HUAWEI

Huawei
IoT Security
White Paper 2017

Content

1 Executive Summary

The Internet of Things (IoT) embodies the convergence of the virtual and physical worlds. It is the vital nexus between device-oriented sensor networks and data-oriented applications facilitated by Internet technologies. IoT creates a geographically distributed infrastructure that provides ubiquitous connectivity between sensors used in everyday life. Thus, information related to many different human activities can be captured and conveyed to IoT applications. Those applications then optimize the effectiveness of those activities at the individual, group and social levels, giving the IoT a far-reaching impact on our world.

The hybrid physical-virtual nature of IoT can be perplexing, and it poses a considerable challenge. So does the openness of IoT, which combines information associated with public, private and community entities and activities. This information is assembled and made available to multiple applications, the purpose and use of which is not always known at the time the data is collected.

The introduction of IoT in modern society should align with the priorities of IoT stakeholders, while meeting their security and privacy requirements. The latter are paramount in IoT as they define the security boundaries of an open system combining public, private and community perspectives. Establishing and preserving these security boundaries – for all stakeholders – is the cornerstone of trust in the open world of IoT. To this end, a holistic, comprehensive and thorough approach to IoT security is paramount.

This white paper is a first step in building executive insights for an IoT security agenda. The paper performs the following functions:

- Provides foundational knowledge in IoT security challenges while describing key technologies.
- Presents the IoT security challenges and the key requirements of an effective architectural approach to IoT security.
- Describes best practices in IoT security from a device, network, and platform standpoint.
- Outlines the role of collaboration in IoT security (e.g. in standardization bodies, community initiatives, etc.).
- Lists priorities for an IoT security architecture agenda, setting the pillars for sound architecture work in IoT security. These pillars include priorities for architecture work, priorities for the use of standards, and important ecosystem perspectives.

2 The dawn of the IoT era

True to its name, the Internet of Things (IoT) interconnects the things of our physical world and makes them available to applications. These things use sensors to measure properties of the physical world and actuators to control parts of it. Owing to its potential direct impact on the physical world, security is of paramount importance in IoT.

2.1 Huawei's 3T+1M views on IoT security

IoT devices have frequently limited resources and may be more exposed to attacks by malicious adversaries. An attacker may compromise an IoT device and use it as a platform for launching attacks on other IoT devices. Thus an intrusion to a single IoT device can gradually spread, like an infection, to thousands of IoT devices. A large network of compromised IoT devices can be used to launch attacks against a service or platform that all devices use or rely upon.

IoT security introduces technological challenges at the device, network and platform level. In addition, there is the process challenge of orchestrating the security technologies in an end-to-end manner. For these challenges, 3 key security technologies and 1 process capability are essential:

1. From the device viewpoint: **Configurable device defense capability**
2. From the network viewpoint: **Malicious device detection and isolation**
3. From the platform viewpoint: **Platform and data protection**
4. From the process viewpoint: **Secure operations and management**

In IoT security, all these viewpoints should be addressed. Huawei is supporting providing security capabilities in these areas, and supports its customers in getting the security guarantees they need.

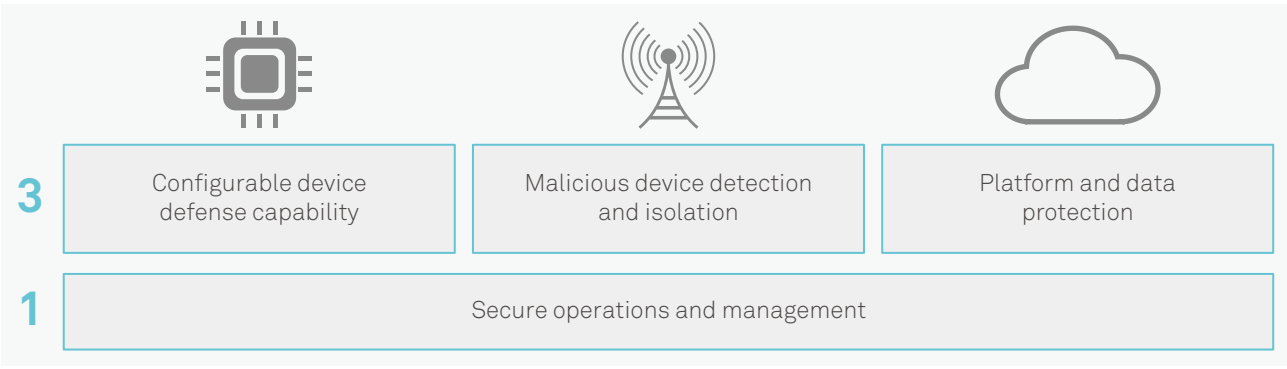


Figure 1. Huawei's "3T+1M" viewpoints on a security architecture.

2.2 The impact of IoT security incidents

On October 20, 2016, a DDoS attack leveraging IoT assets under the Mirai malware's control targeted the Dyn service provider of the Domain Name System (DNS), a critical component of the Internet infrastructure. More than 100,000 IoT assets such as IP cameras, home routers, and other small smart devices were taken over by Mirai in the attack against Dyn[1].

The attack significantly affected Internet service and temporarily took down several high-profile websites (e.g. GitHub, Twitter, Reddit, Netflix, Airbnb, etc.). The Mirai malware was also used in a 20 September 2016 DDoS attack on the Krebs on Security site, reaching 620 Gbps of peak traffic.

The financial cost of IoT security incidents can be considerable[2] and can amount to 13.4% of annual revenues for some organizations.

2.3 Fundamental challenges inherent to IoT

2.3.1 Embedded computing

IoT assets come in small-sized forms and may be embedded within larger-scale assets. For instance, a modern vehicle comes with several sensors embedded in its parts, from its braking system to the air conditioning for the passenger cabin. In addition to being embedded, IoT assets can be mobile, or situated remotely and therefore hard to reach. In addition, IoT assets may have an operating lifespan of 10 or more years. Due to prolonged physical exposure to the elements, IoT devices have a high risk profile. Embedding requirements also constrain the amount of resources available for cryptographic operations and security protocols, thus limiting the security capability of IoT devices.

2.3.2 Device heterogeneity

IoT devices vary significantly in their purpose, form factor, hardware capabilities, and compliance with standards and regulations. For example, IoT devices may operate across a wide variety of industries and scenarios – everything from smart metering to the healthcare or automotive industries. IoT systems must therefore be designed with a huge diversity of devices and services in mind. Having to accommodate a large number of dissimilar device classes runs counter to basic security design principles, which state that, the fewer variations a device must cope with, the more secure it will be. Making the right trade-offs is one of the main challenges in IoT security architecture.

2.3.3 Distribution of entities

Due to its distributed nature, an IoT system comprises several domains that may span different geographical areas (Figure 2).

Applications – This domain hosts applications that need secure access to IoT data, and, optionally, secure control of IoT assets.

Backend – This domain serves as the anchor for the IoT system's security. It is typically hosted in a cloud infrastructure, so it can leverage cloud security capabilities. It comprises the IoT platform that is ultimately in charge of identification, authentication, and policy control.

1.Wikipedia:Mirai, https://en.wikipedia.org/wiki/Mirai_(malware)

2.IoT Business News, "Survey: Nearly Half of U.S. Firms Using Internet of Things Hit By Security Breaches", https://iotbusinessnews.com/2017/06/01/65662-survey-nearly-half-u-s-firms-using-internet-things-hit-security-breaches/

Network – This domain serves as the anchor for the integration of technology infrastructures found in the customer domain through IoT gateways. An IoT gateway shields the IoT platform from the technological heterogeneity of customer systems. It may also act as a local policy point for IoT security (e.g. for enforcing policy rules). An IoT gateway may be a physical device, or, it may be a virtual device (e.g. hosted as service in the cloud infrastructure), depending on the scenario.

Devices – This domain serves as the interface to the physical world through sensors and actuators. Depending on its communication capability, an IoT device may interface directly with the IoT platform, or, through the support of an IoT gateway.

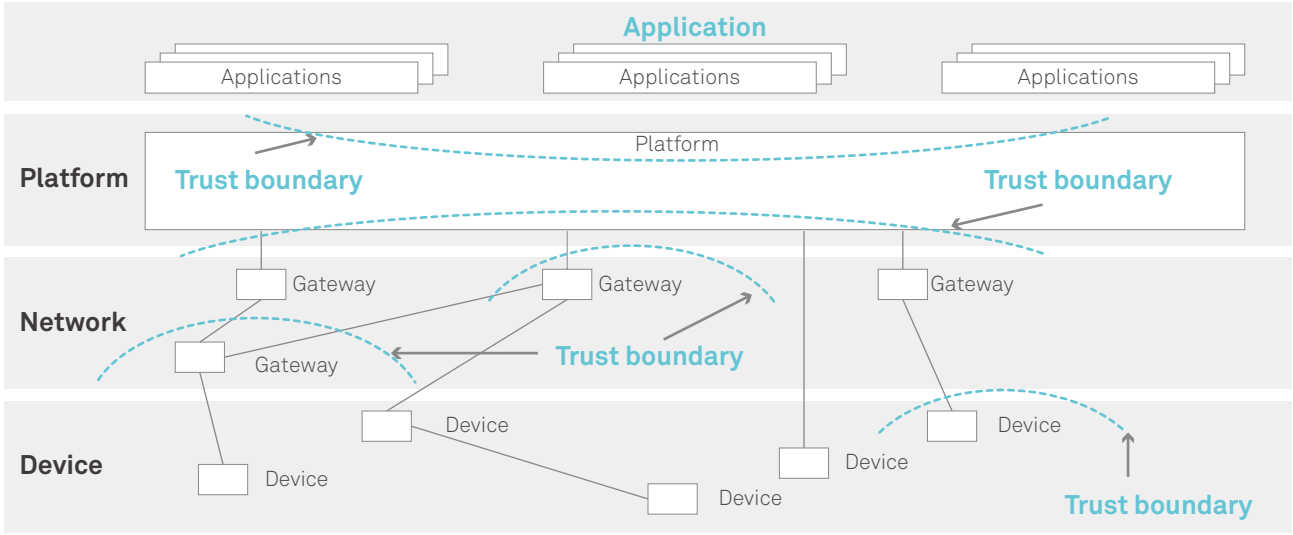


Figure 2. Domains and trust boundaries of IoT.

As shown in Figure 2, these domains and even elements within these domains are separated from each other by trust boundaries (i.e., due to the different risk profiles for physical compromise of their assets). Having devices spread over different locations and geographical regions is a challenge to end-to-end security in IoT, because, in addition to unreliable connectivity, management procedures (e.g. key revocation, etc.) are more complex across trust boundaries.

2.3.4 Authentication and authorization

Due to the higher risk exposure (e.g. to tampering attempts) and the constrained security capability of IoT devices, IoT should always use mutual authentication – that is, all interacting parties should authenticate each other. Because of this heterogeneous and only loosely controlled ecosystem, no single element can assume that the identity declared by any other element is genuine without proper authentication. This can complicate authentication and trust. For instance, for credentials based on certificates and public/private keys, it can be difficult to support certificate and key management (e.g. revocation, etc.) at a scale of billions of devices.

Furthermore, to save resources, IoT devices may have short duty cycles, switching to a power-saving mode when idle. The typical role-based authorization model cannot discriminate between an IoT device that, while in power-saving mode, has been the victim of tampering, and one which has not. Additional information is needed about the state of the device in order to assess its integrity. Therefore, authorization in IoT must react dynamically to the changing contexts in which the devices are used.

2.3.5 Data security

A common practice of securing data for a single purpose is not sufficient in IoT, because the same piece of data may be utilized in multiple use cases. Some use cases have stricter privacy requirements, raising additional security concerns related to data lineage (i.e., the data's origins, what happened to it and where it moved over time) and data provenance. Furthermore, the advancement of data mining capabilities suggests that in IoT, metadata should also be considered for security. For instance, in common practice, the exact details of the physicians visited by an individual (i.e., metadata) will not be part of her GPS track record – the data recorded by her smartphone and accessed by an IoT application. However, a correlation analysis of her movement patterns may reveal that the patient is visiting locations where specific medical services are offered, suggesting an additional piece of knowledge about the state of her health. These possibilities of aggregation present a huge challenge for data security – from the point of collection, to transmission over the network, to data storage.

2.3.6 Flexibility - set of use cases not known in advance

IoT can be a great enabler of multiple domain-specific visions of automation for the human society; visions that are commonly termed "smart" and which share properties of awareness and intelligence. For instance, the vision of Smart Transportation includes use cases that provide a resource-aware transport capability and enable a more efficient end-to-end transport service. Each "Smart" vision comes with multiple use cases, some of which are not even conceived yet, but all of which will include capabilities of awareness and intelligence. On the other hand, IoT security is cutting across domain boundaries and calls for an end-to-end perspective. For instance, the typical home appliances (e.g. refrigerator, oven, microware, etc.) and home controls (e.g. heating, ventilation, etc.) can simultaneously be part of Smart Home use cases as well as Smart Grid use cases. Likewise, a private electric vehicle will be part of Smart Parking, Smart Grid and Smart Vehicle use cases – possibly even at the same time (Figure 3). To ensure correctness of security design, for each IoT asset and use case, the security requirements identified should be cross-checked against those of all other use cases. This means that security in IoT will need a framework for cross-domain coordination.

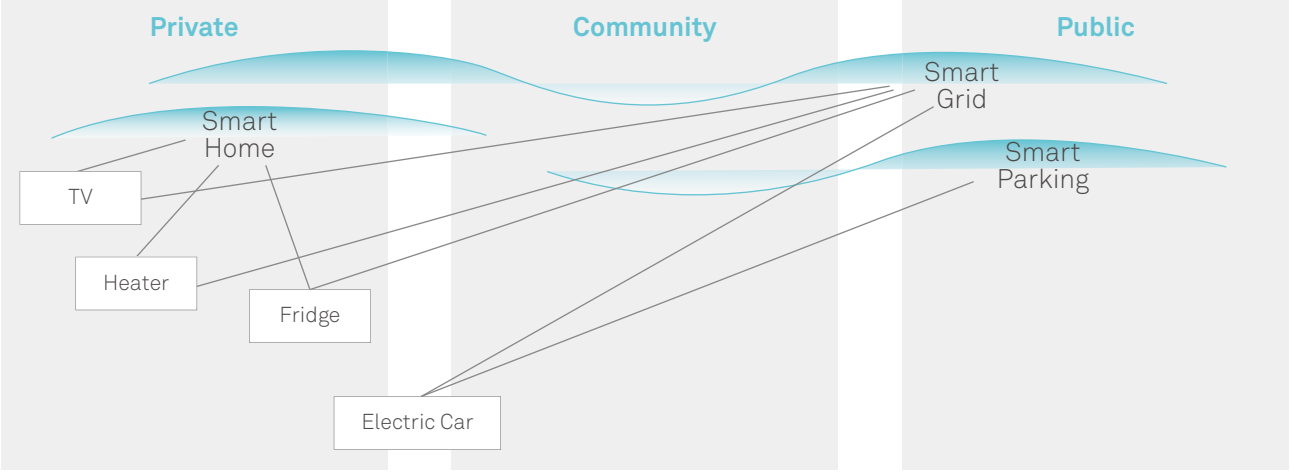


Figure 3. Relative coverage of IoT use cases across domains (illustration of indicative overlap).

When multiple IoT use cases exist, a security breach at one IoT use case can affect other IoT use cases. A breach at a particular layer of IoT offers exploitation opportunities both vertically (i.e., across protocol layers) and laterally (i.e., across adjacent systems). It is impossible to predict all the possibilities about what a compromised IoT asset will be instructed to do by an adversary. Consequently, an important design principle for the IoT security architecture is to have protection measures at multiple levels. In the face of millions of devices requiring action (e.g. smart meter deployments across multiple cities), manual intervention becomes unrealistic. Hence large-scale automation in operations is paramount in IoT security.

2.3.7 Scale of attack

The facts of recent IoT security events highlight the issue of scale in IoT security. The recent DDoS attack on Dyn was the largest ever in terms of peak bandwidth demand – more than 1 Tbps. And yet it involved merely 120,000 or so IoT devices –a tiny fraction of the billions of IoT devices that all market forecasts prescribe. On the defense side, the capacity of most DDoS scrubbing centers does not exceed 8 Tbps. The average peak DDoS attack size is reportedly increasing at a rate of 26% quarterly (i.e., approximately by 100% annually). Given the reported year-on-year increase of 140% on DDoS attacks exceeding 100 Gbps, a response that relies exclusively on increases of the DDoS scrubbing capacity does not seem a realistic approach[3,4]. Additional measures will be necessary and these will require a re-thinking and re-evaluation of our approaches, tools, methods and procedures.

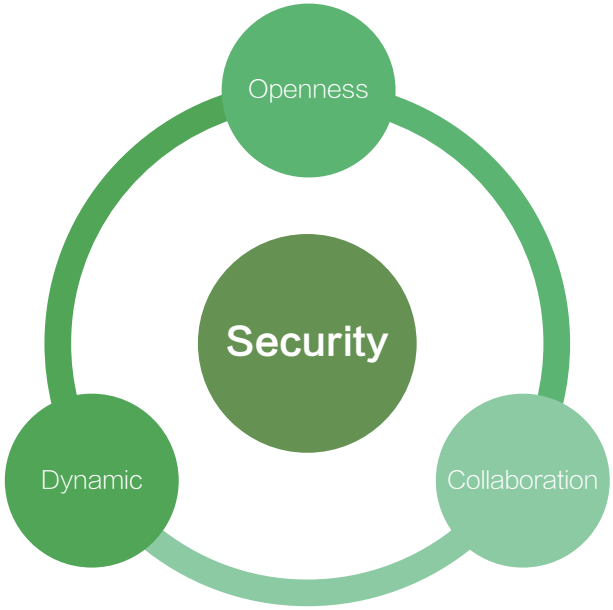
3.Akamai Quarterly Security Reports, 2016 Q4, https://www.akamai.com/us/en/about/our-thinking/state-of-the-internet-report/global-state-of-the-internet-security-ddos-attack-reports.jsp.

4.Verisign DDoS Trends Report, 2016 Q4, http://www.verisign.com/en_US/security-services/ddos-protection/ddos-report/index.xhtml

3 Essential pillars of an IoT security architecture

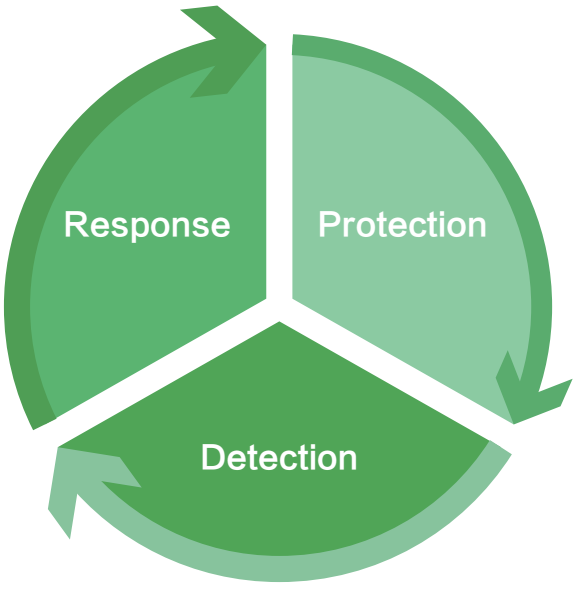
3.1 Vision for security in an open, collaborative and dynamic IoT world

Many IoT systems are open and comprise elements from a multitude of vendors. In many cases, it is this openness and extensibility that brings along a huge value potential for IoT. Platforms, communication networks and gateways, and the multitude of possible devices may come from different vendors. This can pose great challenges to achieve a consistent and coherent secure system for all its use cases. Therefore, it is important to consider the overall system and what we can do to enable a good security baseline and flexible, advanced security capabilities for the best protection of this flexible and open system. There are a multitude of enhancing technologies that can help raise the overall security level, like e.g. common platforms and essential key components for devices, e.g. secure operating systems and robust network elements. These can be leveraged and used by the whole ecosystem to achieve a good base level of security on which individual vendors can build further. Providing these key components and working closely together with our partners benefits the overall industry for more reliable and secure solutions for our customers.



Only through the principles of collaboration and partnership can this vast and complex environment be protected. It requires joint initiatives where partners work together across the whole lifecycle of development, validation, deployment, and operation. Therefore we designed our IoT security strategy as a flexible framework to integrate closely with our partners, enable and empower them and together form complete, flexible and even further extensible end-to-end solutions. Even beyond technology, Huawei is taking steps via our OpenLab program to foster partner collaboration to build and validate complete secure solutions together with our partners and our customers.

As a third aspect, it is important to keep in mind that especially IoT scenarios can be very dynamic. Devices may be added at any times, using a variety of components, vendors and platforms. Some may be less robust than others and we must assume that some components of the IoT ecosystem could be compromised in the future. Therefore we need to design our security measures and controls with this very dynamic and hostile environment in mind. It becomes essential to continuously monitor, evaluate and, if necessary, adapt and evolve the security posture based on metrics of security assurances and risk posture. This takes place through a dynamic security defense strategy with a continuous loop between protection measures, enhanced detection capabilities and security response, all driven by automation. The following chapters explain Huawei's approach to support its vision of IoT security. They share architecture perspectives, discuss key technologies, and identify important best practices.



3.2 Key considerations for IoT security architecture

Because IoT includes so many different use cases, several different designs for an IoT security architectures are possible. However, a disciplined approach to IoT security should be founded on sound principles.

3.2.1 Approach

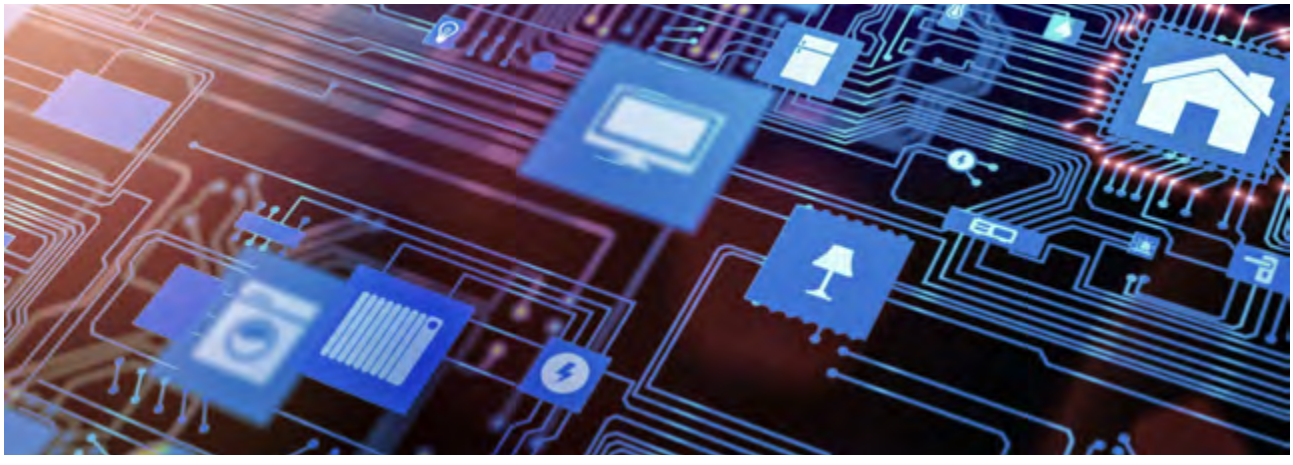
- **Use of standards** – Standards distill security knowledge and expertise from multiple stakeholders and are thus a cost-effective element of architecture design.
- **Best practices** – IoT security should align to and reuse the standard practices in IT security (e.g. multi-layer defense, isolation, least privilege, etc.). This will save effort that should be directed to addressing the security challenges that are inherent to IoT.

3.2.2 Governance

Governance is about having a disciplined approach to the management of the security architecture for IoT. A governed architectural approach supports security priorities by being based on the analysis and modeling of threats.

- **Threat analysis** – In threat analysis, the actions that might negatively affect a system are identified and analyzed, with an emphasis on their probability of occurrence and taking into account their consequences. Therefore, a systematic approach in quantifying the probabilities of security-related events is necessary. In addition, IoT use cases may share devices, data and services, thus calling for a disciplined approach in threat analysis (e.g. in order to address cross-cutting issues).
- **Threat modeling** – Threat modeling is an exercise that identifies the classes of a system's potential attackers and then, for each attacker class, identifies, enumerates and prioritizes potential threats (from the respective attacker's viewpoint). The purpose of threat modeling is to inform system stakeholders (e.g. system developers, system operators, etc.) in key security topics:
  - A systematic analysis of the attacker's profile.
  - A list of the (most) probable attack vectors the attacker may employ.
  - A list of the assets targeted by the attacker.

Unfortunately, in IoT, vendors may not be of the same maturity for secure design and may not use to the same extent threat analysis and threat modeling. For instance, some IoT vendor may lack the security resources or face market factors that force them to prioritize the release of functional features over the engineering of security by design.



3.3 Security architecture blueprint

3.3.1 Business framework

IoT involves multiple stakeholders, e.g. device manufacturers, service providers, network operators and application developers. To ensure IoT security is not ignored, overlooked, or improperly addressed, the collaboration between IoT stakeholders should follow a business framework that includes also a security viewpoint. Establishing governance and auditing for the IoT security architecture enables security topics to be addressed in a controlled manner across the lifecycle of IoT assets (Figure 4):

- During production (design, development, testing, certification, etc.) for overall management and governance of risk injection across the entire chain of supply and production. Instruments from the standard IT security practices can be reused in the production phase of IoT assets according to their risk profile.

- During operation (enrollment, update, etc.) for overall management and governance or risk exposure through the application of software updates and vulnerability patches. These activities include the validation of security measures in deployment (e.g. via penetration testing) and assessments of the organization's ability to provide appropriate responses to security incidents (e.g. CERT programs).
- In the sunset phase (e.g. for monitoring risk exposure, etc.)

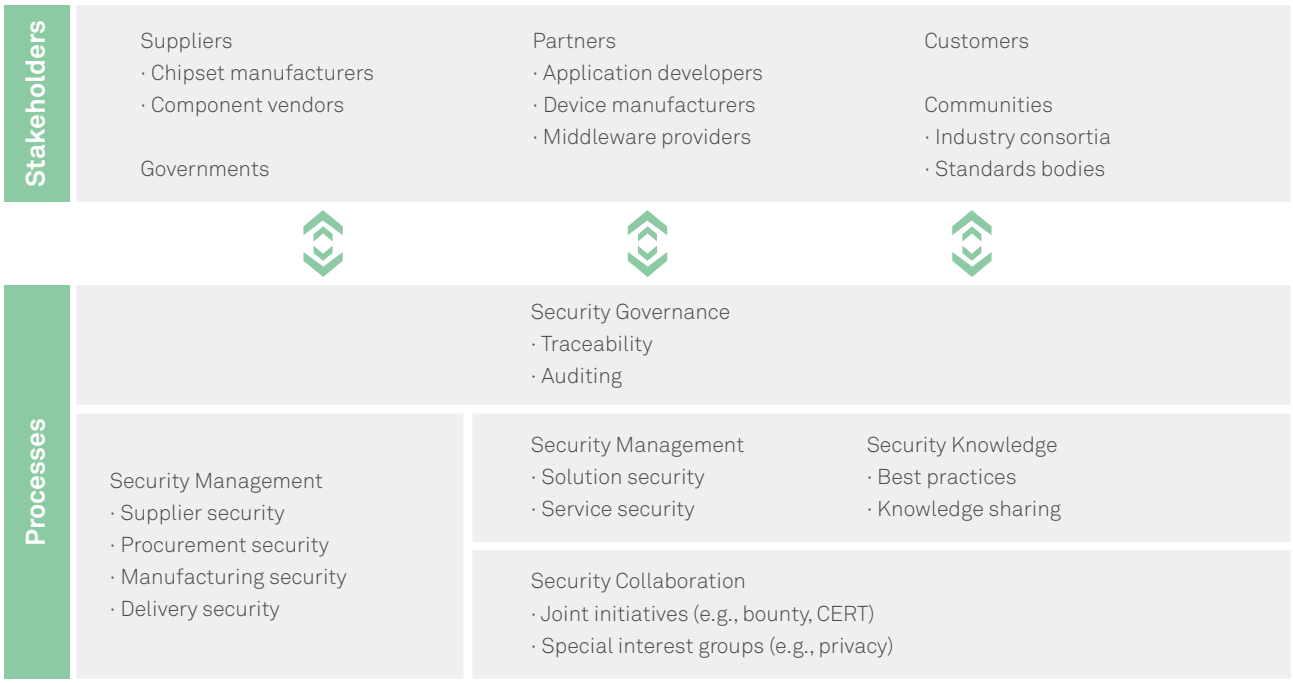


Figure 4. The IoT security business architecture

Governance provides a **controlling oversight of IoT security across all processes, stakeholders and lifecycle phases of an IoT asset.** Auditing enables compliance and certification for IoT security matters (e.g. processes, assets, etc.).

3.3.2 Threat categories

The design of an IoT security architecture needs to provide security capabilities to address the following threat categories:

- **Corruption of system integrity:** If some system components are tampered with, the system cannot function as designed. A typical method of corrupting system integrity is the injection of malware in the system, causing persistent threat to system security.
- **System intrusion:** An attacker breaks through the border protection and identity authentication mechanisms to intrude into the system by exploiting system vulnerabilities or using other attack means. Then, the attacker maliciously uses system resources, corrupts system data or processes, or steals important system data.
- **Malicious privilege abuse:** Users or processes exploit system vulnerabilities to launch attacks such as privilege escalation attacks to obtain unauthorized access privileges. The resulting privilege abuse causes serious threats to system security.
- **Threats to data security:** There are threats to data integrity, confidentiality, and availability as well as threats to privacy information (disclosure or unauthorized use).
- **Service interruption caused by network service attacks:** An attacker compromises the system's ability to provide network services. As a result, network services may degrade in performance or become entirely unavailable.

3.3.3 The security architecture "3T+1M" model

IoT threats target different parts of the IoT infrastructure, from the device to the cloud platform. Focusing on the parts of the IoT infrastructure exposed to threats, Huawei is providing security capabilities, such as the operating system for IoT devices. Huawei IoT security solutions cover the following parts:

1. The IoT Device (e.g. sensor, actuator, etc.) domain that provides instruments to sense and control the physical world.
2. The IoT Network domain that collects and processes sensor data using the communication technology that is applicable in the field (e.g. NFC, IEEE 802.15.4, ModBus, etc.) while also connecting to the IoT Platform layer described below. IoT Gateways in the Network domain can act as local policy enforcement points. The underlying network (e.g. cellular mobile network) provides services for the secure exchange of data across these domains and for the protection from attacks.
3. The IoT Platform domain that provides services for connection management, data management and operations support.
4. Secure operations and management – These include secure operation and support for routine IoT security evaluation, security reporting, and automatic identification of security events using best practice policies.

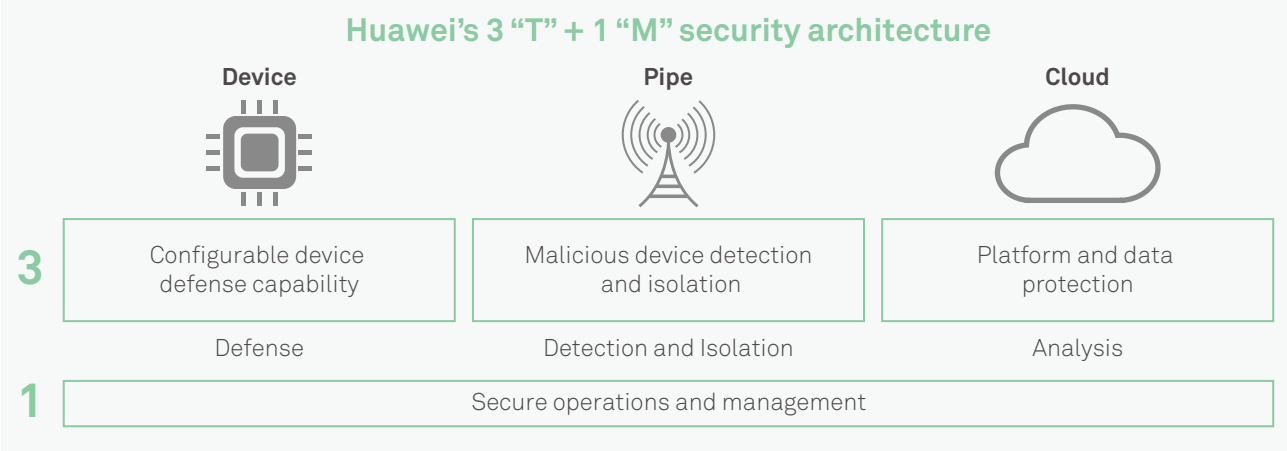


Figure 5 The Huawei IoT security architecture.

To address these threats, the Huawei IoT "3 **T** (Technology) + 1 **M** (Management)" security architecture (Figure 5) includes horizontal security capabilities across its device, network and platform parts, including its data. It also includes operational support for end-to-end security management (e.g. security updates).

Configurable device defense capability – IoT devices typically have basic security capabilities for basic authentication and encrypted transmission. Some IoT devices will need additional capabilities for advanced security (e.g. intrusion prevention and/or detection, support for remote security management, etc.). Huawei's LiteOS provides advanced security capabilities. This is the 1st level of defense against attacks.

- IoT devices should have defense capabilities. IoT devices with limited resources (memory, storage, and CPU resources) provide basic security capabilities; industrial control devices provide X.509 authentication and signature security; and key service devices provide advanced security capabilities.
- Basic security means that the IoT devices must have basic authentication and encrypted transmission capabilities. Advanced security means that IoT devices provide reliability and intrusion prevention capabilities and support remote security management. LiteOS can be deployed to provide advanced security capabilities. In addition, Huawei provides device black-box testing tools and device design guideline.

Malicious device detection and isolation – The network side provides capabilities for monitoring communication behavior and detecting and isolating malicious IoT devices. In a Narrow Band IoT (NB-IoT) device setting, for example, network services provide secure transmission of data and security protection for the IoT platform (i.e., including its physical and virtual infrastructure). The network also provides protocol identification and filtering services with black-list and/or white-list policing. Security services at IoT gateways include secure transmission of data, protocol identification, and intrusion detection. This is the 2nd level of defense against attacks.

Platform and data protection – Protection services of the cloud infrastructure include a Distributed Firewall (DFW), VSG and a Web Application Firewall (WAF) embedded within the hypervisor. The (cloud-hosted) IoT platform offers data protection security capabilities, e.g. isolation of tenant data, data privacy protection, data lifecycle management, security authorization for the data API, and so on. These security capabilities ensure data privacy to comply with European Union (EU) data privacy regulations. In addition, a learning and analysis system based on Big Data technologies analyzes the behavior of IoT assets to detect and isolate persistent threats. This is the 3rd level of defense against attacks.

Secure operations and management (O&M) – These include support for routine IoT security evaluation, security reporting, and automatic identification of security events using best practice policies. They enable awareness of the security posture while providing security guidance and supporting toolsets (e.g. remote device management, secure software management, antivirus, etc.). This level of defense supports standard operating procedures (SOP).

3.3.4 Configurable device defense capability

Physical attack has been a traditionally popular way to compromise an asset. In a network setting (e.g. IoT), the vulnerability of a device becomes a weakness of the entire network. Network attacks in IoT can have severe consequences that include loss of brand credibility, asset damage (e.g. where hackers take control of a vehicle), or even life-threatening situations (e.g. in Smart Health use cases). To this end, Huawei provides holistic protection capabilities for IoT devices (Figure 6):

- The security core provides fundamental security capabilities (e.g. secure boot leveraging chipset security and functions for secure data storage).
- The protocol core provides security for communication protocols (e.g. 3GPP AKA authentication and Anti-DoS capability).
- The application core provides end-to-end session security (e.g. based on DTLS/PSK), particularly for IoT devices which, to save power, can have a prolonged sleep phase.

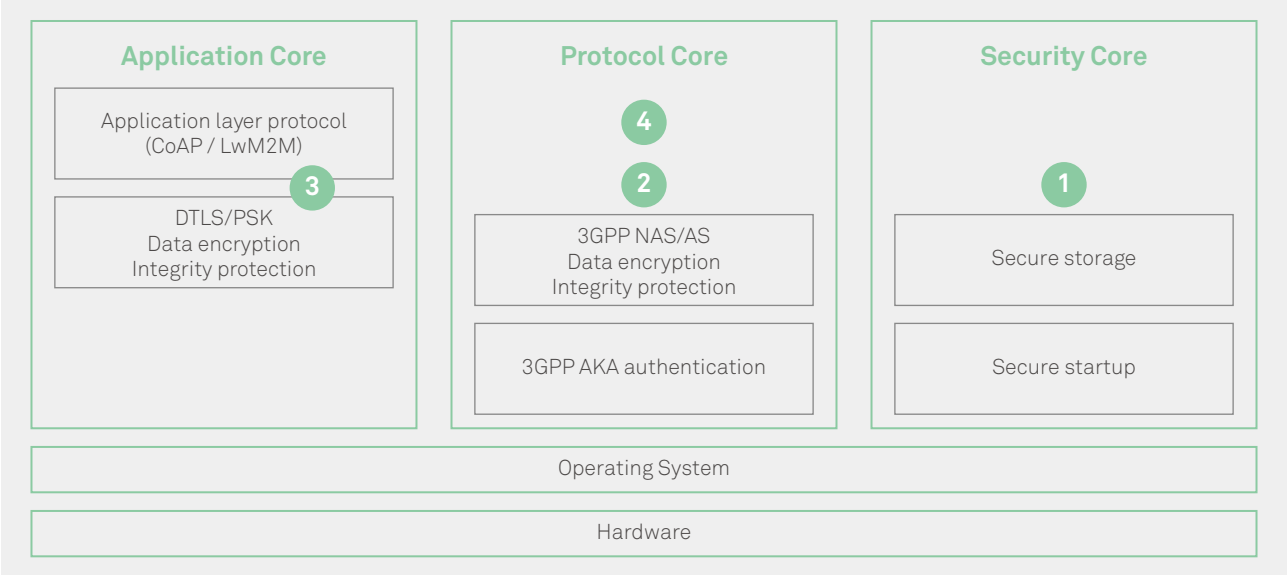


Figure 6 Device security capabilities.

The security core, protocol core, and application core must be isolated from each other. Hence an important security capability of the Operating System (OS) is to isolate applications from each other and from the kernel. A secure OS separates kernel memory from application memory. Through the syscall() mechanism, privileges in kernel and user mode are kept separate and virtual machines are used to protect the privileges of different apps. This provides applications with configurable memory protection interfaces based on the memory protection unit (MPU) or the memory management unit (MMU). Security protection measures (as shown in Figure 7) include proper memory layout, memory protection, distinction between kernel mode and user mode, and process isolation for applications. Major features of the isolation mechanism of the secure OS are:

- Access control – Through control and management of sandbox isolation and of the access channels' setup, unauthorized access (e.g. by malicious code) is prevented.
- Security kernel – Provides the foundation for secure firmware upgrade, (e.g. when downloading and updating the firmware over the air), security storage, key management, encryption and decryption functions, and device identity.

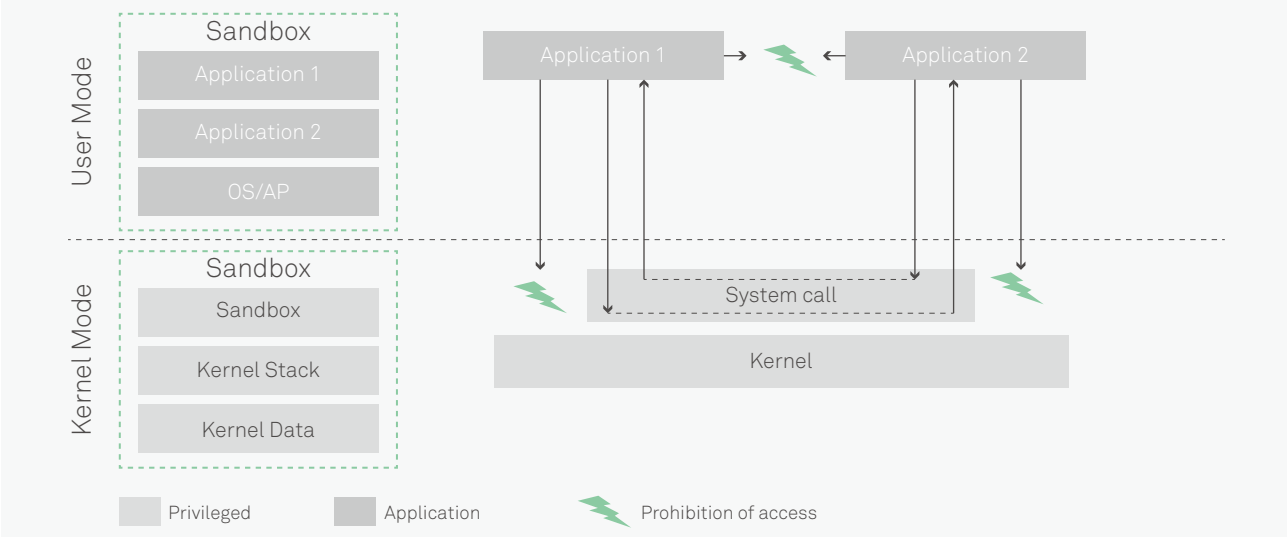


Figure 7 Device security protection measures.

To be reliable, a secure OS requires a tamper-proof hardware platform. A secure OS also supports secure operations and management via common monitoring agents (e.g. antivirus, etc.) and functions for secure software management (e.g. for the application of security patches).

3.3.5 Malicious device detection and isolation

The network layer is responsible for access and transmission. There are many forms of access, such as wireless short-distance access, which includes Wi-Fi, ZigBee, Bluetooth, and infrared; wireless long-distance access, which is found in mobile communications networks; and wired network access. The network layer includes the core network, usually an IP network, and is also the transmission layer for IoT information and data. Data collected on the device layer is transmitted over the network layer to the application layer for processing.

Main security threats facing the network layer:

- In IoT, if data transmissions are unencrypted or if integrity verification is not performed, communication can be easily eavesdropped or tampered with.
- Particular IoT protocols may have flaws in their authentication methods, thus allowing access to malicious users.
- DDoS attacks

Main countermeasures used in ensuring communications security on the network layer are:

- Encrypting and authenticating communications between devices and remote systems.
- Controlling data flows using white-list and black-list policies.
- Reinforcing weaknesses or flaws in particular protocols.
- Isolating network segments.

The security mechanisms that build network security include:

1. Authentication – Using mutual authentication based on certificates and allowing communication only to white-listed devices.
2. Lightweight encryption – Using lightweight algorithm libraries in IoT devices and IoT gateways, to reduce consumption of memory and storage.

3. Secure tunnel – VPN technologies (e.g. TLS, IPSec) can be used to encrypt and verify the integrity of communication.
4. Firewalls – Identify and analyze IoT protocols and handle attack traffic. Firewalls can also support the prevention of flood and scan attacks.
5. Anomaly detection – Protocols are analyzed to detect abnormal behavior. Behavior patterns and data relevance and coordination are also analyzed to detect intrusions.

3.3.6 Platform and data protection

Access and Management Security of IoT Devices

As a minimum, IoT assets (i.e., devices, gateways) require secure access to the IoT platform. For each IoT device, unique identifiers and authentication credentials are preset during manufacturing. Authentication credentials can be based on shared keys, digital certificates, or other technical solutions. These must be protected from tampering (e.g. unauthorized copying of private key) to ensure each IoT asset is correctly identified. For the confidentiality and integrity of the data transmitted between IoT assets and the IoT cloud platform, standard protocols for secure transmission (e.g. TLS, DTLS) should be used. However, in some use cases, the resource constraints of IoT devices may prohibit the use of standard security protocols.

Personal Data and Privacy Protection

Data collected by IoT assets and transmitted to the IoT cloud platform may be subject to privacy concerns (e.g. the EU GDPR rules). Depending on the use case and according to the least authorization principle, an explicit personal data and privacy statement and user authorization might be required. Data owners have the right to revoke their authorization at any time.

Sensitive data must be encrypted while in storage and data owners should be able to define the data retention period. After the retention period expires, data can be deleted in a timely manner.

4 IoT security practices

4.1 Device design practices

Best practices in information technology security can address the challenges of IoT security. It is important to include security concerns in each stage of the IoT service lifecycle, from design to deployment and operation. Risk assessment, threat analysis, and impact analysis, carried out on a use case basis, will inform decision making in security design. This is because use case requirements largely define the restrictions imposed on IoT devices, e.g. processing capacity, storage limitations, and energy consumption. Cost considerations can drive design decisions that irreversibly undercut an IoT device's security capability. Therefore, the IoT device security design needs to consider its corresponding abilities to match with appropriate defense, such as processing capacity, memory resources, cost, power, role, etc. Huawei will provide "IoT Terminal Security Design Specification" to our partners for corresponding terminal security design guide, based on the following principles:

Weak Devices – Needs to accord with basic security level, taking into account the processing capability and cost, such as DTLS/+, two-way authentication, password management, remote update. This kind of terminals have limited processing capacity, constrained memory resources, and are cost and power sensitive. Typical categories include gas/water/electrical metering, smart parking devices, pets tracking devices, agricultural sensors, etc.

Strong Devices / Gateway – Needs to accord with enhanced security level, in addition to the basic security requirements. It can provide enhanced security capabilities, such as safe startup, system reinforcement, TPM/TEE, virus protection, port reinforcement, etc. This kind of terminal has a larger processing capacity, often with an embedded operating system, and the role in IoT network is usually important in defending against attacks. Typical categories include car networking terminals, home IoT gateway, industrial control gateway, camera, interactive terminals, etc.

Based on the Huawei IoT Terminal Security Design Specification, the terminal device security design should focus on the following aspects:

- Transmission security – Focuses on transmission protocols protection, including DTLS/+, PSK, protocol anti-attack, transmission encryption, etc.
- Physical security – Depending on the use case, water proofing, dust proofing, heat dispassion, electromagnetic interference, location and physical damage or destruction may have to be considered.
- Data security – Provides confidentiality, integrity, and availability of data at rest, in memory and in transit.
- System security – Address identification and authentication, access control, auditing, secure software update (including firmware), software security, vulnerability scanning, security startup, secure storage and interface security.
- Access security – Address security safeguards at the network level, including access authentication, access control, defense measures, exception control and isolation.

- Log protection – Realizes IoT device log recording, log auditing protection, including log protection, security events alert, sensitive information updating record, audit record, etc.
- Application security –Includes application authentication, application sensitive data access authentication, interoperation authority management, access authority control, etc.
- Privacy protection – Protects the IoT personal data or sensitive data, to accord with the privacy compliance requirements of all countries and industries, and applies the mechanism of data destruction and encrypted storage on these IoT devices.

Besides providing Huawei IoT Terminal Security Design Specification, Huawei will also help our IoT partner to build IoT device defense capability based on IoT chipset security and on the LiteOS operating system libraries. For instance, Huawei NB-IoT chipset Boudica can provide the basis security capabilities of DTLS/+, FOTA, two-way authentication, etc.

4.2 Security practices in verification and testing

After an IoT device is built and the applicable security practices have been implemented, the security cycle should move to verification and testing, to address:

- Hardware review and tests for manipulation
- Network traffic analysis
- Interface security analysis
- Verification of authentication and weaknesses in default configuration
- Service and input testing to check the defense against DoS and fuzzing attacks
- Verification of the backup and recovery procedures in real scenarios
- Updating mechanism and integrity verification testing for firmware and software
- Regulatory compliance within operation environments

While compliance to security standards is important for device-level security, collaboration with partners in joint initiatives is the best practice in verification and testing for IoT. In alignment to security standards, Huawei has been following 3GPP and GSMA security specifications. As a leader in industry solutions, Huawei is also working with partners in vertical industries to develop a series of specifications to ensure security across the IoT ecosystem, and providing IoT solutions security testing and verification for partners through OpenLab. OpenLab is an open lab offered by Huawei to enable end-to-end IoT system integration and verification for partners. To verify whether relevant security standards and specifications have been properly applied in the design and R&D phases, Huawei tests the security capabilities of individual IoT products in its OpenLab. Huawei's OpenLab can simulate an actual IoT environment in full detail. It has been used jointly with partners for the technical verification of several IoT use cases (e.g. Smart Metering, Smart Water, etc.). It also supports IoT security testing and verification by simulating common attacks in IoT (e.g. physical attacks, DDoS attacks, etc.). To help partners build appropriate defense capabilities of IoT terminals, and construct a healthy IoT security ecosystem, Huawei OpenLab will also provide partners with IoT black-box testing and verification services for terminals.

4.3 Privacy protection practices

Privacy and Data Protection

IoT massive data and privacy protection focuses on the IoT platform. Different IoT applications will have different privacy requirements. The Huawei IoT platform supports the customization of the privacy policy for applications, according to application scenarios. For instance, the privacy requirements of a Smart Home application will be different from those of a Smart Metering application, and proper privacy control measures must be in place.

4.4 Secure operation and maintenance practices

In order to solve all security issues in O&M and meet related requirements, Huawei has developed an E2E secure O&M solution to comprehensively ensure the security in network O&M. The solution focuses on building security capabilities in manual O&M, basic O&M, and cloud-based intelligent O&M (Figure 8).

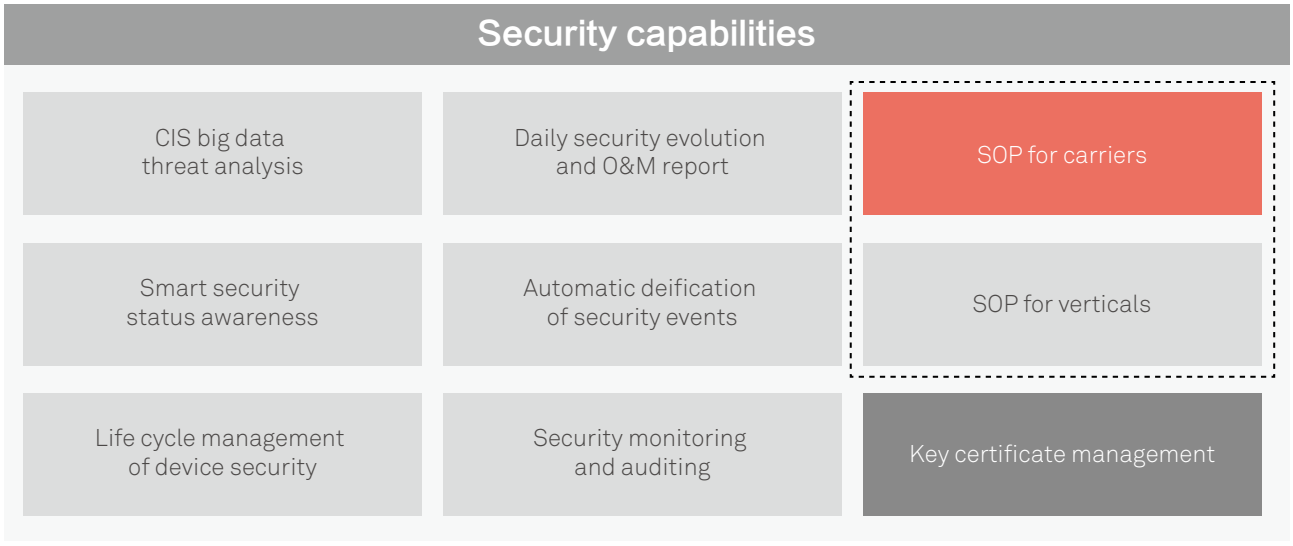


Figure 8 Huawei security framework for O&M.

Practices of ensuring secure O&M are mainly reflected in the following three aspects.

Develop an E2E standard operating procedure (SOP) for O&M personnel

A key element of secure O&M is people. It is important to apply an E2E SOP for O&M personnel to ensure the security in daily IoT O&M. The SOP ensures the security of all IoT applications of different industries, including operators, and a variety of vertical industries (e.g. connected cars, metering, logistics, manufacturing, etc.). Each industry needs to customize the SOP to align it with its needs. The SOP should include multiple end-to-end processes, including device authentication, network installation and delivery, on-site O&M, back-office support, customized application development, and security guarantee in an emergency.

Build basic capabilities for secure O&M on the system side

1. Security of remote configuration

- Two-way secure authentication at access gateways.
- Unique embedded security token or embedded certificates and private keys for authentication with the IoT secure O&M center.
- Gateway-based active registration and passive queries for controlled perception scope.
- Independent TLS or gateway proxy TLS for tunnel security of network connections.
- Over-the-Air (OTA) updates provide real-time update of all things/gateways at any location and automatic rollback if update fails.
- Rule-based engine supports complex and flexible tasks, with fine control over time, location, and event.
- Remote diagnosis and commissioning, including remote rebooting and factory reset.
- Status reporting and querying.
- Secure booting, trusted computing, and remote attestation.
- Logs can be sent to the cloud for review.

2. Authorized software downloads

- Remote attestation by use of integrity verification of downloaded software.
- Whitelist of digital certificates for running software.
- Authentication and whitelist of download center.

3. Authentication of administrators

- Role-based access control (RBAC) with domain-specific permission management.
- Single Sign-On (SSO) for unified authentication.
- Multiple-CA authentication center.
- Role-based verification of certificates.

4. Unified security platform

- Unified IoT security O&M center.
- Customized access policy for individual security keys.
- Analysis of streaming data, unified service dashboard, and estimated residual service life.
- Devices are registered, providing information on how devices are running across the entire network for lifecycle management.
- Security status awareness enables real-time monitoring on the entire network and infrastructure analysis to identify abnormal problems.
- Log review, with regular review of device logs to identify any abnormal problems.

Build intelligent security status awareness and threat analysis capabilities on the cloud

The key to IoT security lies in devices and platforms. The security capabilities of cloud platforms are crucial to secure O&M and ensure security management throughout the IoT system. Building a robust security status awareness and threat analysis on the cloud is crucial to end-to-end security of the IoT system. Those security warning and testing capabilities include CIS big data threat analysis, daily security evolution and O&M report, automatic security status awareness, identification of secure practices, lifecycle management of device security, and security monitoring and auditing.

4.5 Select use cases

4.5.1 Smart Water Metering

With the development of IoT smart water meter technologies and the application of NB-IoT, the water system industry is shifting from manual meter reading to remote intelligent meter reading. Through automatic meter reading, water companies are becoming smarter in water management. Smart water meter is characterized by limited computing power (single-chip microcomputer is usually installed), low power budget (it is required that the battery can supply power for more than six years), and vulnerable metrological data. Therefore, to ensure IoT security, we should guarantee the security of data transmission in the network, prioritize lightweight security protocols and algorithms, and consider their impact on the device's power consumption.

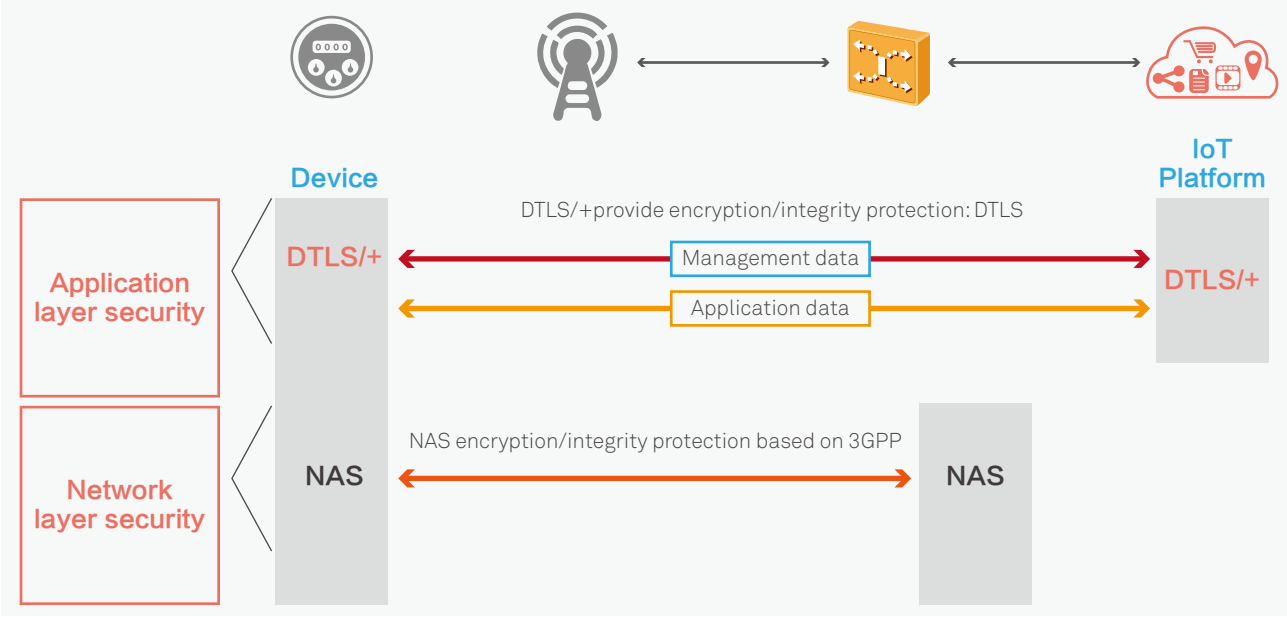


Figure 9 Huawei E2E NB-IoT security framework for Smart metering.

Huawei has proposed a NB-IoT-enabled Smart Water Metering solution, specific to the smart water meter industry. As for network layer security, all user data are sent through the non-access stratum (NAS), and encryption/integrity protection is guaranteed for IoT devices and core network based on 3GPP. As for application layer security, encryption/integrity protection for data between IoT devices and IoT platforms/application servers is ensured through Datagram Transport Layer Security (DTLS). To meet the water meter industry's special needs, Huawei has simplified the DTLS protocol regarding power consumption and protocol processing, to make it better align with the industry's capabilities and requests. Details about the implementation of the solution are as follows:

- The 3GPP Authentication and Key Agreement (AKA) protocol is adopted for the device to access the Evolved Packet Core (EPC), to ensure legal device accessing legal network.
- Secure channels such as NAS and Access Stratum (AS) are built between the device and core network, based on 3GPP.
- A secure channel is built between the Radio Access Network (RAN) and the EPC, based on Internet Protocol Security (IPsec).
- A data security channel is built at the data transmission layer between the water meter and IoT platform, based on DTLS/DTLS+.
- A secure transmission channel is established between the IoT platform and the water meter application, using the HTTPS protocol.

4.5.2 Safe City

A safe city refers to the use of IT and IoT by municipal capabilities for public security for traditional threats or digital threats. Cyber security is one of the top focus areas of safe city development. Thousands of sensors in various types – such as smart cameras, alarms, and mobile devices – are deployed in a safe city. Importance should be placed on the security of these sensors, apart from the security of traditional networks, in a safe city. IP cameras are deployed in various complex conditions. Historically, most confidentiality disclosures in the domain of public security have been caused by human error attributed to the internal staff of involved organizations.

Therefore, the new challenges relating to cyber security in building a safe city are as follows:

- IP cameras and other key IoT devices can be easier to counterfeit and hijack. Thus videos and data can be stolen or tampered with, leading to user privacy leakage and the destruction of valuable information (e.g. evidence data for traffic accidents).
- Hackers can use an IP camera or other IoT device as a springboard to attack the network, and destroy, steal, or tamper the data it relies upon to provide its services.
- IP cameras and other IoT devices are vulnerable. It is difficult to restore them to normal operation after they have been compromised and used to mount DDoS attacks.
- Compliance to international security operations standards (e.g. NG911, ISO27001).

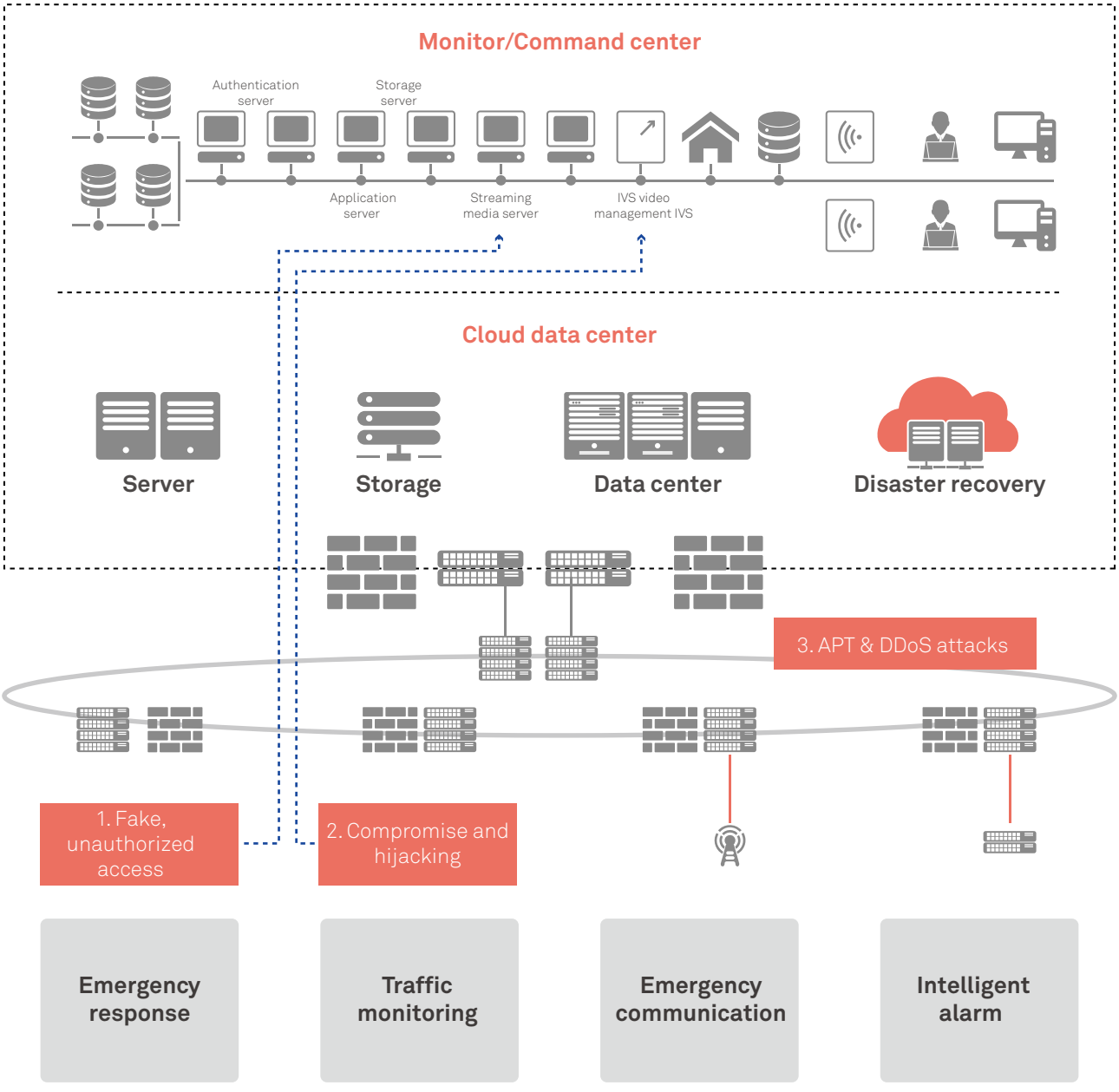


Figure 10 Threats in a Safe City environment.

To address the security challenges of a safe city, we need security solutions that enable elements in the network to collaboratively respond to security threats in the following areas:

- Secure network access: security authentication and encryption for cameras and mobile devices
- Intrusion and C&C detection: The Intrusion Prevention System (IPS) can be used to identify vulnerabilities in the network of the video system. It can also prevent network attacks and support Netflow and C&C detection.
- Internal violation analysis: Identify internal violations based on log information from the Identity and Access Management (IAM) service or through bastion hosts.
- Central management and analysis of all logs of the entire network: The logs of security systems (FW, IPS/IDS, DDoS, cameras, IAM, UMA, and WAF) are collected in a central location. Log analysis can then identify screen false attacks and focus on valid attacks.
- Presentation and linkage: Present all types of threats in the entire network, cameras and handheld devices which are frequently attacked, TDoS attacks, and intercepted and isolated threats.

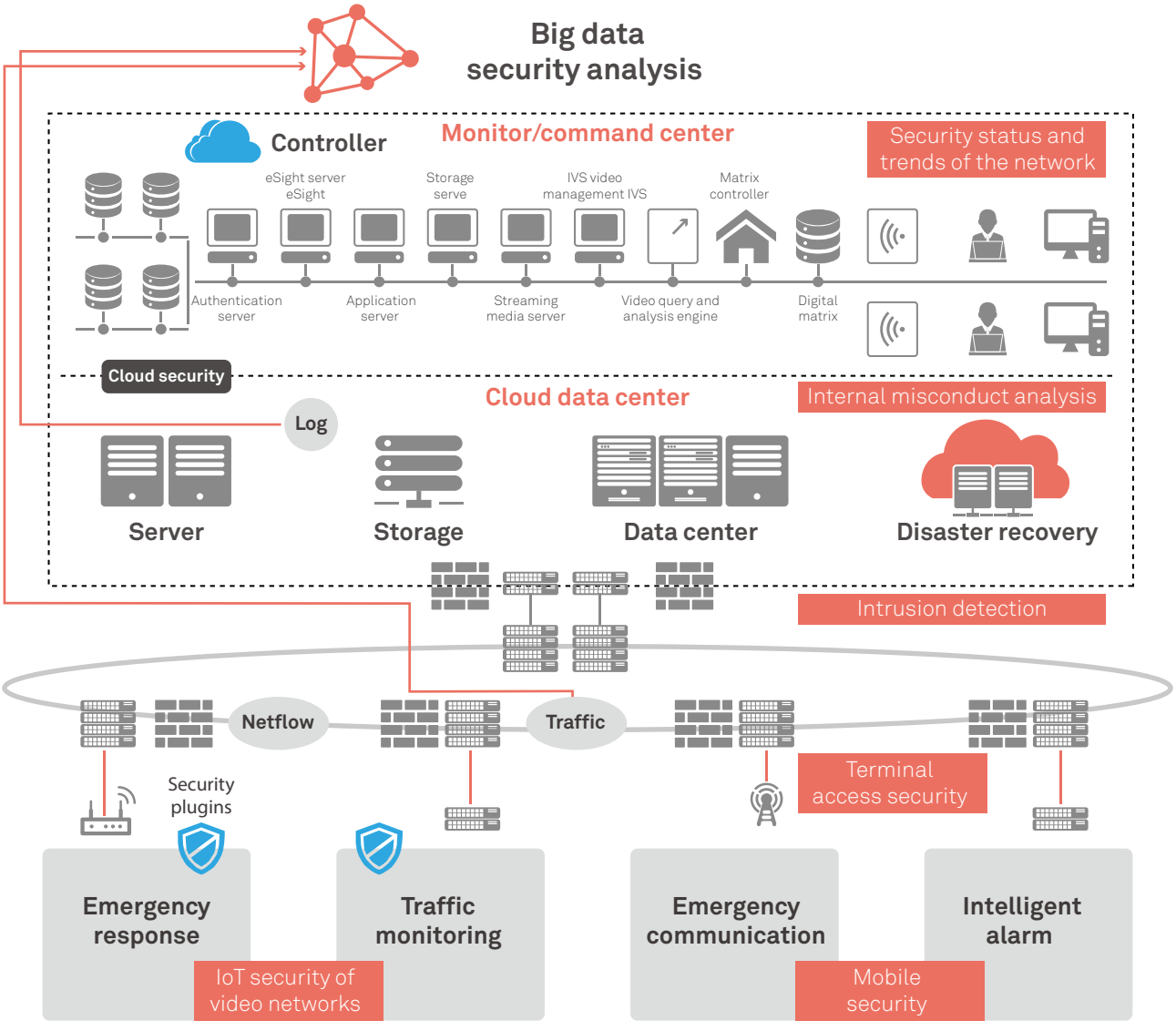


Figure 11 Elements of IoT security in a Safe City environment.

5 Ecosystem perspectives of IoT security

5.1 The importance of the ecosystem

Probably nowhere else is more potential to address the challenges of IoT security found, than through the ecosystem. IoT is by its nature a platform proposition where innovation is enabled and incentivized and the economic benefits of market offerings are shared among collaborating stakeholders (e.g. application developer, platform operator, network service provider, device manufacturer, etc.). The sharing – to varying extents – of responsibility suggests that no stakeholder can successfully resolve IoT security issues alone. Instead, all parties in the ecosystem must invest in cooperation, collaboration and mutual support through joint initiatives that target IoT security issues.

Through its Open Lab program, Huawei is supporting development of the IoT security ecosystem. Globally distributed but sourcing local expertise, OpenLab is enabling joint innovation and solution launches with more than 400 partners in IoT verticals[5], including activities like:

- Collaborating with partners to develop solutions and innovation capacity for industries, expanding the market, and sharing the benefits.
- Building regional innovation centers, partner development centers, solution development centers, and industry experience centers.
- Collaborating openly with industry partners to digitally restructure traditional industries, and power the new industrial revolution.

Partners have publicly acknowledged the benefits they get from the OpenLab program, e.g. in terms of faster testing for IoT components[6]. IoT security aspects of OpenLab include support components (e.g. black-box testing, penetration testing, etc.), integration support, and partner qualification (e.g. in terms of product compatibility, product validation, and product enablement).

Huawei takes action to enables industry stakeholders, developer communities, academic institutions, and standards organizations to work closely to accelerate innovation in IoT. Huawei welcomes a healthy ecosystem that, through openness and transparency, promotes cooperation under a fair competition regime.

5. Huawei announces OpenLab program, http://www.huawei.com/en/news/2017/3/Huawei-Launches-Global-OpenLab-Program.
6. Huawei update on OpenLab, http://www.vodafone.com/business/blog/iot/impressive-start-for-nb-iot-open-labs.

5.2 The role of joint initiatives

Joint initiatives are another important element of the ecosystem perspective on IoT security. Through collaboration, joint initiatives foster knowledge sharing on IoT security and promote the alignment of stakeholders' interests. This creates and propagates awareness of key security issues and builds mutual trust among stakeholders. An open dialogue on IoT security promotes synergies in addressing IoT security challenges through the development of common projects that advance our collective capability on IoT security.

5.3 Security agencies and standards bodies

Standardization efforts also contribute to the security of the IoT ecosystem. The most relevant bodies are:

- National Institute of Standards and Technology (NIST), supporting the development and application of standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed.
- European Union Agency for Network and Information Security (ENISA), working to develop advice and recommendations on good practice in information security in the European Union scope.
- International Telecommunications Union (ITU), defining generic security capabilities and specific security capabilities. Generic security capabilities, which are independent of applications, are authorization, authentication, data confidentiality and integrity protection.
- Internet Engineering Task Force (IETF), developing protocols for use in constrained environments, where network nodes are limited in CPU, memory and power.
- OneM2M (Standards for M2M and Internet of Things), covering requirements, architectures, API specifications, security solution and interoperability for Machine-to-Machine and IoT technologies.
- Trusted Computing Group (TCG), developing, defining and promoting open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms.
- GSM Association (GSMA), providing a set of security guidelines for the benefit of service providers who are looking to develop new IoT services.
- International Electrotechnical Commission (IEC), dealing mostly with safety standards that are relevant in IoT due to its applicability in industrial settings (e.g. Industry 4.0, etc.).

IoT devices vary widely in their energy supply, available processing and message exchange capabilities. Different IoT deployments differ in their security requirements, depending on the vertical domains and the use cases involved. So there is no one-size-fits-all technical solution to IoT security. Hence the standards relevant for IoT security should be regarded as a menu from which the implementers can pick the options most suitable for their product or service. Huawei is actively supporting IoT security standardization. It is chairing 3GPP working groups, leading the NB-IoT work in 3GPP, and promotes LTE-V2X and wearable device standardization. It is also promoting service platform standardization in oneM2M and contributing in OCF, Thread, and OSGi Internet of Things standards.

6 Summary and Conclusion

6.1 Future opportunities to enhance security for IoT

Billions of devices will be joining IoT, thus making security a major challenge. Different industry domains will have different priorities for security solutions, based on their particular needs. However, IoT security is much like a chain; it is only as strong as its weakest link. Partner collaboration will play an important role in completing the picture of IoT security.

Over the last few years, industry players have been actively collaborating in standardization bodies to address the security challenges of IoT. In parallel, security agencies have been raising awareness to IoT security concerns, both within and across industries. These efforts have led to improvements in security technologies and introduced new security solutions. Huawei will continue to promote and support stakeholder collaboration to enhance the end-to-end security in IoT.

6.2 Conclusion

While the challenges of security in IoT can seem daunting, they are only so if faced alone. History provides ample cases where seemingly insurmountable challenges were conquered by collaboration among stakeholders. A few decades ago, the glooming prospect of a gaping hole in our atmosphere's ozone layer seemed like a global finality. Thanks to wide collaboration on a global scale, not only has the foreseen demise been avoided, we now observe evidence of healing in the ozone layer[7].

Collaboration lies at the core of Huawei's vision of IoT security. However challenging security in IoT may be, Huawei is confident in our collective ability to address it successfully. By coming together, equipment vendors, service providers, application developers and customers can resolve much more than any one alone.

7. National Geographic, "Remember the ozone layer? Now there's proof it's healing", http://news.nationalgeographic.com/2016/06/antarctic-ozone-hole-healing-fingerprints/

Trademark Notice

NO WARRANTY

HUAWEI TECHNOLOGIES CO., LTD.
Bantian, Longgang District
Shenzhen518129, P. R. China
Tel:+86-755-28780808

www.huawei.com