Building a Trusted and Managed IoT World
The Internet of Things (IoT) connects huge numbers of devices and offers diverse services, making networks more open and complex. While the IoT ushers us in a new world with everything perceptible, connected, and intelligent, major security challenges are emerging.

This Whitepaper analyzes the development of IoT security technologies, proposes the employment of multilayered end-to-end security mechanisms to safeguard the IoT, and summarizes IoT security practices. IoT technologies are developing apace. However, they are vulnerable to new security issues and threats. The security of the IoT can be ensured only if the industry chain works together as a whole. Therefore, Huawei proposes that all governments, international organizations, and industries join hands to build IoT security and work harder in guiding policies, enacting laws and regulations, setting standards, innovating new technologies, and building industry ecosystems.

Abstract

The Internet of Things (IoT) connects huge numbers of devices and offers diverse services, making networks more open and complex. While the IoT ushers us in a new world with everything perceptible, connected, and intelligent, major security challenges are emerging.

This Whitepaper analyzes the development of IoT security technologies, proposes the employment of multilayered end-to-end security mechanisms to safeguard the IoT, and summarizes IoT security practices. IoT technologies are developing apace. However, they are vulnerable to new security issues and threats. The security of the IoT can be ensured only if the industry chain works together as a whole. Therefore, Huawei proposes that all governments, international organizations, and industries join hands to build IoT security and work harder in guiding policies, enacting laws and regulations, setting standards, innovating new technologies, and building industry ecosystems.
Rapid IoT Development
IoT Development Trend

The IoT is ushering in a new era.

The IoT plays an important role in the digital transformation of all industries. Technological innovation creates huge numbers of connections, greatly improves efficiency and makes people’s life more convenient. The IoT market is about to boom.

The IoT is driving digital transformation in all industries. Companies, governments, organizations, and communities around the world strive to research and invest in the IoT and collect, analyze, and apply the data it generates. This will facilitate the rapid development of all industries.

The IoT will become part of our life, much as the Internet has already. Smart home, smart education, smart healthcare, wearable devices, the Internet of Vehicles (IoV), and other industries make wide use of the IoT. With everything connected, individuals and society as a whole will benefit immensely.

The huge popularity of mobile devices, and the resulting bevy of platforms and services that have grown up around them, is spurring the rapid growth of the IoT market. Gartner, Inc. forecasts that connected devices worldwide will reach 20.8 billion by 2020. This is a compound annual growth rate (CAGR) of 34%. Figure 1-1 shows a forecast of the IoT market by application.

IoT Security Threats and Challenges

Significant challenges blight these tempting figures.

On October 21, 2016, the largest DDoS attack on record took place in the U.S., forcing more than 100 well-known websites, including Amazon, offline for several hours. Attack traffic reached over 1 Tbit/s. This attack was unlike common DDoS attacks launched by IT devices (such as PCs and servers). It was launched by IP cameras (IPCs), home routers, digital video recorders, and other micro smart devices that were infected by the Mirai malware and caused severe disruption.

![IoT market forecast by application](Data source: Ovum, GSMA, Gartner)
On December 23, 2015, Ukrainian power distribution was affected by an attack that cut power to a large number of users for several hours. Hackers used BlackEnergy to access the power distribution management system and were then able to issue outage commands, erase and overwrite system data, and perform power-off operations.

In July 2015, Wired magazine revealed that hackers were able to remotely disrupt the driving of Jeep Cherokee vehicles. Fiat Chrysler Automobiles NV, parent company of Jeep, took network-level security measures to prevent this type of remote manipulation. It also recalled about 1.4 million cars and trucks equipped with vulnerable radios in the U.S.

The truth is security threats are never-ending. Traditional networks are still facing many security issues even with plenty of IT measures. This challenge cannot be avoided in the IoT era. In a Forrester survey of organizations around the world, 47% of industrial organizations that use or plan to use the IoT had previously experienced security breaches in their industrial applications. Further investigation shows that:

* 27% of the control systems were compromised or infected;
* 80% of the equipment uses a simple password;
* 70% of the communication is not encrypted;
* 90% of the firmware upgrades do not check signatures. Many devices may not or cannot upgrade.

The growing IoT enhances productivity and facilitates people’s life but brings about pervasive security threats. Security threats arise from three layers (as shown in Figure 1-3).

Ubiquitous sensors cause IoT endpoints to be untrusted.

* Outdoor endpoints are unmanaged and susceptible to physical attack, tampering, and spoofing.
* Device drivers may be untrustworthy and are easily leaked and controlled.
* Patches are not immediately available for operating system (OS) or software vulnerabilities.
* Considering the cost, the resources and computing capabilities of endpoints are limited. Traditional protection means and security technologies, such as antivirus software, may not be applicable.

Transition of the network layer to IP and convergence brings about threats.

* Flaws in wireless protocols, such as the lack of effective authentication, may lead to leakage at the access side.
* Private industrial applications and protocols cannot be identified by security devices and are easily exploited without timely detection.
* The unencrypted communication process is prone to man-in-the-middle (MITM) attacks, such as hijacking, replaying, tampering, and eavesdropping.
* IP-based networks are vulnerable to Internet-based attacks.
and intrusion.

Service openness at platform and application layers incurs new security threats.

* Platform-managed devices are numerous and widespread, making it difficult to upgrade and manage the security of such devices.
* New communication protocols may bring security issues and vulnerabilities at the application layer, such as malformed packet attacks and flood attacks.
* Vulnerabilities of new platforms and open APIs open doors to new risks.
* Unauthorized access leads to privacy and data leakage, such as authentication credential leakage.
* Various IoT applications may be untrustworthy.

In addition, devices, networks, and applications in the IoT may belong to a variety of vendors; therefore, a single vendor can hardly see the entire attack surface, let alone perform comprehensive security defense.

Privacy is one of the biggest legal challenges for the IoT.

IoT means that a vast number of connected devices will generate, send, and receive large volumes of data that are linked to individuals, resulting in the permanent monitoring of people's activities through many different devices. This monitoring may raise various requirements about privacy and the protection of personal data. Such concerns are nothing new—every relevant technological change has brought about concerns regarding privacy. It is right that we concern ourselves with privacy since the IoT involves more devices and data, and hence greater challenges.

---

<table>
<thead>
<tr>
<th>Sensing</th>
<th>Network</th>
<th>Platform &amp; application</th>
</tr>
</thead>
<tbody>
<tr>
<td>RFID</td>
<td>GSM/3G/4G/5G</td>
<td>Logistics management</td>
</tr>
<tr>
<td>Phone</td>
<td>LTE/3G/NB-IoT</td>
<td>Video surveillance</td>
</tr>
<tr>
<td>Temperature sensor</td>
<td>Wi-Fi</td>
<td>Industrial control</td>
</tr>
<tr>
<td>In-vehicle system</td>
<td>PSTN/ISDN</td>
<td>Health monitoring</td>
</tr>
<tr>
<td>Camera</td>
<td>Access switch</td>
<td>Directory service</td>
</tr>
<tr>
<td>Humidity sensor</td>
<td>WLAN/WSN</td>
<td>IoT service platform</td>
</tr>
<tr>
<td></td>
<td>IoT gateway</td>
<td>ICT management</td>
</tr>
<tr>
<td></td>
<td>Industrial Ethernet</td>
<td>Space information management</td>
</tr>
<tr>
<td></td>
<td>Industrial switch</td>
<td>QOS</td>
</tr>
</tbody>
</table>

Figure 1-3 Three layers of the IoT and their characteristics
Industry Requirements for IoT Security

IoT security is industry-specific (as shown in Figure 1-4) and may vary in terms of forms and requirements with business attributes, objects of service, management bodies, and working modes in different industries.

* Industry and energy: Cyber security of industrial control systems and smart grids, such as security of the intelligent computing service (ICS) and supervisory control and data acquisition (SCADA). An attack on an industrial control system may bring down the entire system, potentially halting production and leading to an outage.

* Mobility:
  Protection of smart vehicles
  Security and protection of unmanned aerial vehicles
  Protection of satellite communication systems
  Attacks may incur severe traffic accidents and endanger people’s lives.

* Healthcare:
  Protection of connected medical devices
  Encryption for medical and pharmaceutical research
  Safe and ubiquitous storage of medical data
  A possible scenario where life is put at risk is when a hacker gains control of the wireless implantable cardioverter defibrillator (ICD) inside a patient.

* Smart city: Secure transmission and storage of information collected by vast numbers of sensors. If a control system used in rail transportation is compromised, improper scheduling or derailment may occur.

* Finance: Protection of mobile payment from spoofing. Individuals and enterprises will inevitably suffer property damage in the case of exploit.

IoT security concerns not only the business success, but also the national economy and people’s livelihood. Building an IoT security environment is therefore an urgent requirement.
Multilayered End-to-End Security System for IoT
Multilayered End-to-End Security System for IoT

With the IoT comes omnipresent security threats, from system platforms to sensors. The IoT market is highly anticipated but full of challenges. Any risk at a single point can endanger the entire network and core systems. Therefore, security must be considered right from the start of IoT planning, and a multilayered end-to-end security system must be built (as shown in Figure 2-1).

IoT security is manifested in chips, devices, and their operating systems, networks, management platforms, apps, and enterprise operation. Security techniques and measures can be analyzed from each layer. In addition to security protection at each layer, a comprehensive end-to-end defense system is developed based on the interdependence of the device, pipe, and cloud. In this system, security situational awareness of the entire IoT is of special significance.

Chip and OS Security

Secure chips are preferred on IoT devices that have high requirements on security. Chip vendors provide strong hardware-level encryption and isolation using different techniques (as shown in Figure 2-2), such as Trusted Execution Environment (TEE) and Trusted Platform Module (TPM), so that important keys are stored in the trusted chip to prevent data breach. Additionally, secure boot is supported and signatures are checked during software and firmware startup and upgrade to assure data integrity. The IoT requires cost-efficient, energy-efficient, and universal chip-level security techniques.

The OS is an indispensable element in a complete security solution. In common lightweight IoT OS scheduling mechanisms, unified memory is shared irrespective of user or kernel mode. Apps and the kernel all run in the privileged mode. This poses many uncertainties and security threats to system services.
If the isolation mechanism of the lightweight secure OS is implemented, the user mode will be isolated from the kernel mode, and apps will be isolated from each other. Memory protection and isolated scheduling mechanisms for the kernel will be supported to greatly enhance system reliability and security.

Secure OS re-arranges and manages the memory to divide the space for the kernel and applications, uses the syscall mechanism to separate privileges in kernel and user mode, and provides users with configurable memory protection interfaces based on memory protection unit (MPU) or memory management unit (MMU).

Security protection measures (as shown in Figure 2-3) include:

- Design of proper memory layout
- Distinguishing kernel mode and user mode
- Process isolation for apps
- Memory protection interface

The safe area created by the lightweight isolation mechanism defends the OS. An app can create an independent safe zone based on the safe area using the MPU. Major features of the lightweight isolation mechanism created by the secure OS are as follows:

- Access control: Sandboxes are isolated from each other, security access channels are set up, and effective management and control is performed to prevent unauthorized access using malicious code.
- Security kernel: Lay the foundation for the security protection of firmware upgrade (firmware over the air or FOTA), security storage, key management, encryption and decryption, and device ID.

Secure OS can provide such functions as trusted identity authentication, secure firmware upgrade, Internet service access control, encryption and decryption, and key management.

**Endpoint Security**

IoT endpoints include access sensors and devices, which can collect data and access networks to report data. The characteristics of such endpoints are: low power consumption, low cost, weak computing and storage capabilities, physically accessible, long lifecycles, complex interfaces and protocols, etc.

The traditional security architecture can no longer satisfy these characteristics. A new security architecture is required to ensure IoT endpoint security (as shown in the Figure 2-4).

- Physical security: Water-, dust-, shock-, and electromagnetic-proof in the IoT environment.
- Access security: Forged devices must be prevented from accessing the network, and IoT endpoints must be protected from becoming zombies in DDoS attacks. The lightweight easy-to-integrate security app plug-ins help analyze endpoint anomalies and encrypt communication data to protect endpoints from being used as stepping stones to attack critical network nodes. In addition, new
technologies, such as the lightweight mandatory authentication mechanism, distributed authentication, and block chain, are also required.

* Running environment security: The kernel-level security mechanism provided by the lightweight, real-time, and embedded OS safeguards the environment. Software signature is supported for secure boot in service code so that only valid and intact software packages can be loaded. Access whitelisting is supported to prevent malicious code and unauthorized access.

* Service data security: Data leakage, copy prevention, and data isolation are used to secure local data.

* Unified management: It provides security management during the complete lifecycle, including device activation, identity authentication, secure storage, secure boot, integrity check, software upgrade, and device decommissioning.

Hardware and software must be fully considered for IoT endpoint security, including chip-level security, OS security, and security hardening of the endpoints running OSs. Trusted and managed endpoints are the basic requirement for IoT security because the IoT cannot widely develop on an untrustworthy basis. Therefore, vendors need to carefully select security techniques to accommodate sophisticated IoT endpoints based on the sensitivity of data, intelligence level of endpoints, and the features of different network architectures. For example, vendors could use new security techniques, such as lightweight security encryption and distributed authentication, to balance security, resource consumption, and cost.

**Network Layer Security**

The IoT brings about the need for networks to support various services, carry large volumes of traffic, and use different wired and wireless techniques. The wired techniques include Ethernet, RS232, RS485, and PLC, and wireless techniques include GPRS, LTE, ZigBee, Z-Wave, Bluetooth, and Wi-Fi. Most of the traditional...
security mechanisms still apply to the IoT world. For example, the following mechanisms can be used: network security zone isolation, authentication on devices attempting to access networks, automatic defense using firewalls, anti-DDoS, app- and web-based attack prevention, and secure transmission on control and user planes using IPsec.

The network layer security of the IoT focuses on two aspects: the security of new IoT communication technologies (such as NB-IoT and 5G) and the security mechanisms for numerous proprietary protocols and industrial control networks.

NB-IoT and 5G raise the following security requirements:

* Unified and distributed authentication of IoT endpoints characterized by high concurrency and decentralization
* Adaption to NFV software, automatic deployment, and dynamic programmability
* End-to-end encryption and new lightweight encryption algorithms in an open environment
* Cross-layer detection on attacks launched using devices of different vendors, and cooperation of multiple security functions

The IoT needs to make full use of the physical layer transport features of wireless mobile communications and apply security technologies for authentication, encryption, and secure transmission to ensure transmission quality, prevent eavesdropping on unknown locations, and increase the difficulty in launching MITM attacks. As for air interfaces, endpoints and networks are mutually authenticated according to wireless standards so that only authorized endpoints can access valid networks. Secure channels are established between endpoints and networks for encryption and integrity protection to prevent data leakage, tampering, and eavesdropping.

IoT endpoints use a large number of dedicated interfaces (including KNX, ModBus, and CANBus), which connect to industrial control networks. Most of these endpoints and networks are designed to run in isolated environments and therefore include poor security mechanisms. New security issues arise when these endpoints and networks are introduced to the IoT. To address these issues, IoT firewalls (as shown in Figure 2-5), security gateways, and other devices must be able to:

* Implement in-depth analysis and automatic filtering for industrial protocols and apps from different industries.
* Support encryption for access devices.
* Support whitelist-based filtering, including self-defined protocol filtering.
* Defend automatically against DDoS attacks characterized by device resource exhaustion and multi-industry app traffic attacks.

Network security products must also provide antivirus and advanced persistent threat (APT) defense for the IoT.

Platform and Application Security

The IoT management platform mainly manages a large number of IoT endpoints, data, operations, and security. As shown in Figure 2-6, the most critical security factor in all types of management is personal data. This is because a large amount of users’ personal data may be transmitted from dispersed endpoints to an IoT cloud platform or processing platform. Therefore, adequate protection must be provided for personal data in accordance with the requirements stated in the privacy protection laws of local countries and regions.

In addition, a variety of vertical applications, such as smart home, IoV, and smart metering, need to access the IoT platform. Security isolation mechanisms must be provided for data storage because the security requirements on data may vary with applications. In addition, the confidentiality and integrity of data in transit must be ensured. Sensitive information such as video data must be encrypted for cloud storage, and the data should be deleted upon the expiry of the required retention period for personal data.

The security of IoT applications must be also considered. Mandatory authentication and access control must be implemented for the access to the cloud. Application vulnerabilities should not expose application data in transit. Effective encryption and isolation must be provided for data storage on PCs and mobile endpoints.

Security Situational Awareness

The IoT system, comprised of devices, networks, platforms, and applications, requires not only multiple security defense measures at each layer, but also the intelligent Big Data security analytics
Figure 2-5 Application of industrial firewalls

API security management

<table>
<thead>
<tr>
<th>Security lifecycle management (provisioning, authentication, binding, upgrade, and retirement)</th>
<th>Security monitoring and exception detection (big data/machine learning/IDS)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Isolation</td>
<td>Security monitoring and exception detection (big data/machine learning/IDS)</td>
</tr>
<tr>
<td>Cipher key management</td>
<td>Basic security maintenance management (account/rights/logs)</td>
</tr>
<tr>
<td>Data encryption</td>
<td>Trusted TPM/vTPM</td>
</tr>
<tr>
<td>Software integrity protection</td>
<td>Privacy protection</td>
</tr>
<tr>
<td>Network isolation and anti-DOS</td>
<td>Security hardening for OS/database/web system</td>
</tr>
<tr>
<td>Basic security maintenance management (account/rights/logs)</td>
<td>Virtualization platform security</td>
</tr>
</tbody>
</table>

Figure 2-6 IoT platform security
capabilities for device-cloud synergy (as shown in Figure 2-7). This will allow the IoT to achieve network-wide intelligent security situational awareness, visualization and security defense, which will be the future of IoT security.

The large quantity of IoT endpoints makes them easy springboards for attacks, posing threats to the IoT core platform. The Big Data security analytics platform monitors and analyzes the traffic and behavior of endpoints against the baselines in real time to quickly locate infected endpoints. The platform can then coordinate security devices to contain the infection and isolate the infected endpoints according to the defined security policies. This series of actions will protect the core platform and service system.

In addition, the Big Data security analytics platform can function as a unified security monitoring and management platform for the entire IoT network. By monitoring the network and scheduling all security devices, the platform can prevent known and unknown threats, especially advanced and persistent threats (APTs), such as the attacks on the Ukrainian power grid. With the threat intelligence library and network-wide situational awareness, the Big Data security analytics platform predicts the IoT security trend and implements countermeasures to actively defend against threats.

![Figure 2-7 Security situational awareness for device-cloud synergy](image)

**Figure 2-7 Security situational awareness for device-cloud synergy**

**Summary**

The IoT brings numerous connections. Security is not an option for the IoT deployment; it is a fundamental requirement. Multilayered end-to-end security and defense mechanisms assure the reliable and secure operations of the IoT. However, IoT security issues are complicated and concern the management of personnel, devices, and systems more than the technology, requiring a systematic solution. New IoT technologies are emerging, and so too are new security issues. Multilayered end-to-end security and defense mechanisms need to catch up and be optimized. In the end, a healthy IoT operation environment could be created through effective management, automatic defense, and active prediction with the assistance of situational awareness (as shown in Figure 2-8).

![Figure 2-8 IoT security and defense](image)

**Figure 2-8 IoT security and defense**
IoT Security Practices
IoT security issues can be addressed following well-known practices in information technology security. This should be done during each stage of the deployment process, from the research and design phases through to the market deployment. Software and hardware vulnerability assessment and hardening of systems and communications should also be considered.

Due to the diverse use of IoT devices in applications such as enterprise environments, domestics, industrial systems, and healthcare, good practices should apply to the proper use and configuration at the endpoint.

Risk assessment, threat analysis, and impact analysis of possible attacks should be performed on a case-by-case basis so that proper security practices can be chosen to achieve the best balance of costs, usability, and security. For example, a device designed to operate in healthcare scenarios must consider many more parameters and apply stricter security practices than a smart watch.

As manufacturers develop IoT devices, there is inherent technical, time-to-market, and cost constraints that factor into device interoperability and design. Some devices are constrained by technical factors like limited internal processing resources, memory, or power consumption demands. Manufacturers are under pressure to reduce the unit cost of the device by minimizing part and product design costs. However, they must also consider the risks of security issues.

**Security Practices in Conceptual Design**

As mentioned earlier, attention must be paid to all possible stages of the IoT deployment lifecycle, from design and implementation to customer use.

* Provide pertinent market regulations and legislative security insights and research related to the target environment.
* This early stage would help determine the viability and things to be considered in subsequent stages.

**Security Practices in Technological Development**

After the conditions and constraints associated with the use case and operation environment have been determined, the security of hardware and software needs to be considered.

* **Hardware**

Depending on the limitations of the sector and its criticality level, the following practices can be observed:

- **Boot security**: Provide mechanisms to protect the boot process and trusted updates.
- **Firmware, memory, and storage**: Ensure secure firmware update and allow cryptographic verification. Verify possible information leakage due to embedded passwords. Make use of encryption on storage media.
- **CPU and microcontrollers**: In highly critical cases of use, it would be desirable to have mechanisms that detect tampering or reverse engineering attacks to avoid manipulation.
- **Physical access**: Protect or disable interfaces such as USB ports and JTAG. Design countermeasures for adverse environmental conditions.
- **Network components**: Use wireless boards, Bluetooth, or RF components compliant with current security standards.
- **Power management**: Have a failback mechanism in case of outage.
Software:

OS: Choose a proven operating system and apply all hardening measures recommended in each case. Follow the principle of the least privilege. Pay special attention to user privileges and permissions and enable anti-exploit protection for OS operations, such as ASLR, NX memory, and sandboxing.

API and development framework: If provided, ensure the security of use through vulnerability assessment and update policies.

Updates: Have a strategy of updates for the OS as well as software, even in the case of third-party software.

Security Practices in Functionality and Deployment

* Installation and configuration: Provide a well-designed set of procedures for setup and installation in a secure fashion. Force users to change the default security-related settings, such as the default password.

* Connectivity and services: Verify unnecessary network configurations such as open ports. Make encryption mandatory in all types of communications.

* Encryption: Choose a proven suite of encryption or verify possible weaknesses, such as pseudo-random number generators, if proprietary encryption is to be used.

* Privacy concerns: Ensure the protection of personal or sensitive data and enable the mechanisms of data destruction and encrypted storage on devices and endpoints where these data can be stored in.

* Authentication and authorization: If necessary, use secure mechanisms to interact and establish connections with devices and services such as cloud services.

* Backup and disaster recovery: In certain cases, it is recommended that security procedures be provided to ensure backup and complete recovery of data and the OS in case of disasters. Backup storage should be encrypted.

Security Practices in Verification and Testing

After a product is built and the applicable security practices have been implemented, the cycle should continue and the efficacy of them must be tested. Checkpoints should include:

* 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

Security Practices for User Operation and Maintenance

The measures taken in the preceding stages would be rendered useless if anyone or anything that interacts with the IoT device ignores security best practices. The following points should be considered:

* If a function or service provided on the device is not used or unnecessary, disable it.

* Keep the device updated and properly set.

* Use robust passwords and change them regularly.

* When IoT devices are to be integrated with other infrastructure, network connectivity and interactions with the environment must be evaluated. Then, a suitable location can be chosen for the device. Avoid undesired interference and exposure.

* Unused IoT devices can become a possible and uncontrolled security problem. Keep track of unused IoT devices. Alternatively, erase data on devices to be discarded.

3.6 Privacy Protection Practices

How can we embrace the IoT without sacrificing privacy?

Privacy can be protected using multiple ways, such as technological
means. However, laws and regulations provide the minimum mandatory set of requirements.

Within the European Union, the main regulation is the new General Data Protection Regulation (EU GDPR). It proposes the concept of “Privacy by Design” and requires privacy impact assessment (PIA) for specific data processing. The PIA is an important tool to fulfill data protection obligations. As stated in the GDPR, a PIA is required where a type of processing is likely to result in a high risk to the rights and freedoms of natural persons.

To ensure the rights and freedoms of individuals as far as is reasonably practical, Article 29 Working Party, the European Union advisory body on data protection, provides some recommendations such as:

* PIAs should be performed before any new applications are launched in the IoT.
* Every stakeholder in the IoT should apply the principles of Privacy by Design and Privacy by Default.
* Many IoT stakeholders only need aggregated data and have no need of the raw data collected by IoT devices. Stakeholders must delete raw data as soon as they have extracted the data required for their data processing.
* Device manufacturers must inform users about the types of data that are collected by sensors and further processed, the types of data that they receive, and how the data will be processed and combined.
* Device manufacturers should be able to communicate with all involved stakeholders as soon as a data subject withdraws consent or opposes the data processing.
* Similarly to the “do not disturb” feature on smartphones, IoT devices should offer a “do not collect” option to schedule or quickly disable sensors.
* To prevent location tracking, device manufacturers should limit device fingerprinting by disabling wireless interfaces when they are not used. Alternatively, they should use random identifiers (such as random MAC addresses to scan Wi-Fi networks) to prevent a persistent identifier from being used for location tracking.
* Users are entitled to access their personal data. They should be provided with tools enabling them to easily export their data in a structured and common format. Therefore, device manufacturers should provide a user-friendly interface for users who want to obtain aggregated data and raw data that is still stored.
* A setting should be available to distinguish between different individuals using the same device so that they cannot learn about each other’s activities.
* Default settings of social applications based on IoT devices should ask users to review, edit, and decide on information generated by their devices before publication on social platforms.
* Information published by IoT devices on social media platforms should not become public or be indexed by search engines, by default.
* Consent to the use of a connected device and to the resulting data processing must be informed and freely given. Users should not be economically penalized or have degraded access to the capabilities of their devices if they decide not to use the device or a specific service.

In Spain, data protection is the responsibility of the Spanish Data Protection Agency (AEPD), which monitors, by the hand of stakeholders, the change of the rules of the game, and have to go hand in hand with the companies that play the leading role, but with the citizens as well. Citizens play multiple roles: internet users, content generators, and data producers. Their safety must be ensured. To achieve this, there are guidelines for the re-use of information in the public sector and guidelines for the anonymization of personal data. If a company respects and protects the confidentiality of data, it is more likely to win the trust of its customers and raise its economic value. Its credibility in the market and its economic value in general are directly related. With this in mind, it needs to be affirmed to re-attain the forgotten rights and to call the attention of the legal security of companies on the internet. Development of the necessary tools for the new regulation that goes into effect in 2018 must also be spurred on. To this end, work being carried out by SETSI (now SESIAD), AEPS, and national security forces in the coming year becomes crucial and critical.
Typical IoT Security Cases
The IoT is gradually being commercialized after years of development and exploration. Uses include smart cities and smart logistics, and it will be broadly applied in areas such as smart home, wearable devices, IoV, and smart elevators. The IoT will connect more things in multiple domains within a short time and greatly facilitate economic development and our daily life. However, there are two sides to every story. The security of giant networks in the IoT and the volumes of data transmitted on them is a big concern. Information leakage or systems being damaged or maliciously controlled will incur great losses. Therefore, security is critical.

The critical infrastructure of the Industrial Internet has already become a target of cyber attacks. National security and social stability are severely affected when critical infrastructure is attacked and networks paralyzed—the damage is immeasurable. Furthermore, hacker organizations and even states have joined the line of attackers with increasingly professional, well-structured, and sophisticated means of attack.

The launch of Tesla cars and the maturity of smart car systems developed by Internet giants such as Apple and Google indicate that the concept of IoV is becoming reality. However, if a smart car is hacked, the owner may be blackmailed and severe traffic accidents may happen, threatening people's lives.

The IoT can be applied to many scenarios. This Whitepaper only selects and analyzes some successful practices in its application to smart city, smart home, smart grid, and internet of elevators for the reference of rapidly growing IoT-concerned vertical industries. Rapid development of new IoT technologies will always bring new security issues and threats. Therefore, IoT security will continue to evolve.

Smart City

The rapid development of information and communications technologies is changing people's lives and the operation and management of cities. Smart city is a new concept that makes use of this development. Many countries, including China, Singapore, and Thailand, are building smart cities. The IoT enables a smart city to build a huge neural network. The IP camera, as a neural network element of the smart city, is deployed in varied complex conditions. As a result, IP cameras are difficult to manage but easy to attack (as shown in Figure 4-2). Due to the large quantity of IP cameras, an attack on them can have severe consequences. Security threats faced by IP cameras should be analyzed so that appropriate IoT countermeasures can be developed (shown in Table 4-1) and widely applied to video surveillance.
<table>
<thead>
<tr>
<th>Typical Security Threat</th>
<th>Countermeasure</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spoofing by rogue IP cameras</td>
<td>Unique device certificate verification</td>
</tr>
<tr>
<td></td>
<td>Device lifecycle management</td>
</tr>
<tr>
<td>Eavesdropping and tampering of video content and interception of local data</td>
<td>Encryption of signaling and data in security tunnels</td>
</tr>
<tr>
<td></td>
<td>Sandboxes to prevent data breach</td>
</tr>
<tr>
<td></td>
<td>Big Data–based threat baseline</td>
</tr>
<tr>
<td>Stepping-stone attacks</td>
<td>Device port management</td>
</tr>
<tr>
<td></td>
<td>Network isolation</td>
</tr>
<tr>
<td></td>
<td>Big Data–based threat baseline</td>
</tr>
<tr>
<td>Weak passwords, vulnerabilities, and intrusions</td>
<td>Self-check by security plug-ins</td>
</tr>
</tbody>
</table>

Table 4-1

Smart Home

Smart home uses IoT technologies to provide home services, such as smart home control, communications, and shopping. AT&T, Telefonica, Vodafone, Deutsche Telekom, China Mobile, China Telecom, and China Unicom are just a few examples of major players in the industry who are developing smart home services, such as home healthcare, entertainment, energy, and security (as shown in Figure 4-3).

Smart home solutions require multilayered end-to-end security and defense mechanisms to assure security:

* **Sensor and device security**: Provide encrypted communication channels using shared keys through short-range communication protocols, such as ZigBee and Z-Wave, to ensure secure connections between endpoints and gateways and hence the security of sensors and devices.

* Install TPM chips inside gateways to implement secure boot and verify the integrity of software and firmware. The trusted status on all gateway devices is reported to the cloud and visualized.

* The cloud platform provides security analysis capabilities based on Big Data and machine learning technologies and collects logs, events, and traffic information to analyze anomalies in IoT devices, endpoint users' behavior, and the
cloud platform status. It can also identify and control the risks of intrusion attacks on endpoints and the cloud platform.

**Smart Grid**

Many countries and organizations desire a smart grid that is flexible, clean, secure, efficient, economic, and user-friendly. Accordingly, they develop their electric power plans and improve infrastructure to achieve this. Four modules are highlighted in the smart grid: advanced metering infrastructure (AMI), advanced distribution operations (ADO), advanced transmission operations (ATO), and advanced asset management (AAM). The global electric metering system is evolving towards AMI, which is the key to a smart grid. In the IoT era, precise metering will become crucial in the supply of electricity, which makes the smart meter the core of AMI. By 2020, smart meters are expected to have a market penetration of 59% globally.

Millions of smart meters help electricity enterprises in smart metering, line loss analysis, electricity consumption analysis,
and prepaid electric functions. However, attacks such as tampering or spoofing of smart meters can lead to the unrecorded consumption of electricity and large-scale outages may occur. This can result in economic losses or even security incidents. Smart meters may become a powerful weapon against the smart grid. Therefore, security must be considered. How to ensure trusted access of smart meters and effectively protect key infrastructure becomes the major challenges for smart grid security.

Meters are usually deployed outdoors and exposed to the risks of spoofing and data tampering. Therefore, meters shall be designed to prevent electricity theft and unauthorized access with effective identity authentication. Anomalies shall be automatically reported for precisely locating the theft. Data on the meters shall be encrypted for reporting to prevent eavesdropping and breach.

In addition, the grid shall protect services from APTs, DDoS attacks, viruses, and other threats.

To this end, solution providers must be able to provide end-to-end solutions and delivery with security as an essential component, and effectively interact with users to improve customer experience and electric supply quality, reduce emissions, and enhance enterprise operation efficiency with lower costs.

### Internet of Elevators

Worldwide, there are more than 15 million elevators in use. This number continues to rise. In recent years, a number of accidents have been associated with elevators. As a result, the demand for operation and maintenance (O&M) services in the elevator market is huge.

Deploying the internet of elevators enables elevators to be controlled through the cloud. However, security issue may result in the loss of control over elevators or the breach of core data such as elevator locations. To ensure the security of the entire internet of elevators, multilayered security mechanisms are needed to assure secure data transmission and O&M from several aspects (as shown in Figure 4-5):

- **Chip**: The authentication information or software packages of sensors, gateways, and other devices must be protected from being tampered with by using TPM.
- **OS**: Security modules should be deployed for underlying software to ensure the security of the OS and running environment.
- **Network**: The channels connecting elevators to the cloud are all encrypted to ensure data security in transit.
- **Cloud platform**: Tailored security defense solutions are provided for the cloud platform, including those for application security, anti-APT, cloud boundary security, logic boundary security, and anti-DDoS.

![Figure 4-5 Security of the internet of elevators](image-url)
Building a Trusted and Managed IoT World
Government & Industry Promotion

The rise of the IoT has attracted interest from a number of major countries, who have started to develop national IoT strategies. In July 2016, the Spanish Cybersecurity Agency, INCIBE, released Market Trends in Cybersecurity to call for the further building of IoT security capabilities. And, in November 2016, the U.S. Department of Homeland Security released Strategic Principles for Securing the Internet of Things, which is used as the guiding principles for IoT security. The European Programmer Horizon 2020 sets several cross-cutting topics, such as the combination of cyber security and the IoT as well as the development of secure societies, protecting the freedom and safety of Europe and its citizens. The Alliance of Industrial Internet (AII) of China establishes an IoT security team to improve IoT standards and other aspects.

The IoT is driving a new wave of industrial revolution. However, in many industries, security needs are diverse, security solutions are neither comprehensive nor mature, and security risk assessment methods and countermeasures are unclear. It is not enough for one or several industries to guide IoT security— a higher-level coordinator is needed to coordinate all concerned industries. Therefore, governments and industry organizations must prioritize IoT security as a national strategy, and pay greater attention to the development of IoT security policies, laws and regulations, and standards to jointly build the IoT.

Faster Development of IoT Security Standards

Standards play a critical role in the development and evolution of technologies. Products and solutions depend on or comply with applicable standards. Similarly, standards become increasingly important for the IoT because the IoT combines multiple types of technologies, ranging from the underlying access technologies to upper layer cross-industry applications. Consequently, the IoT security is becoming a major concern of standard organizations.

Currently, many standards organizations and alliances are actively proposing and designing security technology standards to tackle IoT security challenges for a smarter and fully connected ecosystem.
The development of standards for IoT security is still in its infancy with a focus on guidelines and frameworks. Detailed technical standards that can guide the implementation in industries are scarce. Therefore, it is urgent for standard organizations and alliances to speed up the development of relevant security standards to push the fast growth of the IoT industry.
Active Participation in IoT Security Industry Ecosystem

The highly integrated IoT industry is developing quickly with diverse needs and soaring threats. A single enterprise can hardly meet IoT requirements. It has become necessary to build an open and collaborative security ecosystem for win-win development. Industries, developers, academies, and industry standards organizations must work closely to encourage innovation in business, in science, and in technology, and jointly build a healthy ecosystem for cooperation, fair competition, and win-win development.

IoT security attack and defense are unbalanced—defense usually lags behind attack. From the perspective of economy or return on investment, attackers have a clear target for investment while defenders invest in security defense for risk control, which is to say that attacks may not happen at all. Sophisticated attackers can focus their attacks, whereas defenders must defend against many uncertainties. In contrast, the defenders build a strong defense system in the cyber space with various security products and services. However, security attack incidents only get worse, and cyber attacks cause greater damage with the pervasive application of information technologies in the IoT era.

To win this unbalanced battle, industries need to follow the concepts of openness, fairness, and win-win cooperation. They need to build a healthy security ecosystem for security technologies, products, solutions, and services through such channels as policy guidance, standardization, developer communities, open source communities, and industry alliances. Consequentially, a defense network can be constructed for the IoT (as shown in Table 5-1).

No enterprise or organization can resolve IoT security issues alone. All parties in the ecosystem must cooperate and support each other. All device suppliers, consultation firms, application software vendors, system integrators, and channel partners should embrace win-win cooperation in an open manner to jointly build a healthy and trusted IoT security ecosystem and promote the healthy and rapid development of the IoT industry.

Figure 5-1 IoT security ecosystem building
IoT security concerns every aspect of the digital landscape with high market expectations from consultation firms, enterprises, and carriers. Although the IoT brings many benefits, it also brings threats. Unfortunately, the industry’s understanding of security issues varies. There is a gap between the ideal and the reality. However, fortunately, the IoT will definitely be standardized, open, secure, and made easy-to-use in the future. We must embrace cooperation and innovation from a global perspective to jointly build a multi-layered end-to-end secure IoT world and contribute to the development of the ideology, theories, and architecture. However, this will take time. We must seize the opportunity and work together to accelerate process.

To realize the ideal, security is critical. To promote the large-scale deployment of the IoT, the industry must raise their awareness; governments and international organizations must improve corresponding laws and regulations and the standards system; and a healthy ecosystem must be formed to build a trusted, managed, and secure world with the IoT.

This is the best of times. A trusted and managed secure IoT world built and shared by all will be the wish of global IoT industries and benefit all.

**Abbreviations and Acronyms**

- MQTT: Message Queuing Telemetry Transport
- CoAP: Constrained Application Protocol
- API: Application Platform Interface
- DDoS: Distributed Denial of Service
- ICS: Industrial Control Systems
- SCADA: Supervisory Control and Data Acquisition
- TPM: Trusted Platform Module
- TEE: Trusted Execution Environment
- MPU: Memory Protection Unit
- MMU: Memory Management Unit
- PLC: Power Line Communication
- GPRS: General Packet Radio Service
- LTE: Long Term Evolution
- NB-IoT: Narrow Band Internet of Things
- APT: Advanced Persistent Threat
About INCIBE, Red.es & Huawei

INCIBE

INCIBE. The Instituto Nacional de Ciberseguridad de España, S.A. (Spanish National Cybersecurity Institute) is an organization dependent on the Ministry for Energy, Tourism and Digital Agenda (MINETAD). INCIBE is the benchmark institution with regard to the development of cybersecurity and of digital trust for the general public, for Red.es and for businesses, especially sectors of strategic importance.

As a center of excellence, INCIBE is a service offered by the Spanish Government to work towards the development of cybersecurity as an instrument for social transformation and for developing new fields of innovation. To this end, with its activities focused on research, the provision of services, and cooperation with the relevant actors, INCIBE heads a range of initiatives directed at cybersecurity at both a national and an international level.

The Security and Industry CERT (CERTSI), Computer Emergency Response Team of cybersecurity operated by INCIBE, works to enhance the detection and early warning of new threats, responses to and analysis of information security incidents, and the design of prevention measures to address the needs of society at large. INCIBE, by virtue of a joint working agreement signed by the Secretaría de Estado de Seguridad (Secretary of State for Security), provides public services to the security needs of critical infrastructures and the support in cybercrime research.

Red.es

Red.es is a public corporate entity attached to the Ministry of Energy, Tourism, and Digital Agenda which develops an extensive set of programs so that the Spanish society can benefit from the maximum of the possibilities offered by Information and Communication Technologies (ICT). The mission of Red.es is also to generate employment and foster entrepreneurship, increase the productivity and competitiveness of Spanish companies and increase savings and efficiency in public spending. At the same time, the knowledge and specialization from Red.es allows them to contribute to the establishment of the priorities and actions of the Digital Agenda for Spain which is leaded by the State Secretariat for the Information Society and Digital Agenda (SESIAD), in collaboration with the public authorities and the private sector.

Huawei

Huawei is a leading global information and communications technology (ICT) solutions provider. Driven by responsible operations, ongoing innovation, and open collaboration, we have established a competitive ICT portfolio of end-to-end solutions in telecom and enterprise networks, devices, and cloud computing. Our ICT solutions, products, and services are used in more than 170 countries and regions, serving over one-third of the world’s population. With more than 170,000 employees, Huawei is committed to enabling the future information society, and building a Better Connected World.