MENA Information Security Conference 2017

On the Verge :

Combating Cyber Threats leveraging Threat Intelligence, Faster Detection & Automated Response

Building a Secure Internet of Things World: *How billions of connected devices are transforming the cyber security landscape*

Andy Purdy, JD, CISSP, CIPP/US
CSO, Huawei Technologies USA

HUAWEI

Building a Secure Internet of Things World

How billions of connected devices are transforming the cyber security landscape

The "**Internet of Things**" "refers to 'things,' such as devices or sensors – other than computers, smartphones, or tablets – that connect, communicate or transmit information with or between each other through the Internet."

Agenda

- IoT and its Benefits
- Modern Cyber Security Threats and IoT
- IoT Architecture and Cyber Security
- Huawei 3T+1M Solution
- Appendix - Use Cases

The Future of IoT: IoE (Internet of Everything)

A World of Every Thing Connected!

Vision of IoT:

- All things in the world will get connected
- It will significantly improve our life quality
- It will transform what we do and how we do

Estimated IoT market around 2020:

- 50 billions IoT devices
- 7 trillions revenue

The Future of IoT: IoE (Internet of Everything) - Benefits

- Healthcare - Reduce healthcare costs while giving consumers the ability to record, track, and monitor their own vital signs
- Home Automation - Greater energy efficiency and reduced costs
- Transportation - Safety and convenience benefits
- Societal Benefits - Aggregation of big data can lead to research and breakthroughs.

Courtesy of U.S. Federal Trade Commission. www.business.ftc.gov.

IoT Security Issues Exposed in News

How to Hack WiFi Password from Smart Doorbells

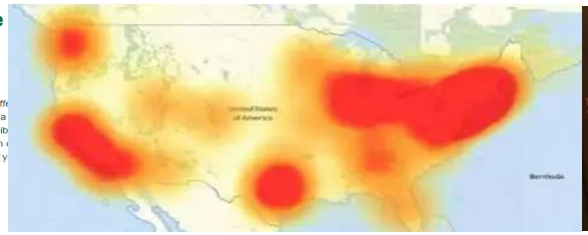
Wednesday, January 13, 2016 Mohit Kumar

A smartphone-controlled coffee machine

What could possibly go wrong?

Risk: leakage of the password to the home wireless network

The coffee machine we've randomly chosen can remotely prepare a cup of coffe
want. You just set the time and when the coffee is ready the app will send you a
also monitor the status of the machine through an app. For instance, it is possib
now or not, if it is ready for brewing or if it is time to refill the water container. In
device, which, unfortunately, gives an attacker a way to hijack the password of



FEB 17, 2016 @ 10:27 AM 30,635 VIEWS

300,000 American Homes Open To Hacks Of 'Unfixable' SimpliSafe Alarm

Thomas Fox-Brewster, FORBES STAFF

I cover crime, privacy and security in digital and physical forms.

FULL BIO

"There is something terribly wrong with the alarm industry." Thus reads marketing material on the site of SimpliSafe, a Boston-based "smart" alarm provider with more than 300,000 customers in the US. It's been on a mission to improve home security since it formed in 2006 by using cellular technology to warn customers via their smartphone if someone has broken in, whilst allowing

Ukraine Power Outage

Event: Power went out for 80,000 customers in Ukraine (Dec 23, 2015)

Impact: 7 substations had to be manually restarted

Specifics: Email spear-phishing introduced "BlackEnergy" malware into computer networks. This likely enabled remote access that took down the substations Phone systems were attacked, preventing customers from reporting outages. A component of the malware wiped computers, covering the perpetrators' tracks.

Recovery time:
- *6 hours*

Lessons learned:
- Employees need ongoing training e.g., spear-phishing
- Implement good network design and segmentation
- Incorporate active network monitoring tools

Stuxnet re-programmes centrifuges

The worm found the controlling software and inserted itself into it, seizing control of the centrifuges.

Stuxnet carried out two separate attacks. First, it made the centrifuges spin dangerously fast, for about 15 minutes, before returning to normal speed. Then, about a month later, it slowed the centrifuges down for around 50 minutes. This was repeated for several months.

Several months later

1,000 machines are destroyed

Hundreds of centrifuges were hijacked and instructed to spin out of control.

THIS HACKER'S TINY DEVICE UNLOCKS CARS AND OPENS GARAGES

Mirai was a wake-up call; WannaCry was just passed.

MENA INFORMATION SECURITY CONFERENCE 2017

HUAWEI

IoT Security Issues Exposed in News

IoT Security Issues Exposed in News

A smartphone-controlled coffee machine

What could possibly go wrong?

Risk: leakage of the password to the home wireless network

The coffee machine we've randomly chosen can remotely prepare a cup of coffe
want. You just set the time and when the coffee is ready the app will send you a
also monitor the status of the machine through an app. For instance, it is possib
now or not, if it is ready for brewing or if it is time to refill the water container. In c
device, which, unfortunately, gives an attacker a way to hijack the password of y

IoT Security Issues Exposed in News

IoT Security Issues Exposed in News

FEB 17, 2016 @ 10:27 AM 30,635 VIEWS

300,000 American Homes Open To Hacks Of 'Unfixable' SimpliSafe Alarm

Thomas Fox-Brewster, FORBES STAFF
I cover crime, privacy and security in digital and physical forms.
FULL BIO

"There is something terribly wrong with the alarm industry." Thus reads marketing material on the site of SimpliSafe, a Boston-based "smart" alarm provider with more than 300,000 customers in the US. It's been on a mission to improve home security since it formed in 2006 by using cellular technology to warn customers via their smartphone if someone has broken in, whilst allowing

IoT Security Issues Exposed in News

Ukraine Power Outage

Event: Power went out for 80,000 customers in Ukraine (Dec 23, 2015)

Impact: 7 substations had to be manually restarted

Specifics: Email spear-phishing introduced "BlackEnergy" malware into computer networks. This likely enabled remote access that took down the substations Phone systems were attacked, preventing customers from reporting outages. A component of the malware wiped computers, covering the perpetrators' tracks.

Recovery time:
- *6 hours*

Lessons learned:
- Employees need ongoing training e.g., spear-phishing
- Implement good network design and segmentation
- Incorporate active network monitoring tools

Stuxnet re-programmes centrifuges

The worm found the controlling software and inserted itself into it, seizing control of the centrifuges.

Stuxnet carried out two separate attacks. First, it made the centrifuges spin dangerously fast, for about 15 minutes, before returning to normal speed. Then, about a month later, it slowed the centrifuges down for around 50 minutes. This was repeated for several months.

Several months later

1,000 machines are destroyed

Hundreds of centrifuges were hijacked and instructed to spin out of control.

Mirai was a wake-up call; WannaCry touched thousands.

Traditional vs Modern Network Security Threats

Traditional Networks

Single entry point

Perfect isolation

Strict access control

Predictive threat

Modern All IP Networks

Multiple entry points

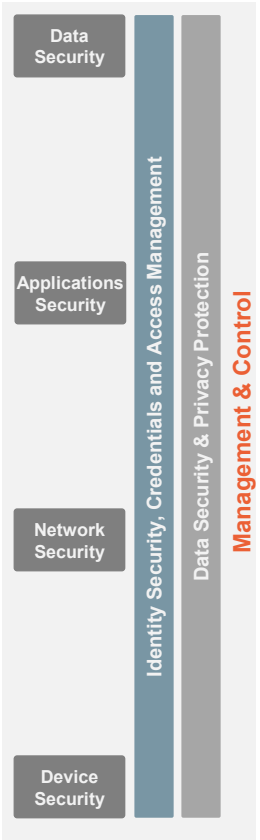
Chaos interleaving

Loose access control

Unexpected threat

IoT Architecture

IoT Architecture – Threat Categories & Defenses



Major Differences

- Limited end-point resource constraints: computing power, etc.
- No typical network protocols
- Harsh environment: dust, shock, humidity, strong electromagnetic fields, wide temperature limits.
- Safety issues beyond security

Similar Points

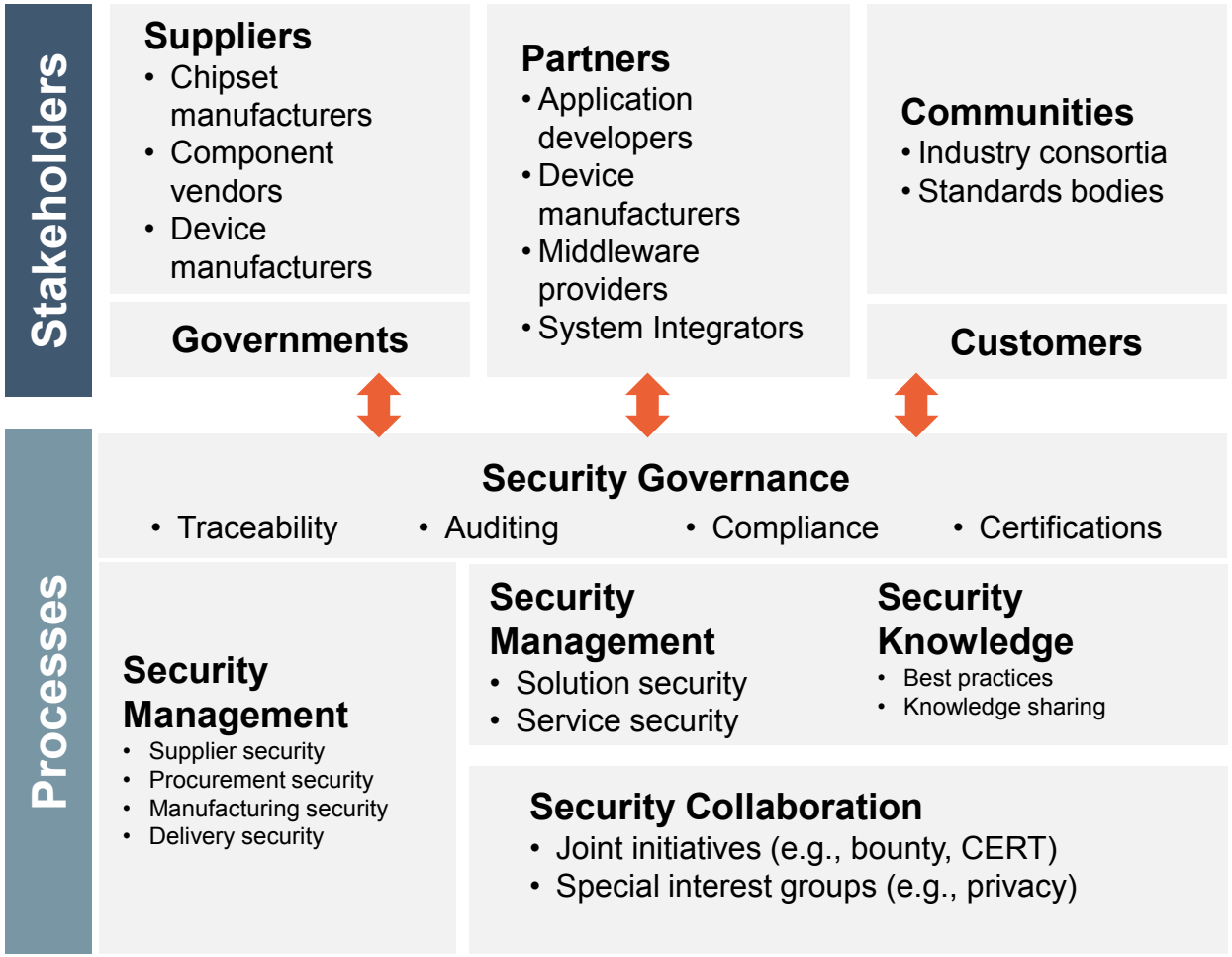
- The basic security protection principles: Privacy, Security, Reliability, Resilience
- The E2E security protection architecture
- Both of their security mechanisms are based on 'before, during, after' emergency response.

Cloud
- User data and privacy
- Data intrusion & attacks
- API & Applications security
- Credential disclosure
- Service penetration risks

Pipe
- Network transmission eavesdropping
- Hijacking and tampering
- IoT protocols vulnerabilities
- Network attacks & intrusion risks

Device
- Resources Restrictions
- Identity theft and physical attack
- Security risks of low-power devices
- Lack of endpoint protection
- OS Parches and updates

IoT Security Business Architecture



- IoT Security involves multiple stakeholders
- Standards and Compliance
- Governance and auditing
- Security measures validation
- Best practices sharing
- Risk exposure monitoring
- Collaboration is essential
- Buyer's power

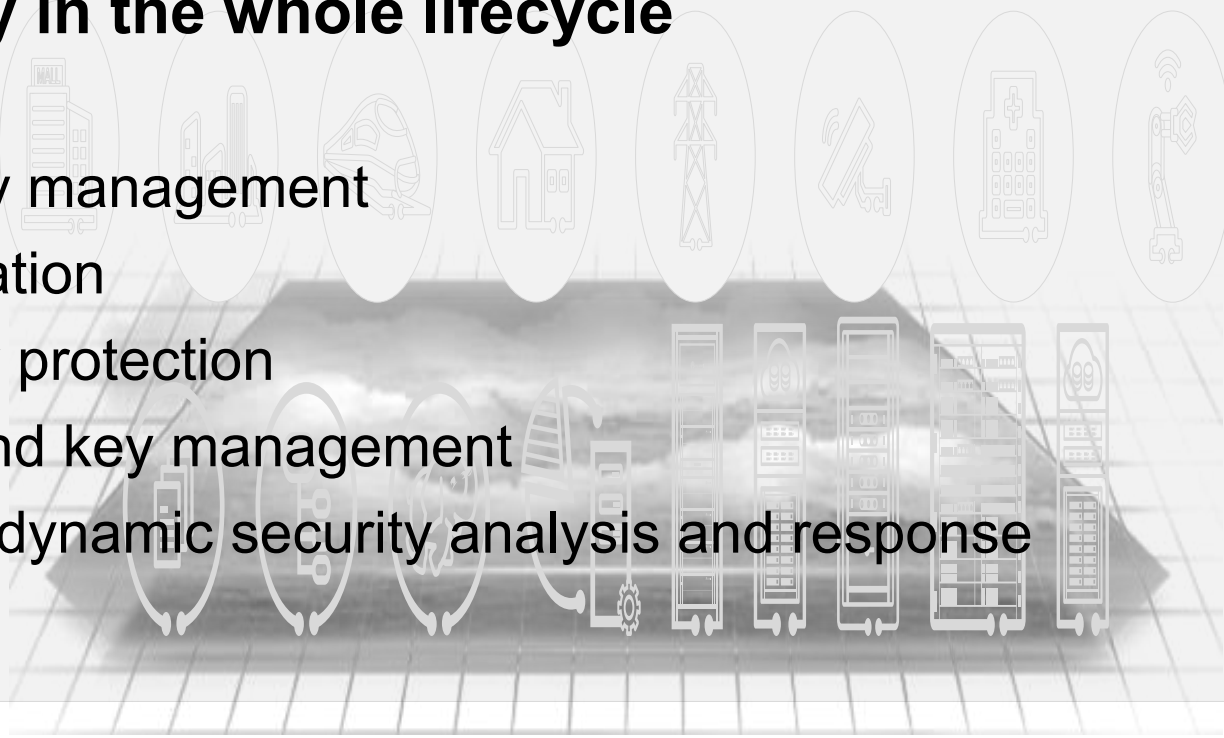
Huawei's 3 "T" + 1 "M" IoT Security Architecture

IoT Security (3T+1M)
Defense-in-Depth Solution Providing E2E Security

T Platform and Data Protection

Data Security in the whole lifecycle

- API security
- Data security management
- Tenants isolation
- Data Privacy protection
- Certificate and key management
- Big data/ML dynamic security analysis and response

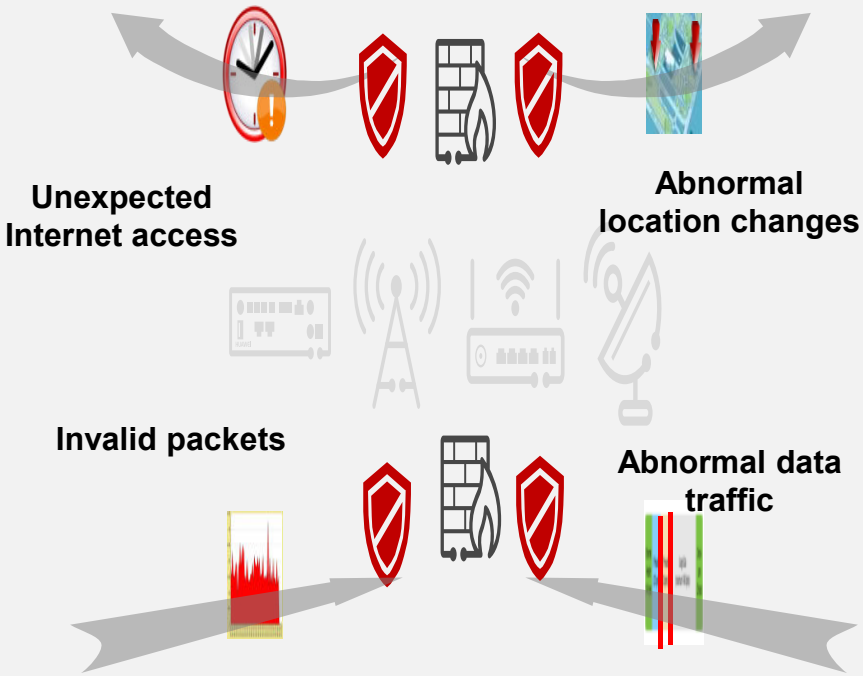


IoT Security (3T+1M) (2)
Defense-in-Depth Solution Providing E2E Security

T Malicious device detection and isolation

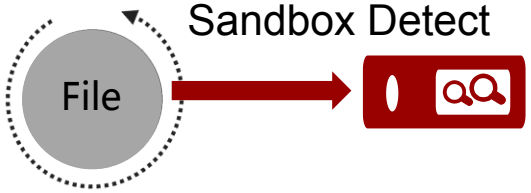
API security

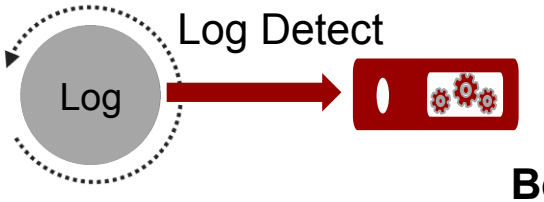
- DataBlacklists and whitelists
- Defense against surge signaling storms
- Fast detection of malicious device
- Isolation rules and policies
- IoT protocol identification and filtering



Malicious Device Detection and Isolation

Visible Abnormal Behavior Detection



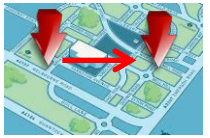


Behavior analysis

Access in abnormal time

Invalid packet

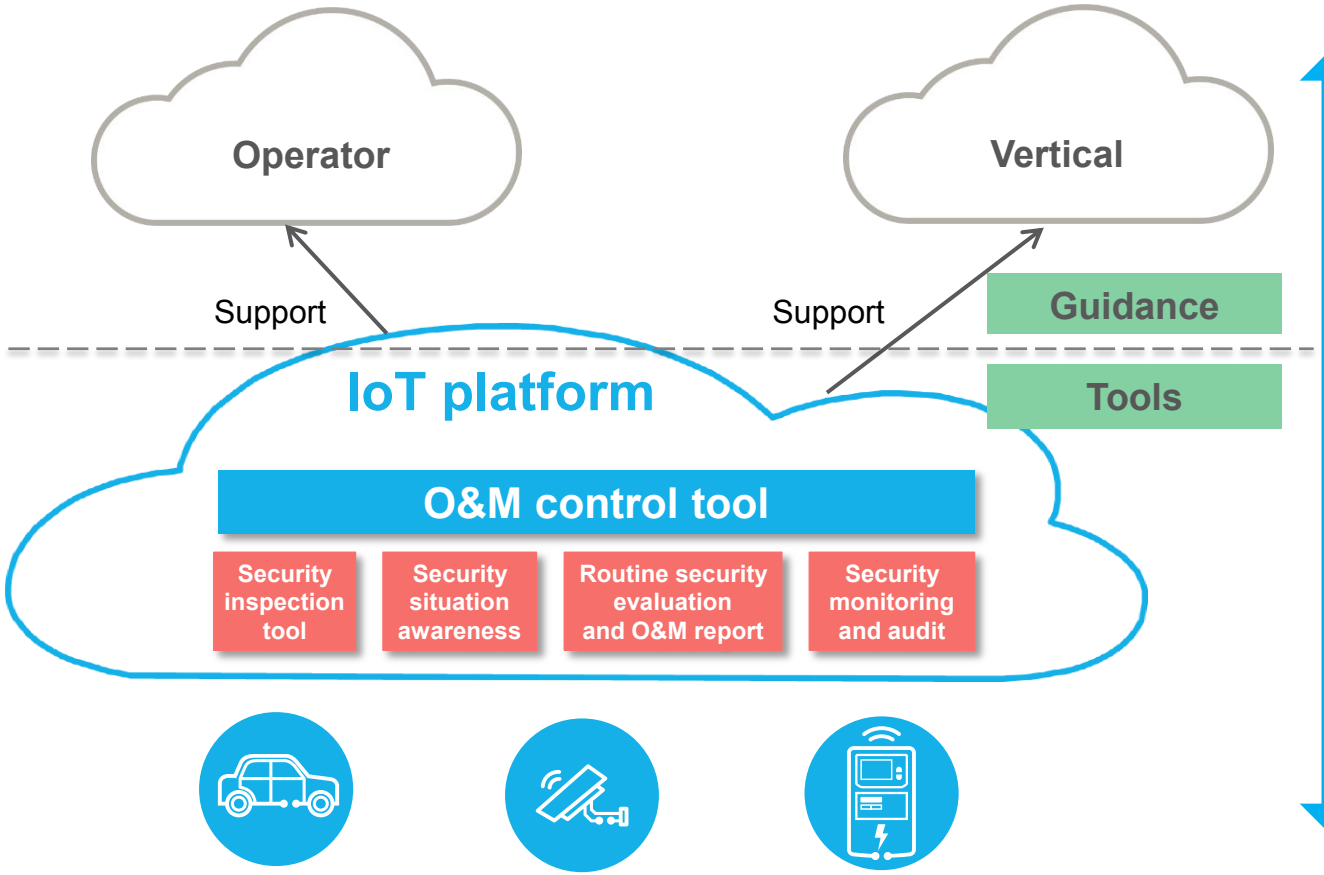
Abnormal data traffic



Abnormal location movement

Behavior analysis, Unknown risk identification, and DM to isolate malicious attacks

Secure Operations and Management Providing Operational Guidance

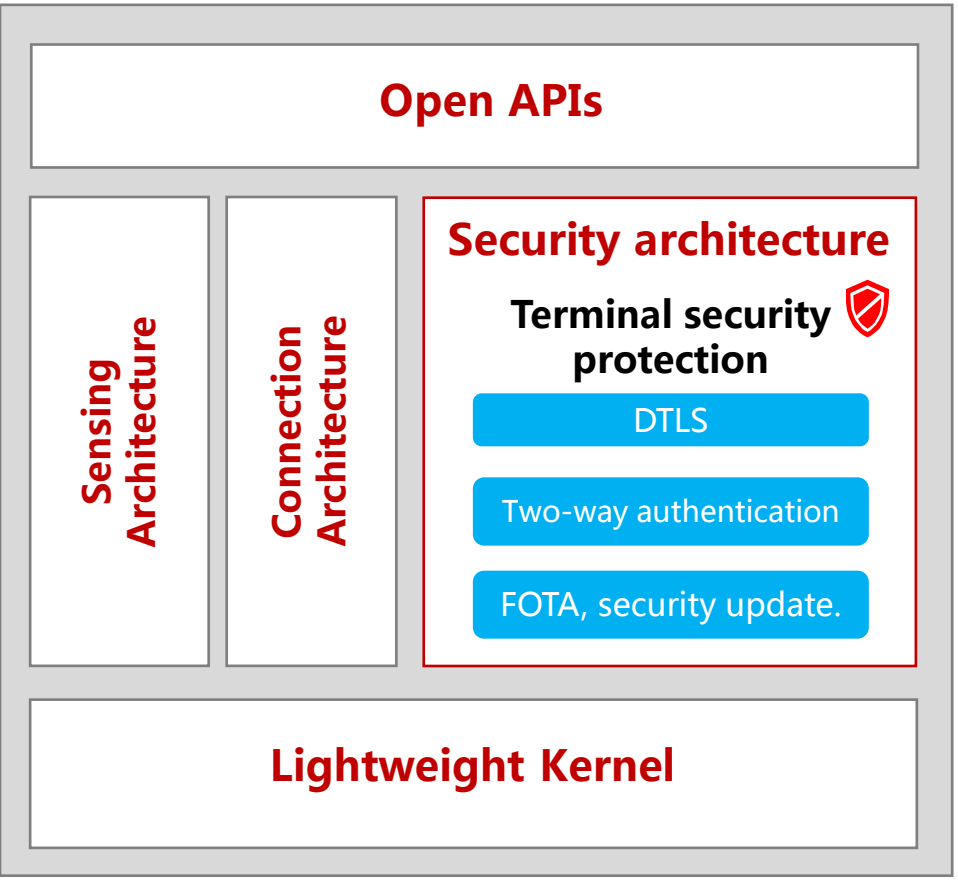


- Management decision-making
- Emergency assurance
- Background support
- On-site O&M
- Customized development
- Installation delivery
- Terminal authentication

To provide basis for O&M personnel and decision makers

Configurable device defense capability
LiteOS+ Chip Security capabilities + SDK

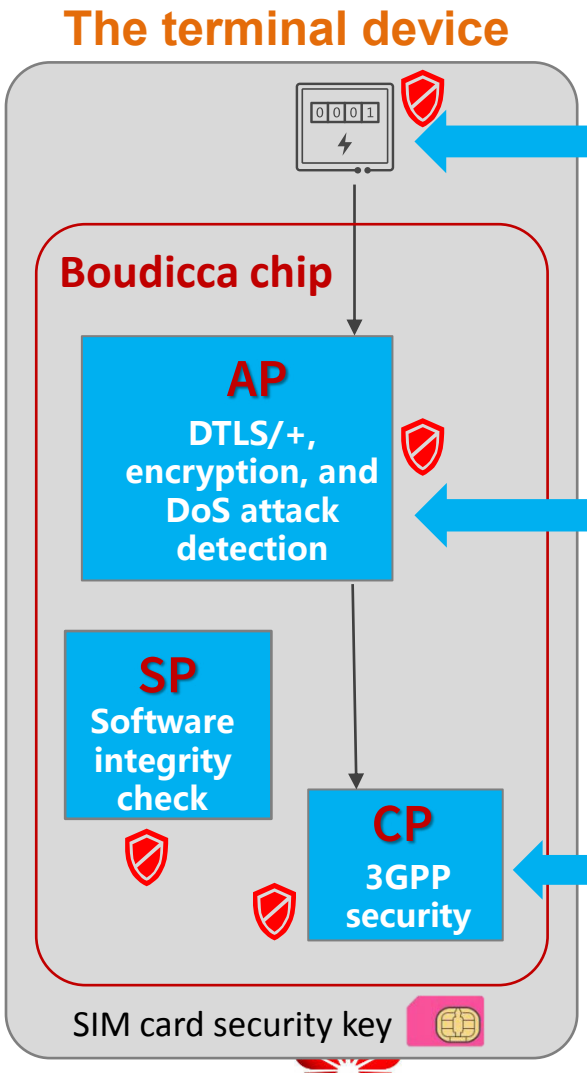
LiteOS system security



The terminal device

Configurable device defense capability
LiteOS+ Chip Security capabilities + SDK (2)

LiteOS system security



Application layer

The value is provided by the industry

Device security

Application Server

Https

Transport layer

DTLS/+: NB-IoT Adding security

IoT platform

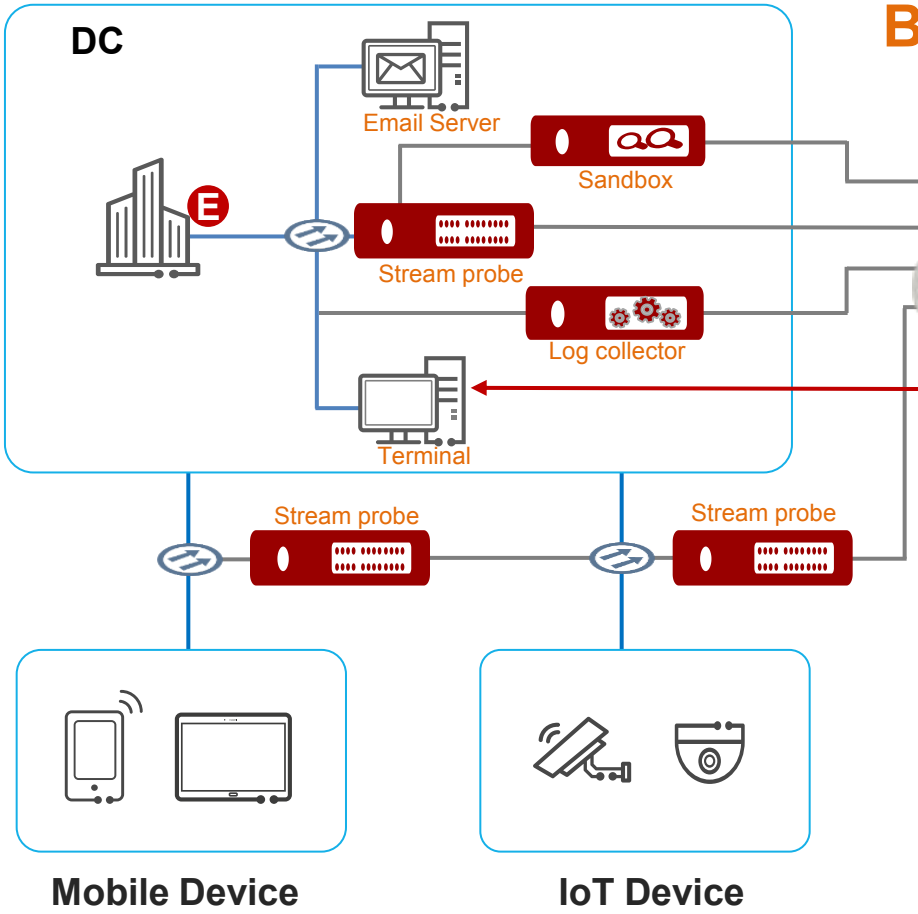
Data link layer

4G security algorithm

AP: application processor; SP: Security Processor; CP: general processor

DTLS: packet transport-layer security protocol

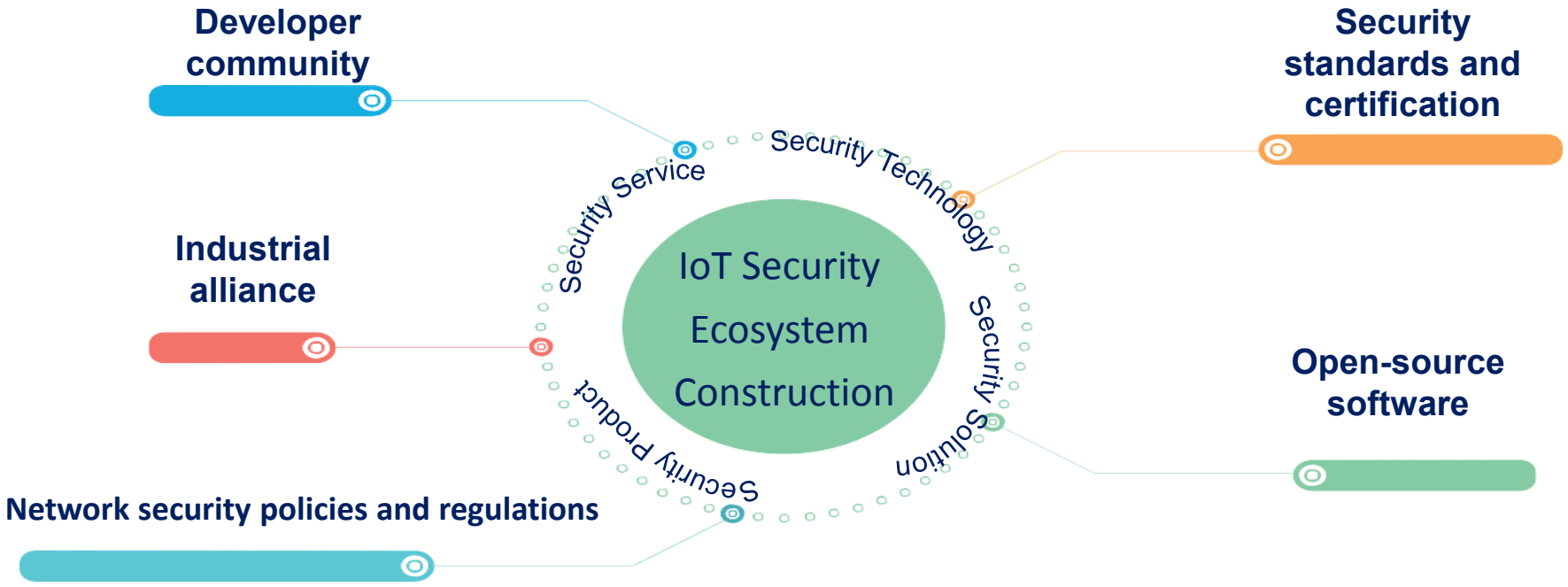
Big Data Analysis of IoT Cybersecurity



Big Data analysis platform

- Intelligent center of whole network, network security situation awareness.
- Collect all logs & traffic metadata, deep association and behavior analysis, identify APT and other potential unknown threats
- Cooperate with Terminal Security Management System, clean up malwares.
- Identify and display APT attack paths and quickly investigate APT attacks.

Cooperating with Partners to Build a Harmonious, Open, and Win-win IoT Security Ecosystem



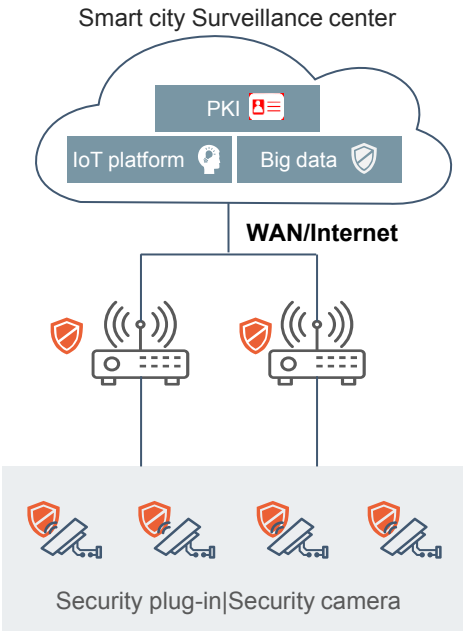
Summary

- IoT is here and the threats are REAL
- Partnership and collaboration are key for success
- Best security practices and architectures must be followed – e.g., 3T+1M
- Effective governance and strict compliance are essential

THANK YOU

Case Study 1: Smart City

Network architecture



③ **Management risks:** blind management areas and invisible risks

② **Network risks:** IoT protocol attacks and DDoS attacks

① **Device risks:** unmanaged, spoofing, and intrusion

Security solution

1. Device risks: The security plug-in provides embedded security capabilities.

- Device lifecycle management: periodic upgrade and maintenance
- PKI certificate management system, ensuring trusted access
- Security encryption, ensuring the confidentiality and integrity of original data

2. Network risks: IoT security gatewaya

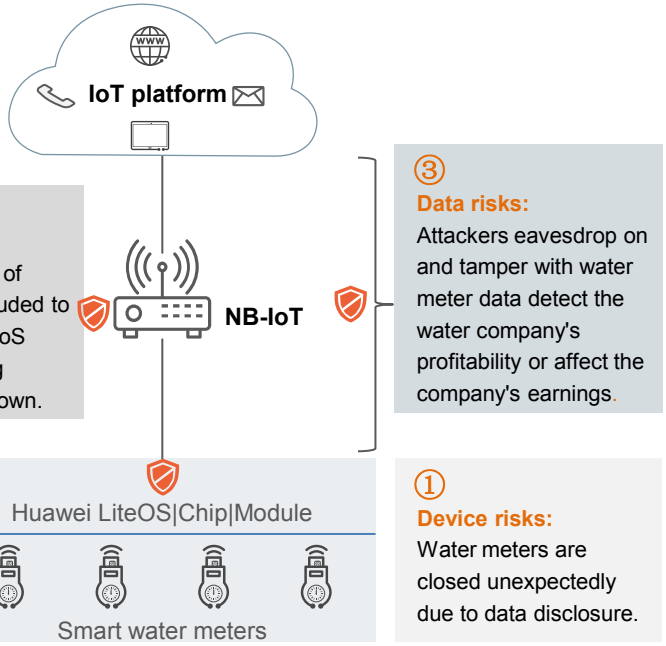
- Lightweight tunnel encryption algorithm, ensuring the access from million devices
- Protocol whitelist, filtering IoT protocol traffic

3. Management risks: Big data analysis-based unified security monitoring platform

- Awareness and display of security postures and collaborative cloud protection
- Network collaboration, defending against unknown threats

Case Study 2: Smart Metering

Network architecture



② **Network risks:** A large number of devices are intruded to launch DoS/DDoS attacks, causing network breakdown.

③ **Data risks:** Attackers eavesdrop on and tamper with water meter data detect the water company's profitability or affect the company's earnings.

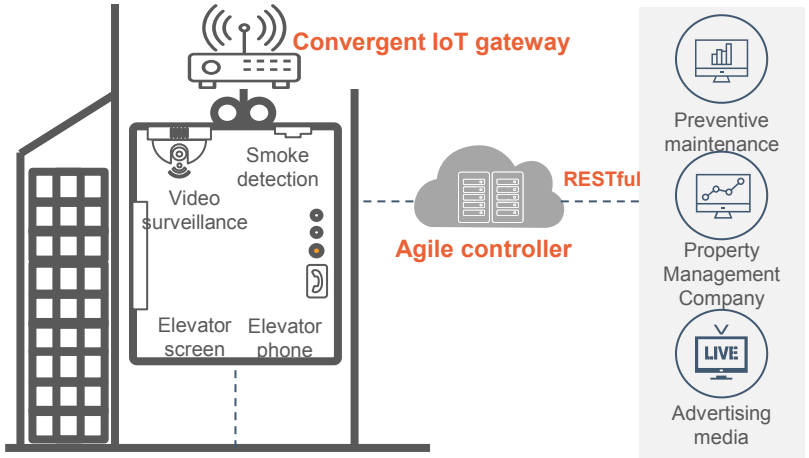
① **Device risks:** Water meters are closed unexpectedly due to data disclosure.

Security solution

1. **Device risks: Provide comprehensive security mechanisms.**
   - External interface security: Provide serial interface authentication to prevent external attacks.
   - Internal protection: Provide software signature verification to prevent malware implantation in hacker attacks.
   - LiteOS security: Provide SafeArea and differential upgrade.
2. **Network risks: Provide data transmission security protection and network anti-DDoS.**
   - E2E transmission security ensures the confidentiality and integrity of data during transmission.
   - Network anti-DDoS: In the IoT scenario, based on defense against traditional attacks, the core network and base stations work together to provide a new overload control mechanism to defend against DoS attacks that may be introduced by a large number of devices.
3. **Data risks: anti-attack for the IoT platform, data loss prevention, and privacy protection**

Case Study 3: Internet of Elevators

Network architecture



Device risks:
The elevator control is lost, endangering personal safety and causing service interruption

Cloud risks:
Commercial confidential information, such as the elevator location and customer information are stolen

Security solution

1. Device risks:

- Chip security: supports TPM
- OS security: supports secure boot and software security signature
- The IoT gateway determines whether elevator instructions are valid

2. Cloud risks:

- Data transmission: Data is encrypted during transmission and storage.
- Cloud platform security: anti-APT and anti-DDoS