Closing the gaps in IoT security

The security of the Internet of Things (IoT) is critical given the potential damage hackers can cause by hijacking huge numbers of networked objects and creating zombie botnets. Yet, awareness of enterprise IoT security is generally very poor. In fact, IoT products from many companies have zero security protocols.

By Wang Xiaojun & Yu Junhua

IoT security threats and challenges

HP's Security Research *Cyber Risk Report 2015* shows that 27 percent of IoT control systems have been compromised or infected, over 80 percent of IoT devices have simple passwords, more than 80 percent of devices retain hardware debug interfaces, 70 percent of device communication processes are not encrypted, and over 90 percent of device firmware updates are not signed or verified. A large number of IoT communications protocols also lack security mechanisms, according to the report.

This reality has allowed a successive spate of attacks targeting or originating from IoT devices in the past few years, including an Internet outage over a large swathe of the US, a simulated attack on a Tesla car, and a power blackout in Ukraine.

The large-scale US Internet outage on October 21, 2016 was the worst DDoS (distributed denial-of-service) attack in the country's history, leading to Internet services going down over a large area of the east coast. The attack originated from tens of millions of IP addresses – mostly IoT devices such as DVRs, IP cameras, routers, and Linux servers – infected by the Mirai virus. These devices were vulnerable to becoming bots for a DDoS attack because they were using standard, fixed hardcoded passwords and other unsecured mechanisms.

There are two major challenges facing IoT security. The first is complex deployment environments and network structures, including access and data processing for massive numbers of devices, complex network structures, excessive numbers of communication protocols, and the different security requirements of different industries. The second is limited computing and network resources. IoT sensors and some gateways have tight cost and power consumption constraints plus limited computing power and storage capacities. As a result, it's difficult to run complex security protocols on them. Furthermore, their network bandwidth tends to be limited, with many local networks only offering tens of kbps of shared bandwidth.

3T+1M architecture security

The security requirements of IoT devices, networks, platforms/clouds, applications, and privacy compliance are much higher than they are for traditional networks. The key to IoT security lies in building device security and protection capabilities. IoT devices can be roughly divided into two categories based on their features: weak devices and strong devices/gateways. Each faces different security threats and demands.

Access and data processing for massive numbers of devices, particularly in high concurrency access scenarios such as surge attacks, is a huge challenge for IoT networks and platform security. In scenarios with massive numbers and amounts of devices and data on the network and platform side, it's critical to be able to quickly detect malicious device behaviors like DDoS attacks and malicious tampering. This must be followed by fast threat diagnosis and response in the form of warning and isolation processes.

Protecting data such as user location, consumption data, and health data has much higher privacy compliance requirements for cloud-based IoT platforms, especially in verticals like electricity and the Internet of Vehicles (IoV), which have high certification requirements.

The cloudification of IoT services brings greater challenges for end-to-end (E2E) security operations and management such as smart security inspections and situational awareness in visual security.

Huawei developed its 3T+1M (technology + management) security architecture with the following in mind: IoT security threats, IoT

Analysis of the security requirements of IoT devices

Type of device	Main features	Typical threats	Security requirements	Typical applications
Weak devices	Weak computing power, limited memory resources, sensitive to cost and power consumption	No or weak passwords, no certification, easy to counterfeit, not upgradable, vulnerable to theft	Must meet some basic security requirements that consider computing power and cost; for example DTLS/+, remote upgrades, and password management	Water and gas meters, vehicle parking, logistics tracking, wearables, and agricultural sensors
Strong devices	Powerful computing power, embedded operating systems, multiple means of attack. Attacks have greater impact	Illegal device startup, illegal upgrades, plaintext storage, virus attacks, and system defects	Basic and enhanced security requirements must be met, including secure startup, PKI, TPM/TEE, virus protection, and system hardening	IoV, cameras, IoT gateways, and handheld interactive devices

Building a device security system is the first line of defense in ensuring IoT security.

application scenarios, and specific IoT security requirements. 3T+1M architecture encompasses devices, pipes, clouds/ platforms, data security, privacy protection, and E2E security O&M.

Device and cloud anti-attack measures

Building a device security system is the first line of defense in ensuring IoT security. The security capabilities of devices need to be configured to match their functions and computing resources, including memory, storage, and CPU. For weak devices, such as NB-IoT water and gas meters, where resources are limited and cost and power consumption are issues, basic security capabilities are a must. These include basic two-way authentication, DTLS, encrypted transmission, and remote upgradability. Scenarios like meter reading, where power consumption is a key factor, best suit lightweight, optimized, and secure transmission protocols.

Strong devices with more powerful computing capabilities that don’t have power consumption constraints and are operationally critical, such as industrial control terminals and car networking equipment, require advanced security capabilities, including trusted devices, intrusion detection, secure startup, and anti-virus protection. Device chip security and security for lightweight operating systems such as LiteOS need defense capabilities in line with the functions of strong devices.

Cloud is also an essential piece of the security puzzle: Coordinated device and cloud defense systems will enable security situation awareness, monitoring, and device upgrades to be carried out on the cloud.

Detect and isolate

To quickly detect and identify malicious behavior in massive numbers of IoT devices and carry out isolation and warning alarm processes, network and IoT platforms require malicious terminal detection and isolation technologies. First, the network side needs to have surge and DDoS attack protection capabilities. Second, the network must be able to coordinate with the IoT platform to identify malicious devices using rule matching, big data analysis, machine learning, and other rapid detection analysis algorithms like device behavior traces, traffic anomalies, and packet analysis. The IoT platform also needs to be able to quickly diagnose and respond to device behavior according to the application scenario and specific situation based on device behavior detection results. Responses include early warnings, observations, isolation and forcing devices offline, and instructing networks to take appropriate measures. This is the second line of defense in IoT security.

Platform and data protection

The requirements for cloud platforms and data protection are much higher for IoT, including the platform's own security, data storage, processing, transmission, and sharing functions. As well as cloud native security such as WAF, firewalls, and HIDS, data privacy protection, various other measures are required to meet specific IoT data protection requirements; for example, data lifecycle management, data API security authorization, tenant data isolation, and encrypted video data storage, plus compliance with national IoT data privacy compliance requirements. This is the third line of defense in IoT security.

Security operations and management

Establishing O&M system tools and the operating capabilities of O&M personnel is critical to IoT security O&M. For the coordinated handling of layered device-pipe-cloud architecture, O&M system tools provide E2E whole network visual security situation awareness, daily security assessments, O&M security reports, and smart security inspection. Providing security O&M guidance for IoT O&M personnel and standard security operating procedures for O&M operations enables O&M personnel and policy makers to perform service management. This improves the capability of the whole IoT security system, from preventative early warnings and detection and analysis to dealing with events after they occur.

When building a 3T+1M IoT security defense system, it’s crucial to develop key support technologies. These include lightweight security protocols, lightweight device system security, malicious device behavior rapid detection algorithms, and visual security situation awareness.

The security ecosystem is essential

The IoT security ecosystem must focus on device security, but the technological capabilities of many IoT verticals in device security are very limited. With this in mind, Huawei’s various OpenLabs are designed to help industry partners develop device security capabilities.

OpenLabs provides E2E IoT security testing and verification services for devices, networks, and platforms, with security features comprising a key part of IoT partner certification. The lab provides partners with technical specifications and test cases for IoT device security to develop corresponding black box testing tools to ensure the access security of different devices. To build a healthy and open IoT security ecosystem, Huawei has opened its IoT network and platform security capabilities and O&M tools to carriers and vertical industry partners.

With research on IoT security ecosystems and standards development just getting underway, Huawei believes in collaboration, combining the strength of upstream and downstream manufacturers to lead trials and experiments that will drive the maturity of key technologies, solutions, testing and verification, and industrial applications in IoT security.

Huawei will also encourage industry standards organizations to develop and improve IoT security standards as quickly as possible, and regulate IoT security certification to enable the rapid development of the IoT industry.