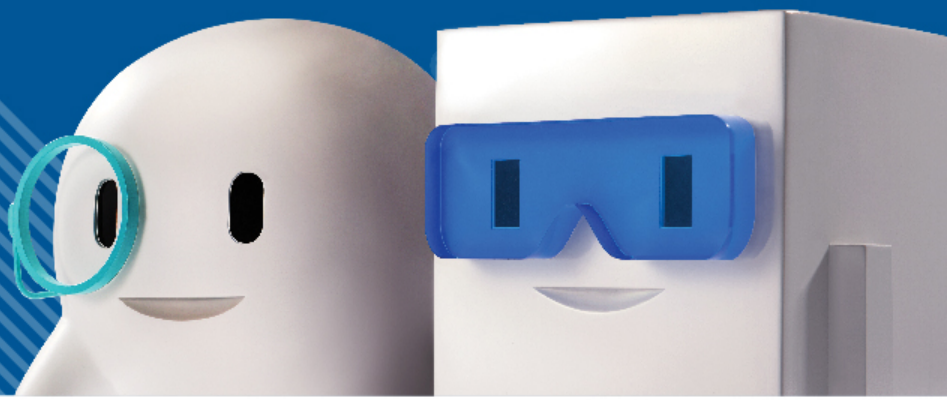
HKPC

HKCERT

Outlook of IoT Security Challenges

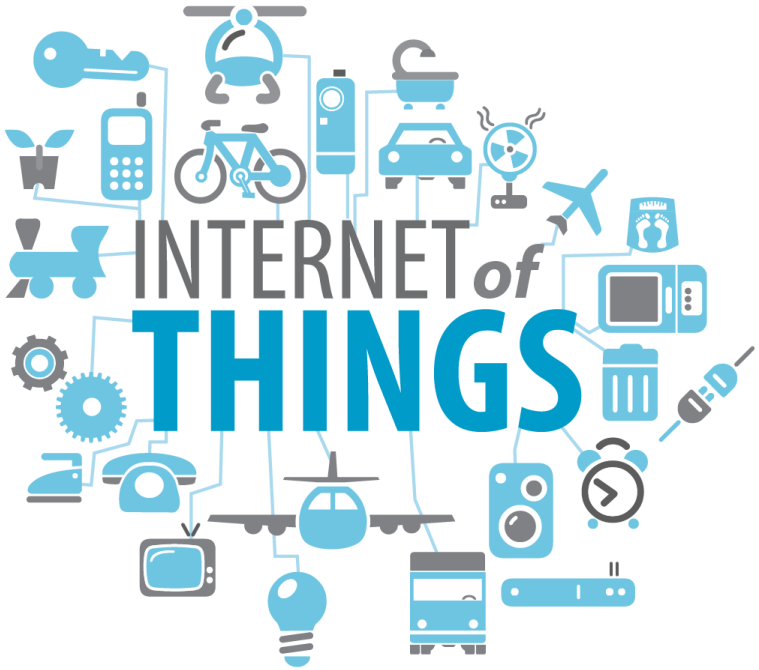


All-round Productivity Partner
全方位企業伙伴

What is Smart?

- Automation
- Real time monitoring & control
- Give advice or make decision for you

Internet of Things (IoT)



- Interconnection of a wide range of smart devices using the existing Internet infrastructure
- Machine-to-machine communication
- Many devices made for real life application → can impact daily life, economy or even safety

Internet of Things (IoT)

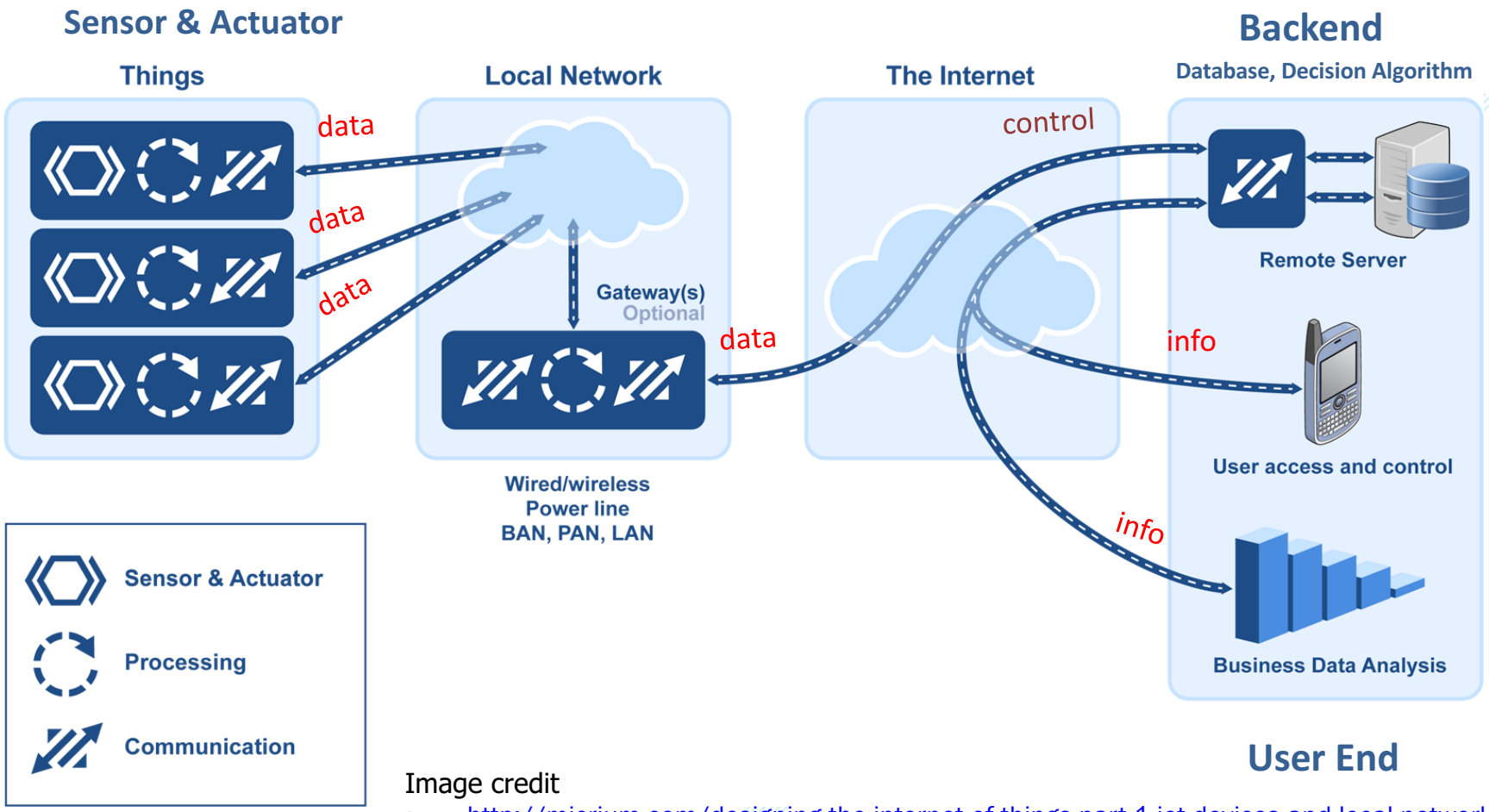


Image credit

- http://micrium.com/designing-the-internet-of-things-part-1-iot-devices-and-local-networks/

Data collection

- Data collecting devices
  - Smart meters, smartphones, smart cars, street CCTV , Wearable devices and other ubiquitous sensors

- Personal Data involved
  - Personal Identifiable information (HKID, driver license, credit card)
  - Derived data (credit score, transactional data)
  - Behavior data (location, preference, purchase, booking)
  - Self identified data (purchase intent, self-generated content, health data)

Application and Attack Scenarios in Smart Age

Electricity in Smart Cities

- Smart power generation plants
- Smart distribution and transmission
- Smart Meter

Electricity in Smart Cities (Smart Meter)

- Researchers in Spain
- Possibilities
- Shut down home electricity
- Over/Under bill
- Forward data out
- Install network worm

Reference
http://www.itpro.co.uk/security/23251/smart-meter-hack-could-leave-homes-in-the-dark

Electricity in Smart Cities (Power plant)

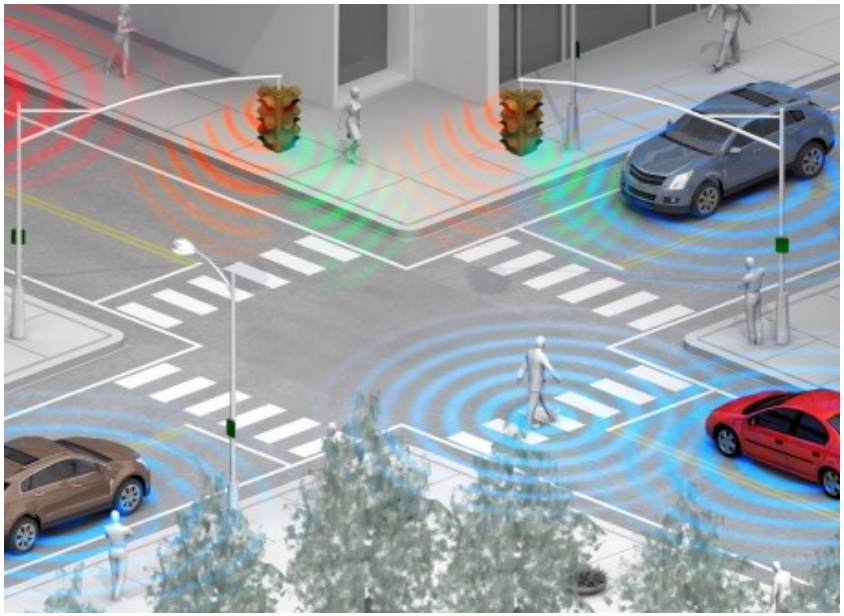
30 Dec **2015**

Current Reporting on the Cyber Attack in Ukraine Resulting in Power Outage

13 comments Posted by robertmlee

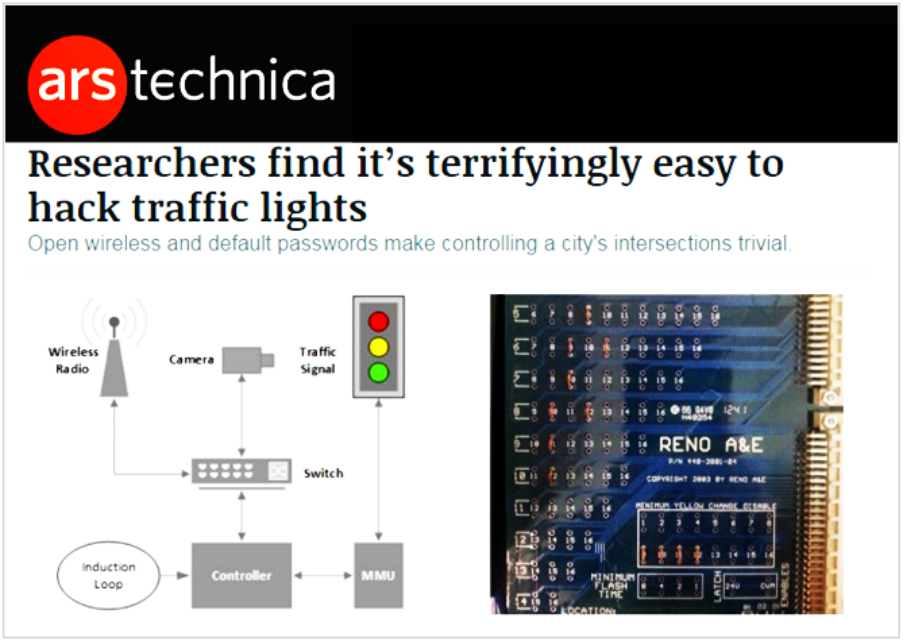
- Ukraine: Over 30 power substations down in 2015 Dec
- The power outage lasted for six hours
- affecting 230K people
- Compromise of corporate networks using spear-phishing emails with BlackEnergy malware
- Steal grid workers VPN account in corporate networks and using VPN connect to SCADA networks

Smart Transportation



- Autonomous Vehicles
- Intelligent Transportation Systems
  - Parking Information System
  - Real-Time Traffic Monitoring System
  - Intelligent Signaling System

Smart Transportation (traffic light)



Researchers @ University of Michigan with road agency
August 2014

- Camera & Controller of traffic light
  - communication via WiFi
- Controller
  - running VxWorks, debug port open
- Control system communication
  - no encryption, no authentication

Smart Health

- Wearable devices
- Monitor devices
  - blood pressure
  - glucose level
  - etc.
- Relay info. to healthcare service provider

Smart Health

FDA U.S. FOOD & DRUG ADMINISTRATION

Search FDA

back to Safety Communications

Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication

SHARE | TWEET | + | EMAIL

Date Issued:

January 9, 2017

- Pacemakers
- Connect to home Transmitter
- Could be hacked to send modified commands

Reference: http://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm

Smart Home

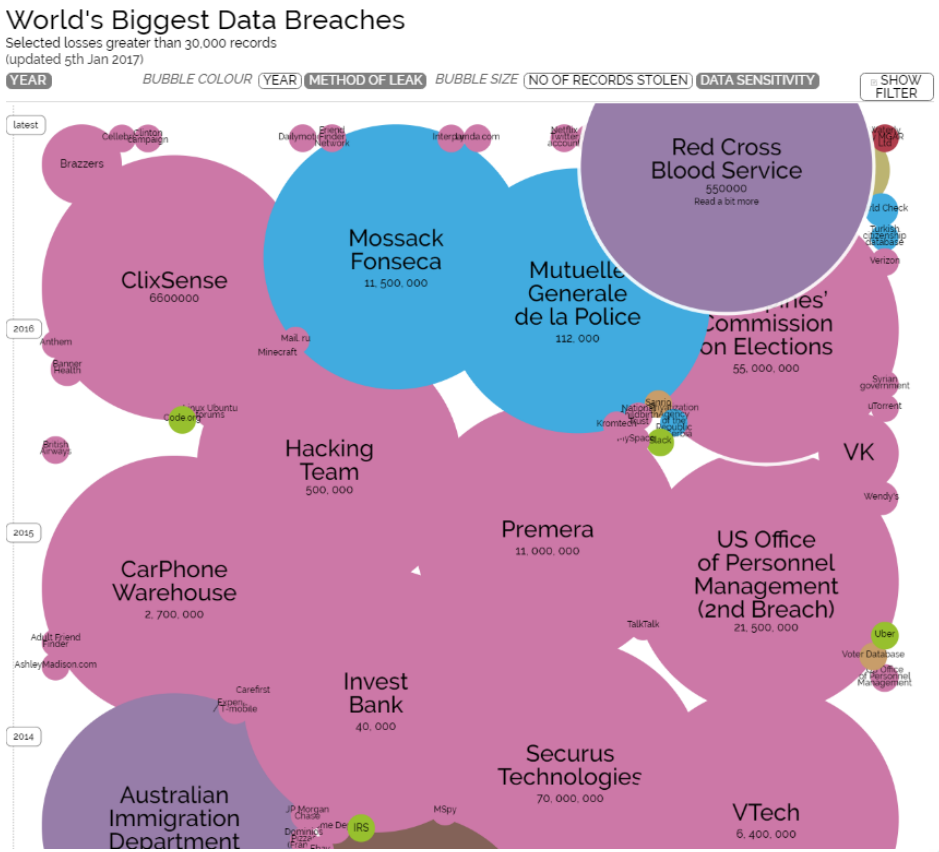
- Smart door lock
- Thermostats & HVAC
- Light & Switches
- Security & Cameras
- Mobile Phone

Smart Home

- Users not aware of log content and cannot turn off
- The thermostat bootup has backdoor - bypass verification
  - Can boot via USB and install any code
  - Can read log file that contains local Wifi credentials in plaintext
  - Can block sending log back to server
  - (Researchers @ University of Central Florida)

Reference:
https://www.blackhat.com/docs/us-14/materials/us-14-Jin-Smart-Nest-Thermostat-A-Smart-Spy-In-Your-Home.pdf

Data Breaches Incident



- Data leakage
- Tampering
- Blackmail
- Damage

Reference:
http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Security Attack in Smart Age

- Very wide attack surface
- Cyberattack can impact physical world
- More remote attack method
- Attack becomes complicated and difficult to track
- Massive data leakage
- Difficult to patch the system

Real case study

Real Case – Mirai (未来) Malware

- 20 September 2016 attack on the Krebs on Security site which reached 620 Gbps
- 21 October 2016 attack on Dyn DNS service
  - Amazon.com
  - BBC
  - PlayStation Network
  - etc

Mirai Malware


PCWorld
FROM IDG

NEWS

Chinese firm admits its hacked DVRs, cameras were behind Friday's massive DDOS attack

Botnets created from the Mirai malware were involved in Friday's cyber attack.

By Michael Kan | Follow

U.S. Correspondent, IDG News Service OCT 23, 2016 12:14 PM PT

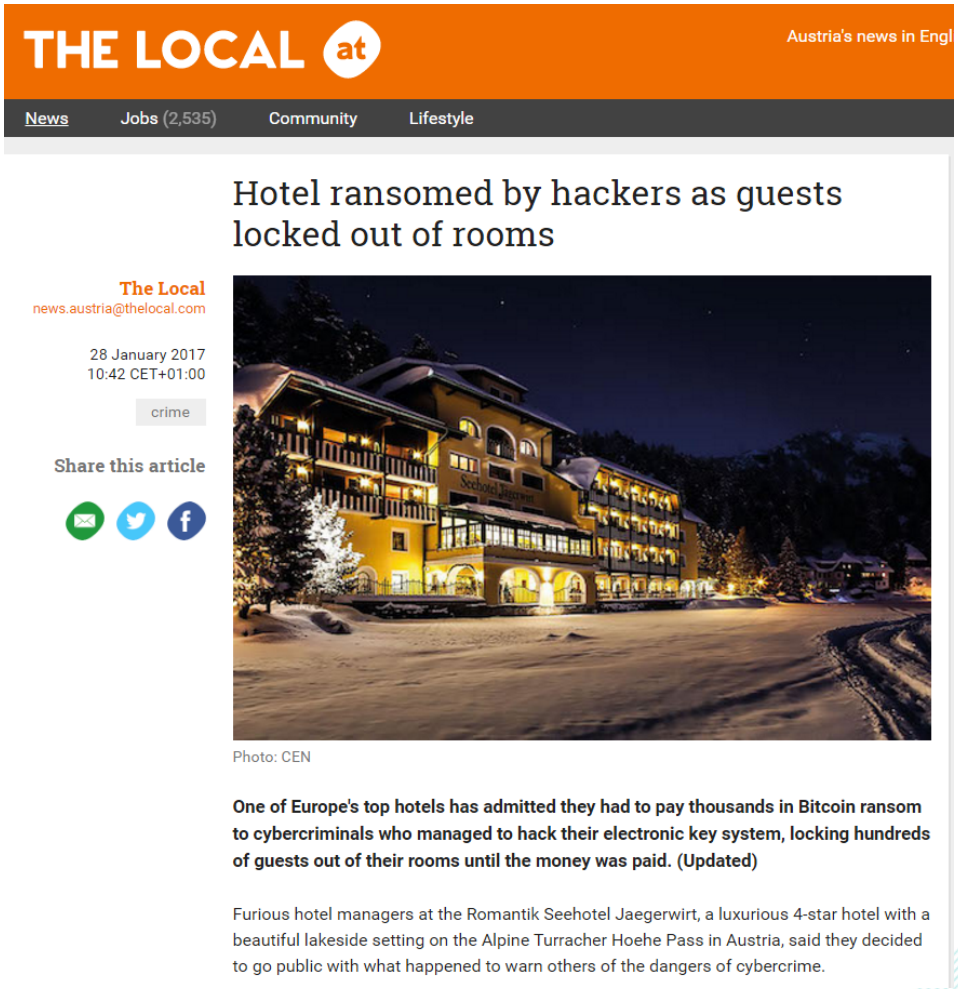
Credit: Downdetector

- 雄邁 (Xiongmai)
- DVR, IP Cam
- Use of hard-coded password
- Default Opened Telnet
- Can install program code

Problem

- Provide the back door for Development
- hard-coded password
- No provide firmware update to patch the device
- No provide security option to disable it

Real Case 2



THE LOCAL at

Austria's news in Engl

News Jobs (2,535) Community Lifestyle

Hotel ransomed by hackers as guests locked out of rooms

The Local
news.austria@thelocal.com

28 January 2017
10:42 CET+01:00

crime

Share this article

Photo: CEN

One of Europe's top hotels has admitted they had to pay thousands in Bitcoin ransom to cybercriminals who managed to hack their electronic key system, locking hundreds of guests out of their rooms until the money was paid. (Updated)

Furious hotel managers at the Romantik Seehotel Jaegerwirt, a luxurious 4-star hotel with a beautiful lakeside setting on the Alpine Turracher Hoehe Pass in Austria, said they decided to go public with what happened to warn others of the dangers of cybercrime.

- Romantik Seehotel Jaegerwirt
- 28 January 2017
- Hack their electronic key system
- ~~Locking hundreds of guests out of their rooms~~

Reference: *http://www.thelocal.at/20170128/hotel-ransomed-by-hackers-as-guests-locked-in-rooms*

Problem

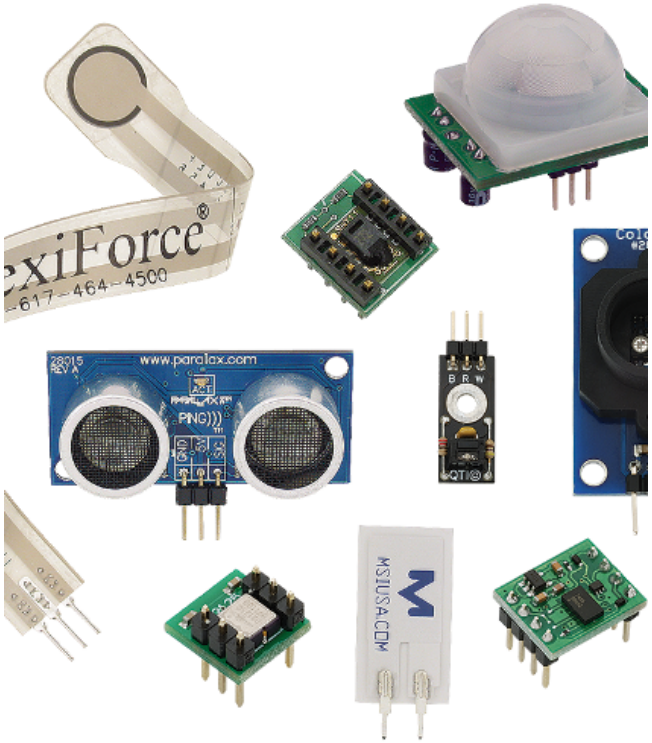
- Hacker take down the key card system.
- IT system and key card system is not separated
- 1,500 EUR (1,272 GBP) in Bitcoin was paid to hacker
- Hackers left a back door open in the system


THIS
HELPFUL

Smart System Safety from Design, Default & Implement

- Start from the design phase of the system
  - Involve the designers and engineers, the users and may be regulators if appropriate
- Shipping products with security by default
- Critical systems/networks should be isolated

Devices, Sensors and Controllers



- Firmware update
  - OTA
  - Schedule check
- Firmware
  - Firmware signing
  - Firmware verification
- No hard-coded Password
- No back door
- Easy to setup
- Provide security features and settings

Communication

- All communications should be encrypted
- Do not open inbound ports
- Implement token-based access control in publishing/subscription channel

- For Cloud API
  - Using secure and reliable communication protocols like MQTT, WebSockets, and HTTP/2

Management interface & Database

- Devices Authentication
- Access Control
- Encryption
- Isolation
- Assessment & Penetration test

Takeaway

- Cybersecurity risks/threats:
  - Your private life or office/shop sensitive information can be exposed in internet (e.g. IP camera, smart TV camera)
  - IoT device can also be a jumping board for breaching other devices / leaking your password.
  - Controlled and abused by cybercriminals to attack others (Mirai botnet)

Takeaway

- Protection of existing devices:
  - Change admin password of your devices (if you find out how).
  - Block unnecessary components, e.g. do you need to use the camera of your smart TV?
  - Check manufacturer website - any security update for the devices?

Takeaway

- With security in mind even before purchase
  (you may not have chance to change/update anything after the purchase)
  - Can change admin password?
  - Will security update be provided?
  - Provide other security features, e.g. encrypted data transfer?

Takeaway

- Cybersecurity awareness not only to avoid your loss, but also ensure you to be a ‘responsible’ internet user:
  - Insecure IP camera can become cybercriminal’s attack tool.

Useful resources

- OWASP Internet of Things Project

  https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project

- Internet of Things security best practices

  https://docs.microsoft.com/en-us/azure/iot-suite/iot-security-best-practices

- 13 Steps to Developing Secure IoT Products

  https://downloads.cloudsecurityalliance.org/assets/research/internet-of-things/future-proofing-the-connected-world.pdf

- IoT Security Blogs or Articles

  http://embedded-computing.com/topics/security/

Our study

- Some Home routers in Hong Kong prone to security issues

  https://www.hkcert.org/my_url/en/blog/15032502

  https://www.hkcert.org/my_url/en/blog/15052903

- Vulnerabilities in Hong Kong Internet Devices

  https://www.hkcert.org/my_url/en/blog/15073101

- Security Risks of Network-Attached Storages (NAS)

  https://www.hkcert.org/my_url/en/blog/15092401

- Security Risks of Networked Industrial Control System (ICS)

  https://www.hkcert.org/my_url/en/blog/15122402