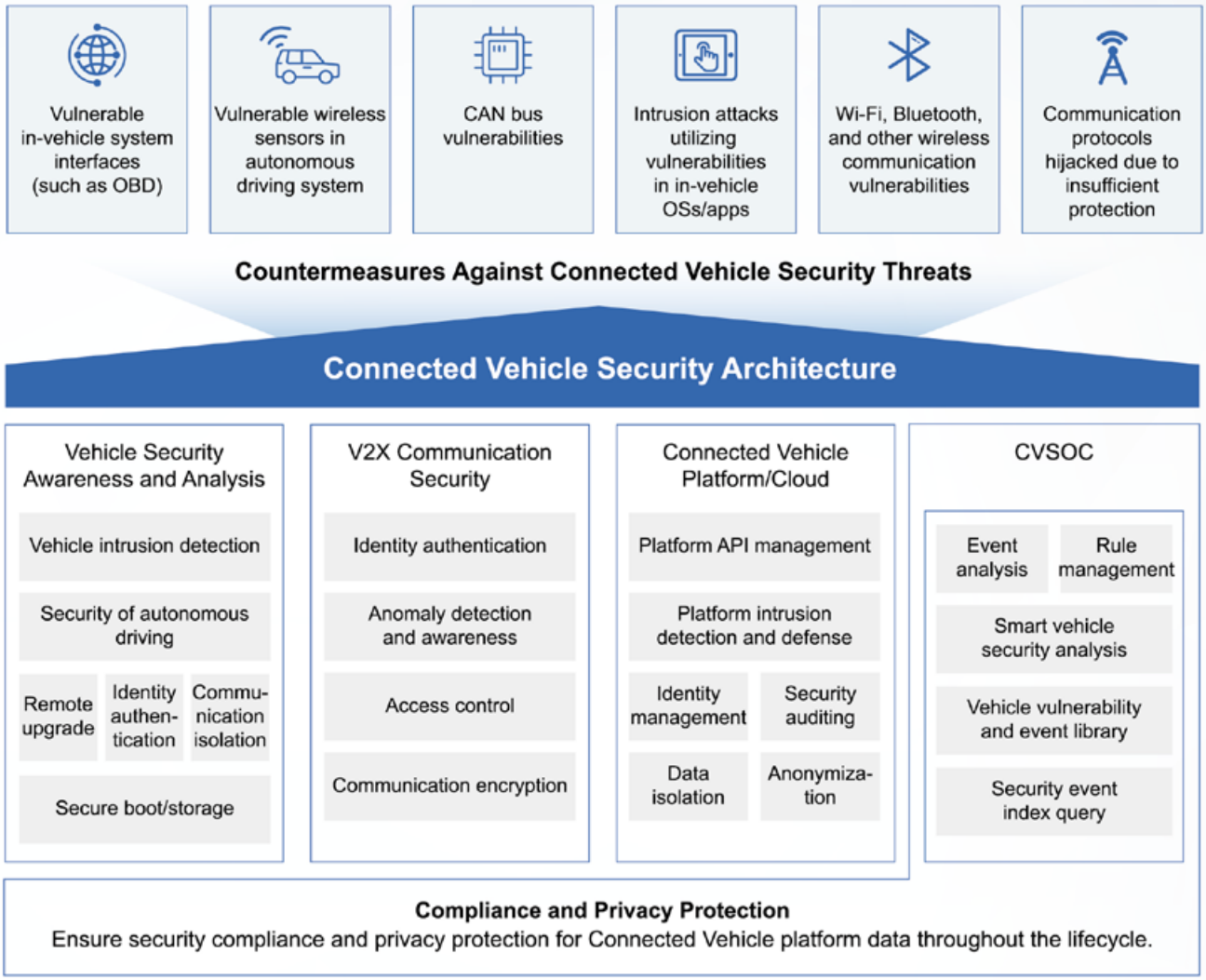
Industry organizations around the world have been developing the IoV for decades. With the promotion of pilot projects and IoV alliances, relevant standards have been gradually improved and technologies have become mature. Many countries give direct financial and professional support for IoV development.

Huawei's Connected Vehicle Solution includes vehicles, roads, networks, and a connected vehicle cloud platform, all of which collaborate with each other in a smart manner to facilitate travelling and ensure personal safety. Connected vehicle components face different security threats.

Connected Vehicle Component	Characteristics	Major Threats
Smart vehicle	Multiple wireless access modes: Bluetooth, Wi-Fi, 2G/3G/4G/5G, V2X, etc.	Attackers can use different wireless access modes to gain entry to and control vehicles.
	Multiple wired access modes: CAN, OBD-2, Ethernet, USB, etc.	During vehicle repair and maintenance, attackers can gain entry to and control vehicles by installing malicious hardware or software carrying intrusion programs.
	The vehicle's electronic system is becoming more sophisticated. Most vehicles have more than 100 Electronic Control Units (ECUs) running more than 100 million lines of code.	Attackers use reverse engineering to discover vulnerabilities and control remote vehicles. For example, an attacker may remotely control a running vehicle to brake or change direction, posing serious security threats.
	The autonomous driving system is being developed and deployed on high-end smart vehicles. Some newly developed mid-range vehicles also have the L2 autonomous driving capability.	Attackers can deceive some detectors, such as satellite positioning signal spoofing, image spoofing, Wi-Fi location spoofing, and radar signal spoofing.
	Keyless vehicles are widely available.	Cases of keyless vehicle thefts are common.
Smart road	Traffic devices (such as network cameras and traffic screens) and V2X devices (RSU) are used to communicate with vehicles and drivers to reduce traffic jams.	Traffic devices (such as cameras) may be accessed and controlled due to vulnerabilities such as weak passwords, permission authentication bypass, and XML injection vulnerabilities. Attackers can broadcast false information to cause traffic chaos.
Network	As a pipe for information transmission, the communication system must prevent sensitive data leakage and ensure data confidentiality and security. Mature communications technologies, such as identity authentication, secure channel, and data encryption, are used to protect communication data security.	Data leakage and MITM attacks are likely to occur in the communication system due to vulnerabilities of communications protocols.
Connected vehicle cloud/platform	The connected vehicle cloud stores a large amount of data about vehicles and their owners (for example, user IDs, locations, and driving routes) and is a high-value attack target.	By exploiting platform vulnerabilities and identity authentication defects, attackers have launched numerous intrusion and data theft attacks to expose large volumes of privacy information.

The connected vehicle security architecture embraces all connected vehicle components. In addition to traditional IT security capabilities, such as secure boot, secure storage, access control, cloud firewall, identity authentication, anti-DDoS, and virus detection, the connected vehicle security architecture uses new technologies, including big data analytics and vehicle intrusion detection and prevention.

Figure 4-1 Connected vehicle security architecture



Vehicles are an essential mode of transport, with over 1 billion vehicles on the world's roads. Many of these vehicles are vulnerable to attacks and intrusions during their lifecycle. Timely intrusion detection is an important measure to ensure vehicle security. The IDS and IPS protect the wireless and physical attack entry points, such as Wi-Fi, Bluetooth, mobile, OBD-2, USB, TPM, GPS, and radar interfaces, on vehicles. Different interfaces require different security technologies to detect and defend against external attacks. At the same time, functional modules inside the vehicle must be isolated from each other. For example, the In-Vehicle Infotainment (IVI) system must be strictly forbidden to send instructions to the vehicle control system. Abnormal behavior needs to be recorded in real time and reported to the Connected Vehicle SOC (CVSOC) on a regular basis.

The CVSOC conducts intelligent analysis on the reported data to determine whether real threats exist. Once a threat event is confirmed, the CVSOC traces the source of the threat and generates a rule for detecting and preventing the threat. The rule is then delivered to each connected vehicle through a secure channel so that the vehicles can detect and defend against such a threat in real time.

Counterfeit entities cause serious risks to connected vehicle services. For example, a counterfeit RSU may send fake traffic accident information, resulting is traffic disruption; therefore, mutual trust must be established among the vehicle, RSU, connected vehicle cloud platform, and communications network. An independent identity authentication system must be established for connected vehicle services to ensure mutual service trust and identify counterfeit entities in a timely manner.

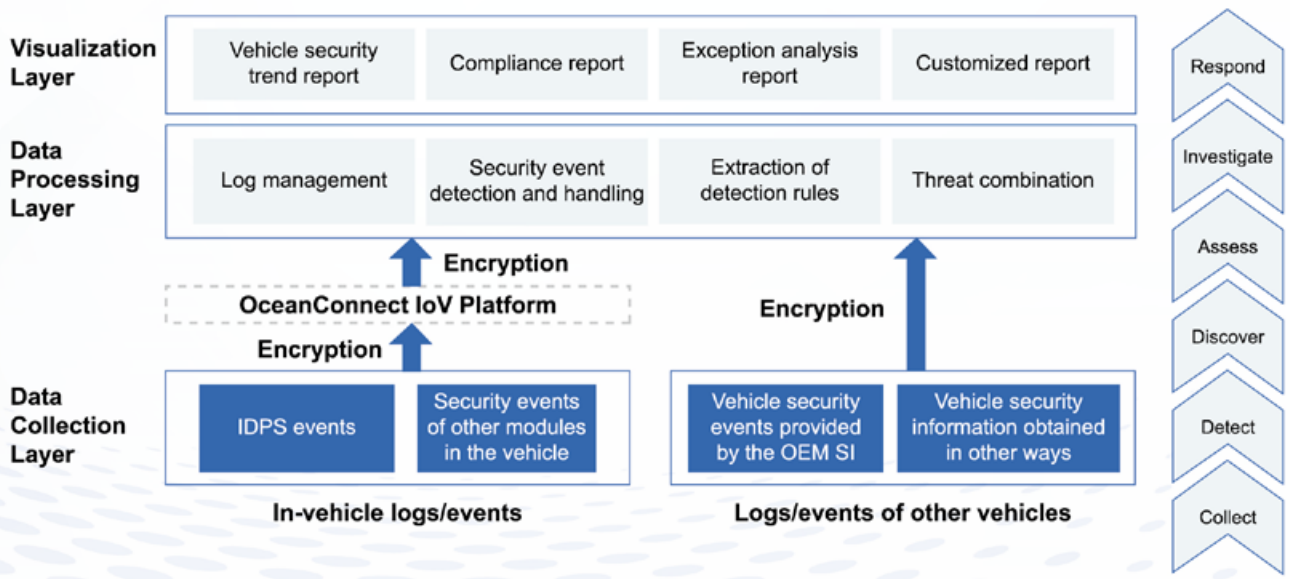
The connected vehicle cloud platform contains a large amount of private user information. Most people want to protect their privacy as far as is reasonably practical. China's Personal Information Protection Act has been drafted to solicit comments and suggestions. The General Data Protection Regulation (GDPR) in the EU has set detailed privacy protection requirements. Protecting the privacy of data in connected vehicles is critical, in terms of both customers and relevant laws and regulations.

4.1 Security Detection Analysis and Awareness of Connected Vehicle

Vehicle security is a major concern of vehicle manufacturers. In connected vehicles, security refers to personal safety incidents caused by network vulnerabilities or property loss caused by vehicle theft. Vehicle security protection and threat visualization are indispensable to connected vehicle security.

The CVSOC collects, analyzes, and visualizes the security events of connected vehicles on the cloud.

Figure 4-2 CVSOC



Data collection layer: collects security logs and events from connected devices, such as the ECU, gateway, and IVI. The CVSOC processes and analyzes the collected data in a unified manner. This layer can also import security logs and events provided by vehicle OEM vendors and other vehicle service providers.

Data processing layer: classifies the collected security logs and events, generates indexes, implements correlation analysis to automatically detect security events, generates alerts, and evaluates event severity. In addition, this layer displays security events and their severity on the dashboard, or alerts related operation personnel by email. The data processing layer determines whether the reported security event is a real security threat. If security threats are detected, the data processing layer analyzes the threats and generates detection and prevention rules. This layer allows you to define your own security detection and prevention rules based on analysis by security professionals, thereby consistently improving the threat detection and prevention capabilities of connected vehicles.

Visualization layer: helps the operation personnel learn about vehicle security conditions (for example, how many vehicles are attacked, how many vehicles are intruded, and how many vehicles are vulnerable) by displaying security analysis reports and security situation information on the dashboard. O&M teams can establish security O&M policies based on the current security situation.

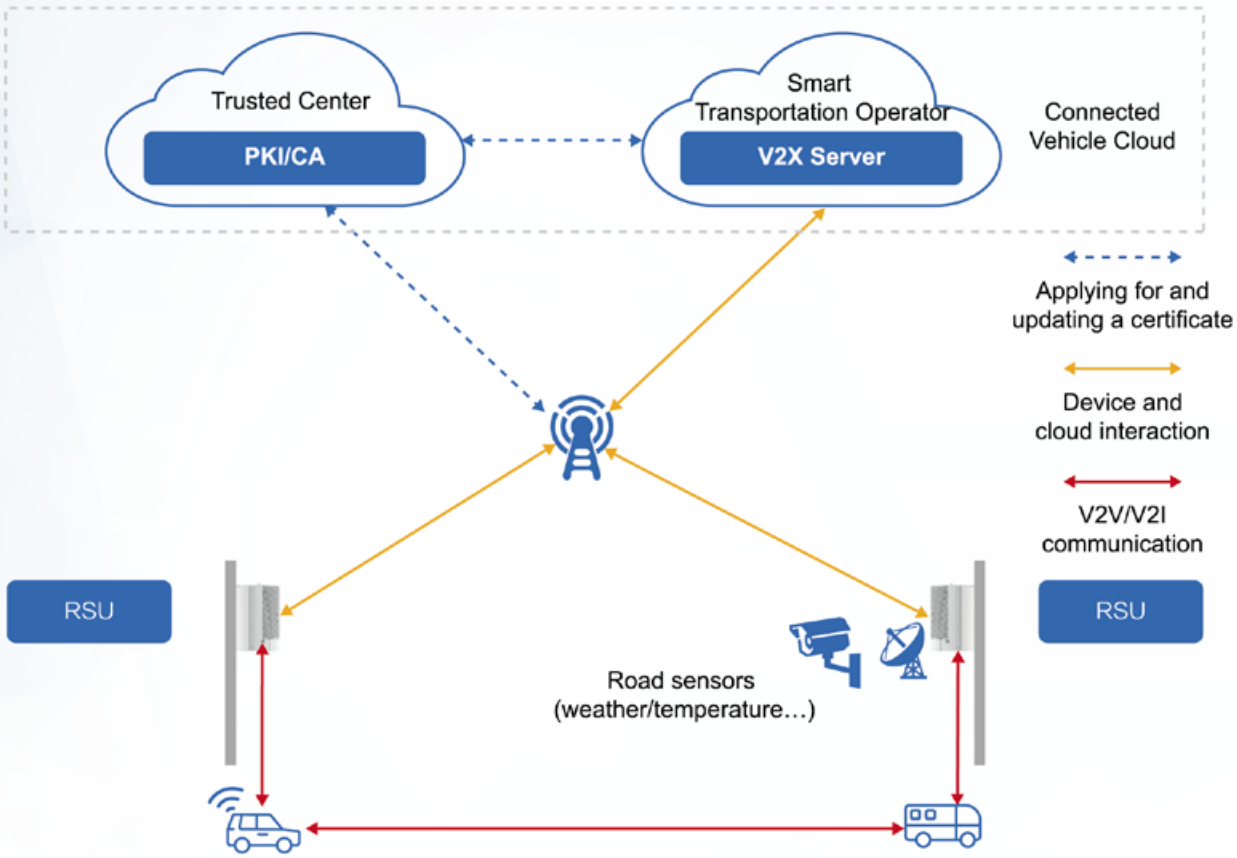
The CVSOC analyzes numerous logs to search for security attack behavior and uses technologies such as Machine Learning (ML) and Artificial Intelligence (AI) to analyze security big data and abnormal behavior. The CVSOC also considers third-party threats and analysis results from vehicle security specialists to monitor and prevent security threats so that it can ensure vehicle security. With the CVSOC, the operation personnel can learn about vehicle security situation in real time to monitor and mitigate complex, unknown, and ever-changing threats in a smart manner, preventing personal injury and property loss caused by security issues.

4.2 V2X Collaborative Authentication

If the entities in Connected Vehicle are counterfeited, travel efficiency may be compromised, and traffic congestion or even traffic accidents may occur; therefore, establishing trust relationships among vehicles, roads, networks, and clouds is fundamental to blocking counterfeited entities from V2X services.

Trust relationships need to be established for services, such as fleet vehicle management and vehicle sharing services, based on Connected Vehicle. For fleet vehicle management services, ensure mutual trust between fleet vehicles and the fleet management platform. For vehicle sharing services, ensure mutual trust between shared vehicles and the sharing platform. Specifically, different Connected Vehicle services or applications must use different trust subjects to ensure trust relationships, prevent identity spoofing, and further ensure data integrity and source reliability.

In V2X services, trust relationships must be established between entities (including the vehicles, RSU, and V2X platform). This ensures that messages sent by each entity can be trusted and counterfeited entities can be identified and eliminated. If a CA is used to establish a trust relationship, a trusted center authorized by an intelligent transport operator is required to issue V2X service certificates to each legitimate entity, allowing trust relationships to be established between entities. After a trust relationship is established, a legitimate entity includes its signature in the V2X service message it sends. The receiving end checks whether the message source is legitimate and whether the message is intact, preventing fake messages from counterfeited entities.



Because the network layer is the information transmission channel of all services, it must be able to distinguish legitimate devices from illegitimate devices. Currently, operators' identity identification technologies, such as the SIM, are used to ensure mutual authentication between devices and the network. Confidentiality of sensitive data in transit must be ensured. At the network layer, secure channel protocols such as TLS can be used to ensure data confidentiality. Identity authentication and secure channel technologies ensure the integrity and confidentiality of the data transmitted on the communication channel and ensure trusted data sources.

4.3 Vehicle Data Security and Privacy Protection

The connected vehicle platform holds a large amount of data about vehicles and their owners, including user IDs, locations, and driving routes, as well as infrastructure data. This platform is, therefore, a high-value attack target. In 2017, an outsourced employee working at an enterprise stole and sold a large volume of users' travel records, compromising user privacy. In 2016, an Internet platform was attacked, leaking personal information about more than 50 million users and drivers. These incidents shattered customer confidence, destroying the business's reputation and causing significant business losses. Legal proceedings were even brought. Information disclosure may have a greater impact on individuals, affecting people in not only psychological and reputation terms but even their personal safety.

The main issues of privacy protection concerns are irrelevance, transparency, and intervention. Using privacy protection technologies can reduce management costs and privacy leakage risks. Common privacy protection technologies include data masking, equivalence class anonymity, and differential privacy protection. Data masking means anonymizing data using such tools as mask, truncation, hash, and noise algorithms. After data anonymization is complete, private information is effectively protected. Privacy disclosure through data correlation persists when common anonymity technologies are used.

To cope with this situation, equivalence class anonymity technology is used to prevent sensitive information and identity information from being correlated from multiple user attributes. This technology can form equivalence classes by generalizing individual user information. Users in each equivalence class have common attributes, and attackers cannot correlate user information with a single user. This reduces privacy risks. The differential privacy technology distorts data by adding random noise to prevent attackers from learning information about a single user, and meets the requirements of statistics analysis and data mining for group data. The differential privacy technology outperforms other privacy protection technologies, and its protection can be proved and measurable.

Technologies that are more-efficient and advanced (such as differential privacy protection) are maturing, and laws and regulations impose strict privacy protection requirements. Applying these advanced technologies to various services is a growing trend. While protecting user privacy data, the connected vehicle cloud platform needs to use advanced technologies to ensure law/regulation compliance during data collection and reduce data leakage risks.

According to the GDPR (EU) regulations, the connected vehicle platform needs to pay significant attention to privacy risk assessment, privacy management policies/organizations, and privacy protection technologies to prevent data leakages. Currently, the Privacy Impact Assessments (PIA) analysis method is used for privacy risk assessment. Huawei works closely with third-party partners to prevent data leakages.

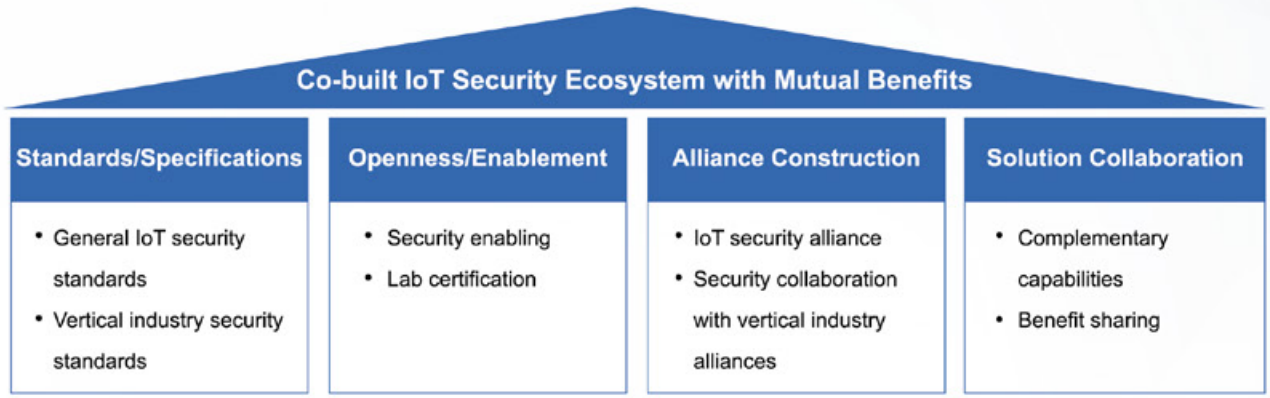
Ensuring user privacy is the basic responsibility of an enterprise. The enterprise technically protects user privacy while formulating sound rules and regulations on privacy protection.

5 Co-building IoT Security for Mutual Benefits

Security assurance is the prerequisite for IoT development. In many industries, security requirements are different, and neither comprehensive nor mature industry security solutions are available. Security risk assessment and response are still underway. IoT security research is a new technology field, and construction of a security ecosystem is just beginning.

The IoT industry requires constant technological innovations. Huawei works with governments, industry partners, and users to address new technology risks in different IoT fields, build IoT security, and enjoy social and economic benefits and conveniences from IoT development.

Figure 5-1 IoT security ecosystem



5.1 Defining Security in Standards

Standards play a vital role in the development of technology. Products and solutions must depend on or comply with their applicable standards. Likewise, IoT standards play an increasingly important role because the IoT is a combination of multiple technologies, from underlying access technologies to upper-layer applications in different vertical industries. IoT security is receiving considerable attention from various standards organizations, including ICT organizations (such as 3GPP, OneM2M, ITU, IETF, IEEE, and CCSA) and associations/organizations of different vertical industries (such as the IoV, gas, water, street light, and environmental protection). Standardization of IoT security is still in the initial phase. Relevant organizations are putting forward security proposals and working out security technical standards to respond to IoT security challenges and build ecosystems that are more intelligent and connected.

Today, many IoT and vertical industry standards organizations are promoting IoT security standards and making great achievements, especially in device security, NB-IoT network security, and IoT distributed security authorization. Take LPWA as an example. Traditional DTLS cannot apply to services (such as metering, parking, and firefighting) that are powered by batteries and sensitive to power consumption. To address this issue, Huawei innovatively optimizes DTLS to DTLS+. Compared with the traditional DTLS, DTLS+ reduces power consumption by 40 percent, and is accepted as a standard IETF TLS1.2/TLS1.3 draft. This improvement is security assurance for rapid development of the IoT industry.

Industry-leading operators and device manufactures are promoting security standards for vertical industries, such as the IoV, smart manufacturing, gas, and door locking. Worldwide, vertical industry IoT standards and alliance organizations, such as 5GAA, Industrial Internet Alliance, and National Technical Committee of Auto Standardization, have played roles in the industry.

5.2 Promoting Security During Capability Open-up

IoT industry partners have different security capabilities. Many IoT enterprises in vertical industries are confined to existing security technologies and security protection awareness. Opening up and sharing industry security capabilities will play a major role in improving the security capabilities of industry partners.

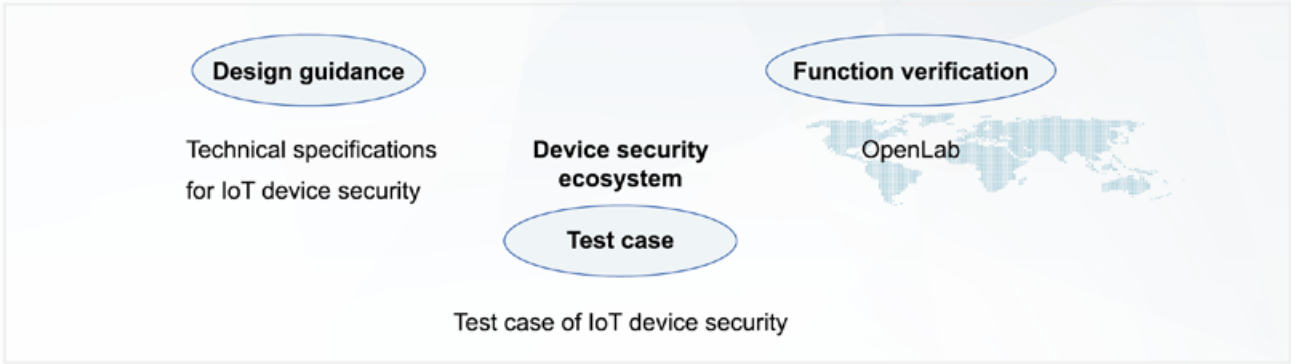
Dedicated to improving the security capability of the IoT industry chain, Huawei shares its solution security capabilities and best practices with IoT partners in different vertical industries through various channels. In addition, Huawei provides IoT solution security design guidance and integration verification services for industry partners, strives to build open and secure IoT ecosystems, and works with industry partners to incubate industries and unleash industry potential.

Based on the security characteristics of vertical industries, Huawei provides scenario-specific solution security design capabilities, develops technical specifications of end-to-end security design and test cases, and provides security enablement and certification services for partners. This is especially important for improving the security capabilities of partners. Specifically, Huawei provides open solution functions, technical proposals for device and application security, security self-check lists, system O&M and device detection tools, O&M guidelines, and one-stop IoT security verification services.

The IoT cloud platform helps apply the practices of Huawei partners to the live network by means of various clouds. Huawei's three-level certification initiatives help foster partners' products. Level 1 and level 2 are device compatibility and application-enabling certifications, respectively. Level 3 is validated certification in terms of industry functions, performance, security, reliability, and maintainability on the basis of the other two levels.

For example, in LPWA scenarios, the opening up and sharing of security capabilities is typically involved in smart gas meters, smart locks, the Internet of Cows, smoke detectors, parking, bicycle sharing, water meters, trackers, mail boxes, and electricity meters. Huawei has worked with dozens of industry partners to jointly innovate solutions and build end-to-end solution security capabilities.

Figure 5-2 Device security ecosystem



5.3 Building Security in Alliances

Building industry alliances is an important part of the IoT ecosystem. IoT security is possible through joint efforts of all stakeholders, including IoT enterprises, industry associations, research institutes, standards organizations, and governments. Building alliances is an effective way of promoting the development of IoT security standards, best practices, policy enacting, joint innovation, and open labs, thereby advancing IoT security.

There are two types of IoT security alliances. One is the vertical industry security alliance, and the other is the dedicated IoT security alliance. Members of the vertical industry security alliance come from IoT vendors, such as the Industrial Internet Alliance (AII), China ITS Industry Alliance (C-ITS), and Mobile Internet of Things Alliance (MIoTA). The vertical industry security alliance promotes IoT security in smart manufacturing, IoV, LPWA-based mobile IoT, and other industries. Members of the dedicated IoT security alliance come from professional security companies, which develop general IoT security white papers, security frameworks, and best security practices.

As a leading enterprise in the IoT industry, Huawei works with the security alliances in multiple IoT market segments to promote the development of IoT security best practices and standards.

With the MIoTA, alliance members partner with the MIIT, CAICT, CTTL, major ICT vendors, and leading vertical industry enterprises (gas, street light, and firefighting) to develop MIoTA IoT security specifications and IoT security pilots (such as Smart City metering, street lights, and parking) in Jiangxi, China. (CAICT is short for China Academy of Information and Communications Technology, and CTTL is short for China Telecommunication Technology Labs.)

5.4 Hardening Security in Collaboration

As for IoT security, technical defense often falls behind attacks. When new attack methods or models are emerging, the defense party immediately fixes the vulnerabilities and improves its protection capabilities. Professional security companies are important members in the IoT ecosystem. They work with communications service providers to offer security products and services, handle known and unknown security threats, and ensure user data and service security. They also support IoT security incubation for commercial use, in the hope of accelerating digital transformation in gas, water, the IoV, industrial Internet, and other industries.

Huawei consistently works with leading industry security companies, universities/colleges, and research institutes to promote security technologies, including data security and privacy protection, malicious device detection and isolation, device attack defense, big data security analysis, and identity authentication, to enhance the solution security capability of the IoT industry. Huawei shares security responsibilities and benefits with professional security companies and organizations.

6 Summary

IoT is a combination of multiple technologies and requires an open, cooperative, and win-win security ecosystem. Governments, industries, developers, academic institutions, and industry standards organizations need to cooperate with each other to stimulate business and technology innovations and establish win-win, fair, and sustainable industry ecosystems.

There is little doubt that standards are the most reliable metric, innovation is the best firewall, alliance is the best protection network, and collaboration is the most reliable key. At Huawei, we will continue to innovate technologies, carry out research on cutting-edge IoT security technologies, and address the security requirements of various industries to advance the 3T+1M security architecture and create ongoing value for customers. Together, we will be proactive, share ideas and collaborate, and embrace challenges to work towards a new era with everything perceptible, connected, and intelligent.

HUAWEI TECHNOLOGIES CO., LTD.

Bantian, Longgang District

Shenzhen518129, P. R. China

Tel:+86-755-28780808

www.huawei.com