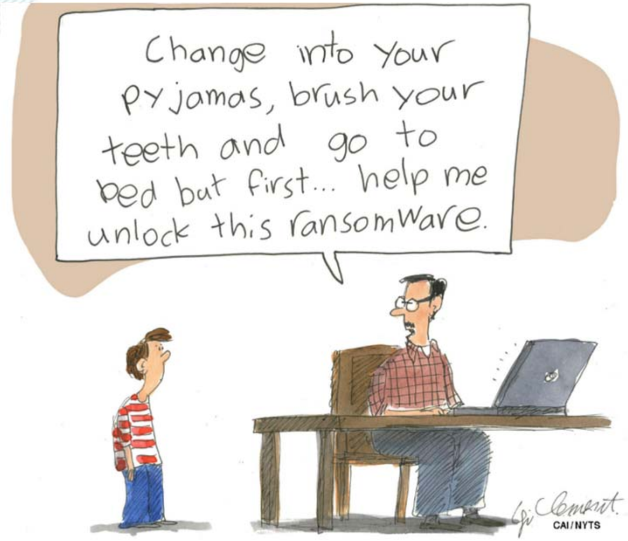
The Need of IoT Security Assessment

Bernard Kan
Senior Consultant
HKCERT

Agenda

- About HKCERT
- HKCERT Security Incident Report
- Potential Trend in 2018
- IoT Attacks & Security Assessment


Change into your pyjamas, brush your teeth and go to bed but first... help me unlock this ransomware.
CAI/NYTS

Hong Kong Computer Emergency Response Team Coordination Centre

HKCERT

香港電腦保安事故協調中心

- Established in 2001
- Funded by the HKSAR Government
- Operated by **Hong Kong Productivity Council (香港生產力促進局)**
- Mission
  - –As the coordination of local cyber security incidents, serving Internet Users and SMEs in Hong Kong
  - –As the Point of Contact of cyber security incidents across the border

HKCERT Services

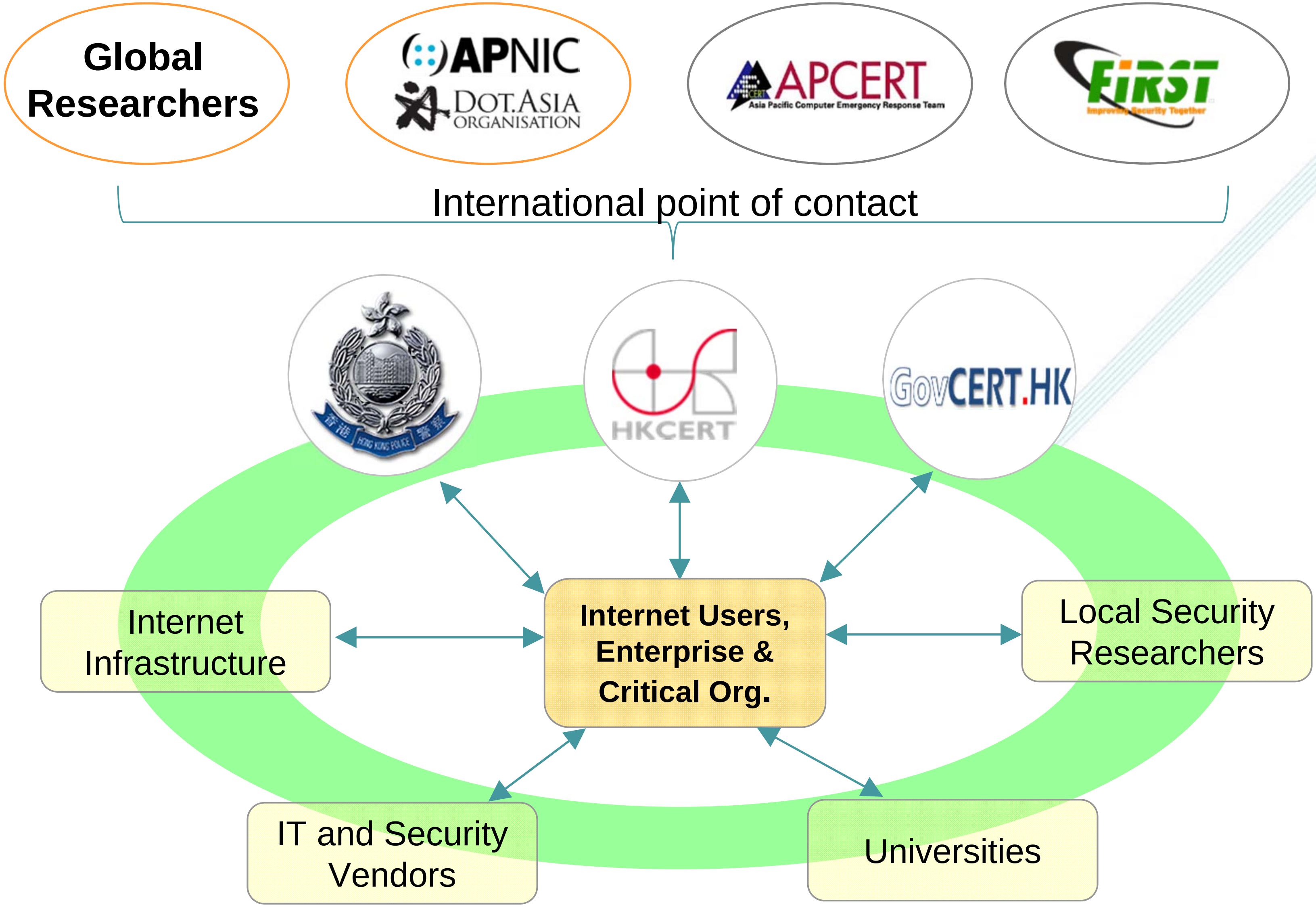
- Incident Report **24-hr Hotline**: 8105-6060

- Security Watch and Warning **Free subscription**

- Cross-border collaboration

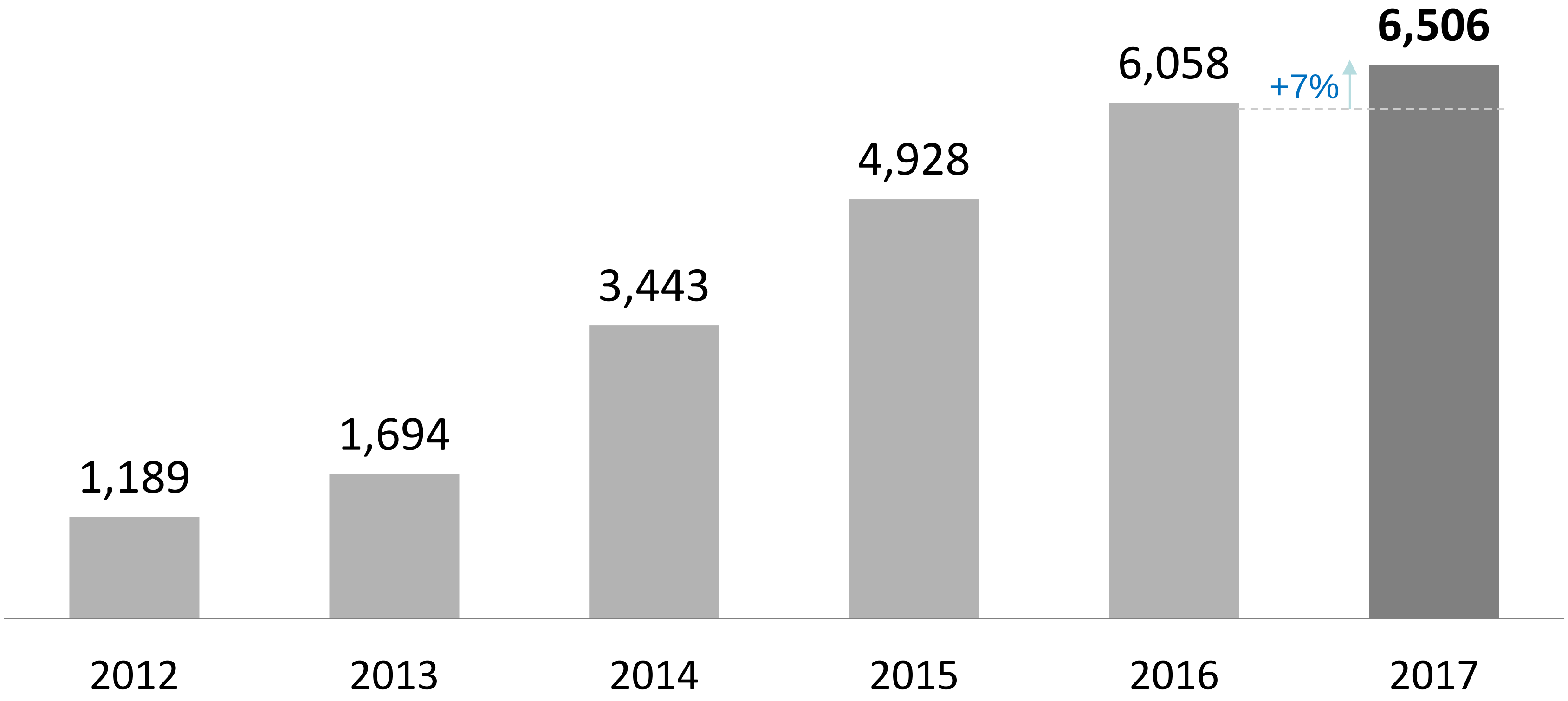
- Awareness education and guideline

As the Coordination Centre



Global Researchers
APNIC
DOT.ASIA ORGANISATION
APCERT
Asia Pacific Computer Emergency Response Team
FIRST
Improving Security Together
International point of contact
HONG KONG POLICE
HKCERT
GovCERT.HK
Internet Infrastructure
Internet Users, Enterprise & Critical Org.
Local Security Researchers
IT and Security Vendors
Universities

HKCERT Security Incident Reports
保安事故報告



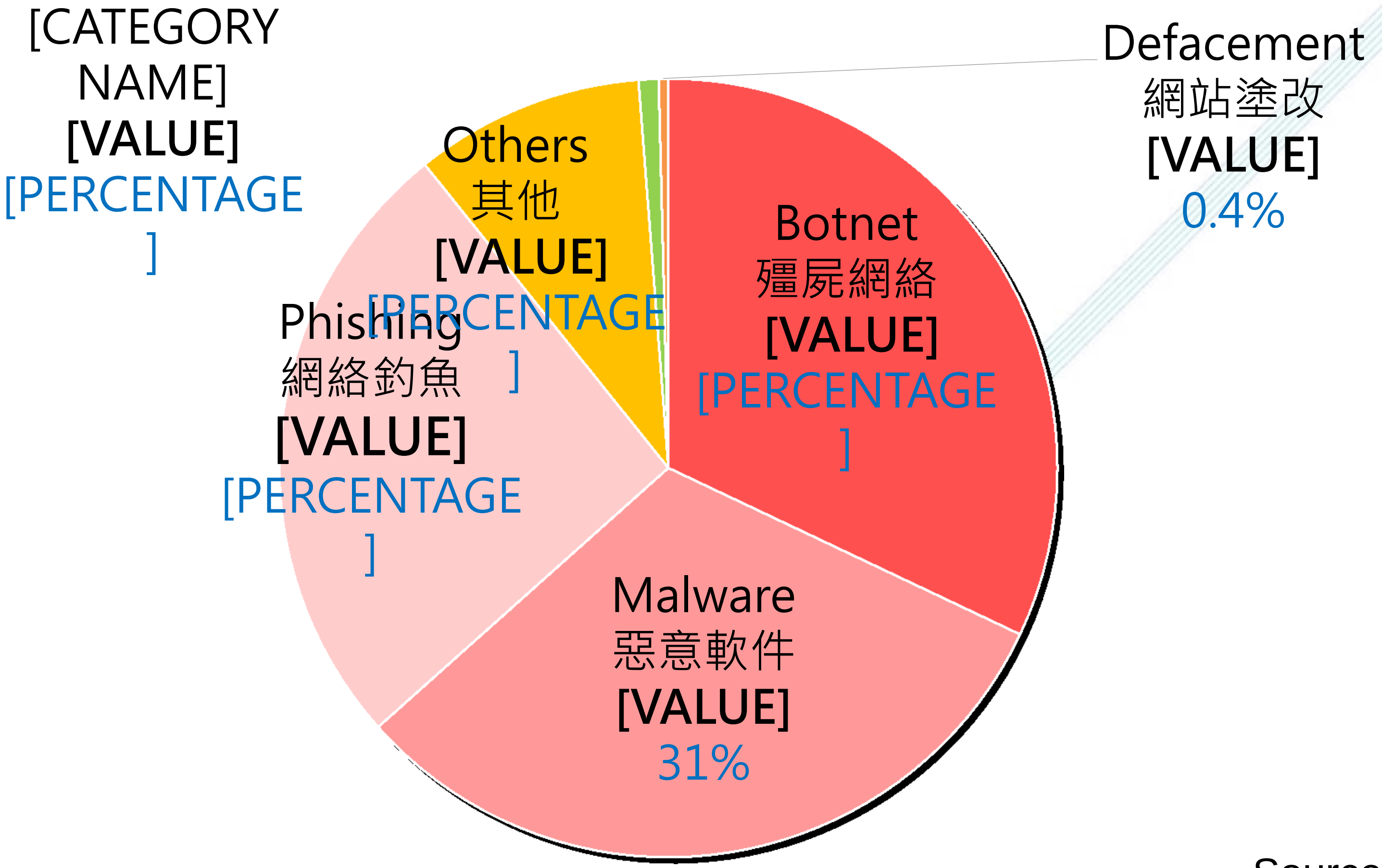
Referral cases with global collaboration accounted for **91%** of cases

與全球資訊保安機構合作, 2017年 **91%** 個案屬於轉介個案。

Source: HKCERT

HKCERT Incident Reports in 2017 by Type

Total : 6,506 (↑7%)



Source: HKCERT

Potential Trends in 2018

1. **Financially Motivated Cyber Crimes** continue to proliferate
   以榨取金錢為目標的網絡攻擊持續上升
2. **Internet of Things (IoT) attacks** on the Rise
   物聯網攻擊上升
3. **Mobile Payment Apps** as New Attack Targets
   流動付款程式或成為攻擊對象
4. **More Regulation** for Security and Privacy
   更多有關網絡安全和隱私的規管
5. **Supply Chain Attacks** bypass Enterprise Defense
   供應鏈攻擊繞過企業的防禦

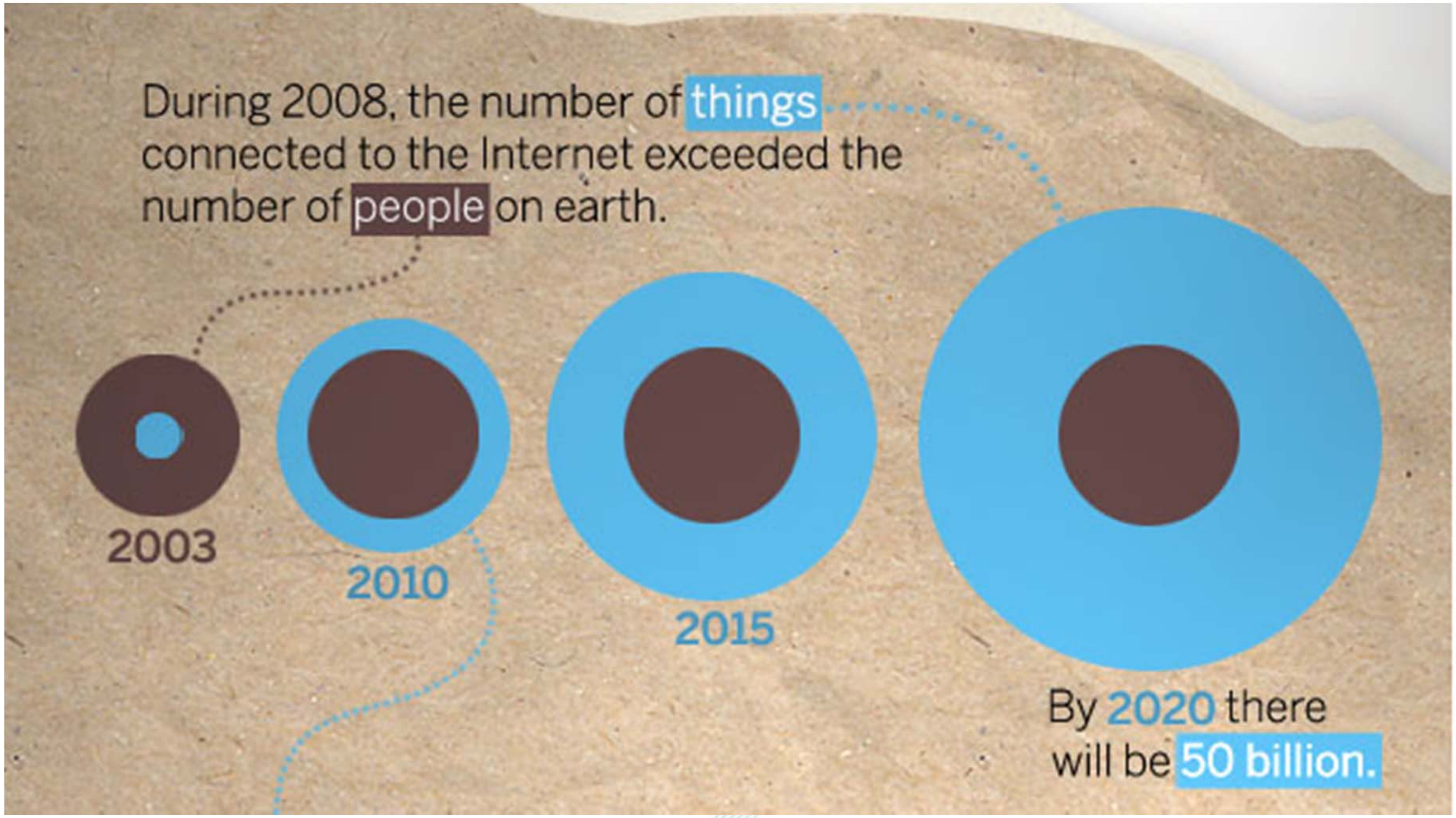
What is Internet of Things (IoT)?

- A network of physical objects that contain embedded tech to communicate, sense, and interact with internal states or external environment (Gartner)

- “Uniquely identifiable objects (things) and their virtual representations in an Internet-like structure.” (Wikipedia)

- More general, the Internet of Things as non-traditional personal computing devices connected to the Internet either directly or indirectly.

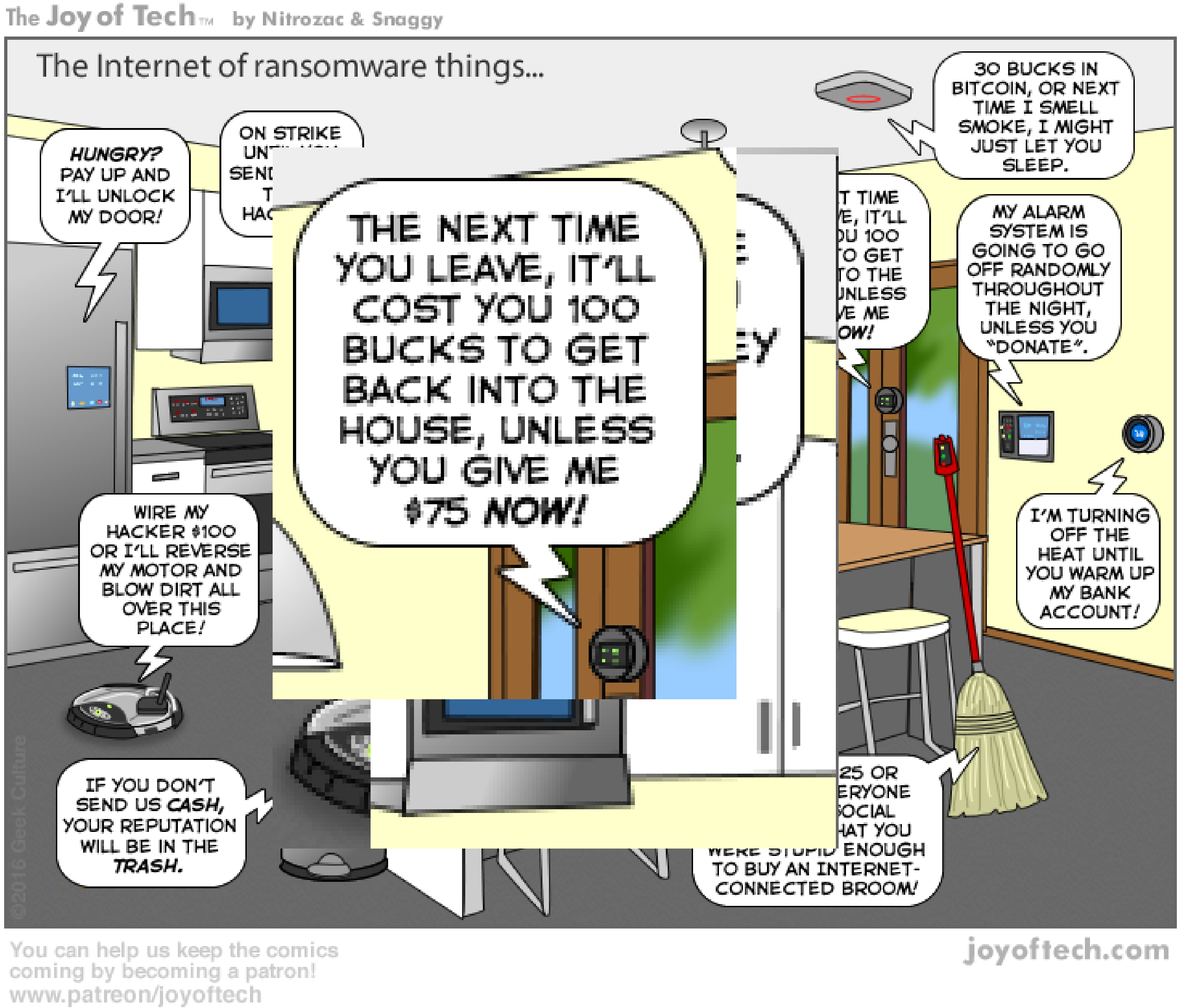
"Things" Connected to the Internet



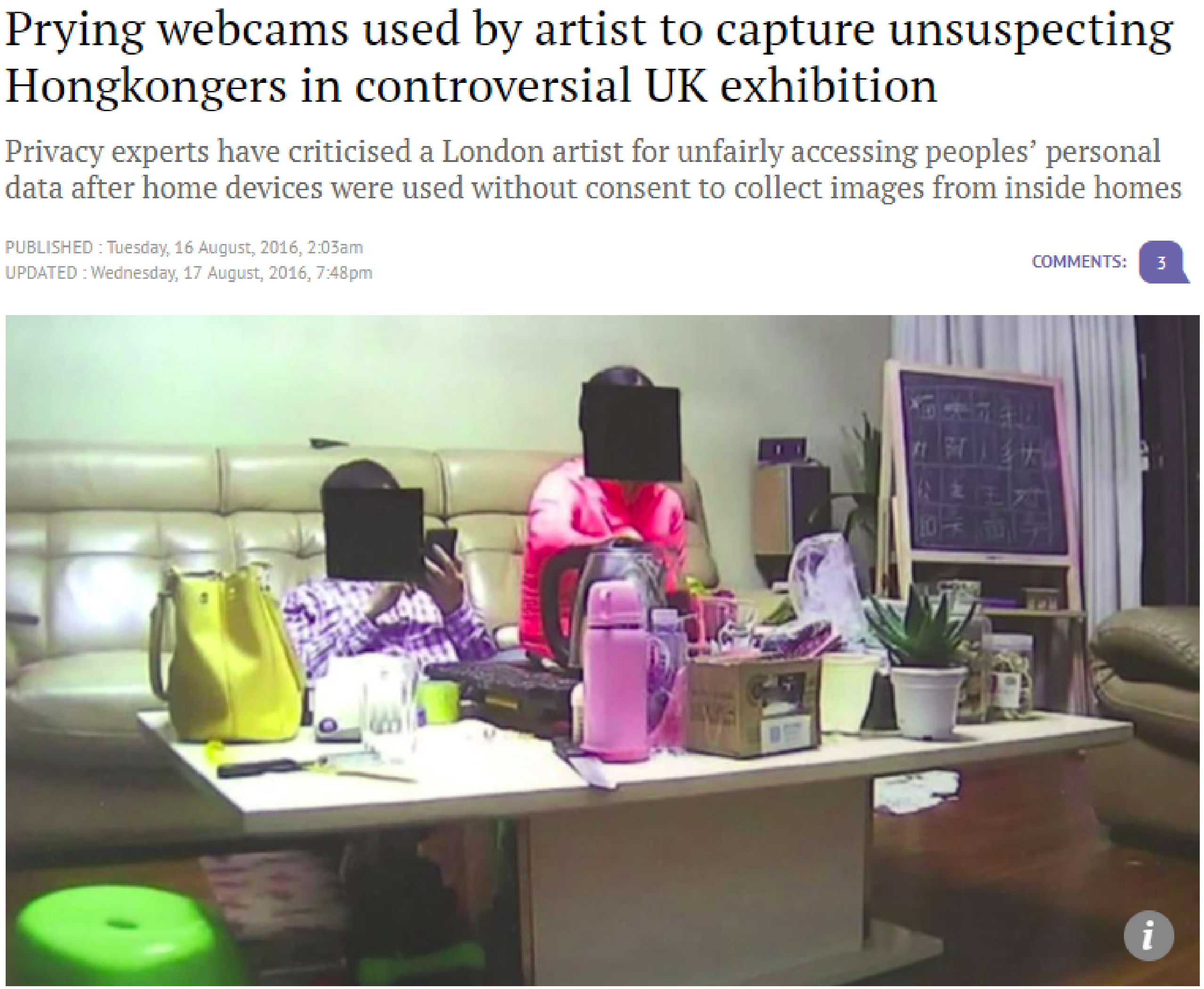
Source: CISCO

What Can Go Wrong with IoT?

What happen if IoTs were infected by ransomwares?


The Joy of Tech™ by Nitrozac & Snaggy
The Internet of ransomware things...
HUNGRY? PAY UP AND I'LL UNLOCK MY DOOR!
ON STRIKE UN... SEND ... T... HAC...
THE NEXT TIME YOU LEAVE, IT'LL COST YOU 100 BUCKS TO GET BACK INTO THE HOUSE, UNLESS YOU GIVE ME $75 NOW!
30 BUCKS IN BITCOIN, OR NEXT TIME I SMELL SMOKE, I MIGHT JUST LET YOU SLEEP.
MY ALARM SYSTEM IS GOING TO GO OFF RANDOMLY THROUGHOUT THE NIGHT, UNLESS YOU "DONATE".
WIRE MY HACKER $100 OR I'LL REVERSE MY MOTOR AND BLOW DIRT ALL OVER THIS PLACE!
I'M TURNING OFF THE HEAT UNTIL YOU WARM UP MY BANK ACCOUNT!
IF YOU DON'T SEND US CASH, YOUR REPUTATION WILL BE IN THE TRASH.
...25 OR ...ERYONE ...SOCIAL ...HAT YOU WERE STUPID ENOUGH TO BUY AN INTERNET-CONNECTED BROOM!
©2016 Geek Culture
You can help us keep the comics coming by becoming a patron! www.patreon/joyoftech
joyoftech.com

What Can Go Wrong with IoT?



Prying webcams used by artist to capture unsuspecting Hongkongers in controversial UK exhibition

Privacy experts have criticised a London artist for unfairly accessing peoples' personal data after home devices were used without consent to collect images from inside homes

PUBLISHED : Tuesday, 16 August, 2016, 2:03am
UPDATED : Wednesday, 17 August, 2016, 7:48pm

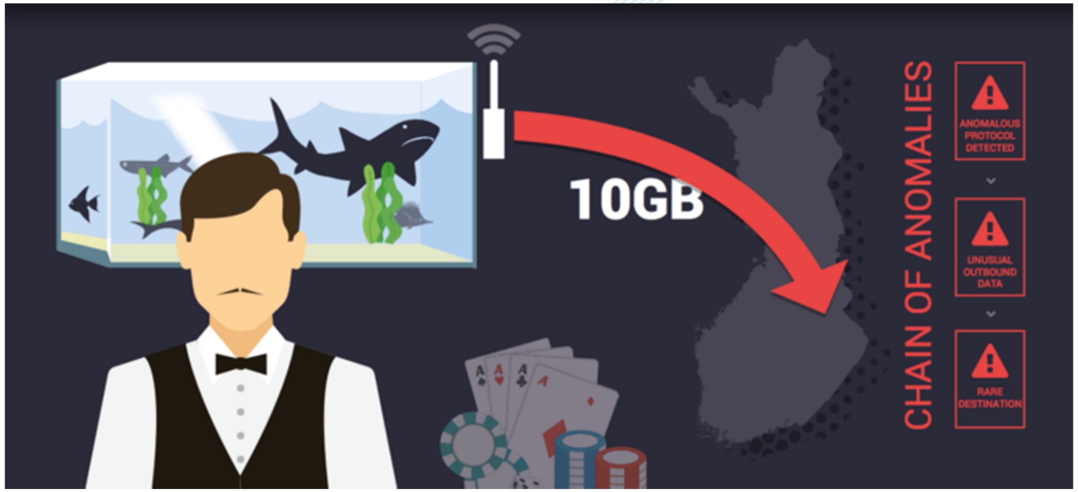
What Can Go Wrong with IoT?

TOYMAKER 'VTECH' HACKED!

4.8 Million Parents' Data & Images of Children Leaked

What Can Go Wrong with IoT?

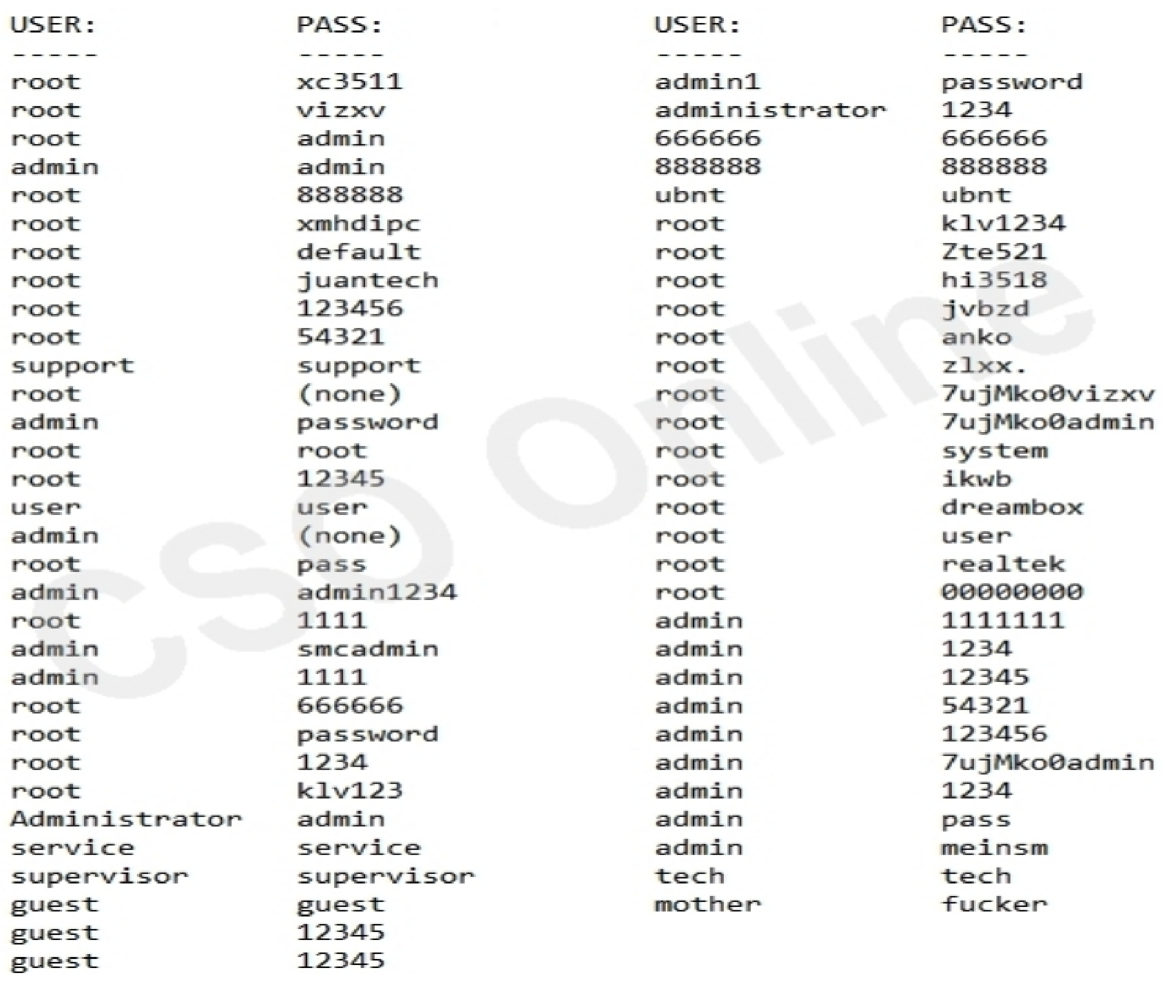
A Casino Was Hacked Thanks To The Internet Of Broken Things & A Fish Tank Thermometer



Mirai Botnet

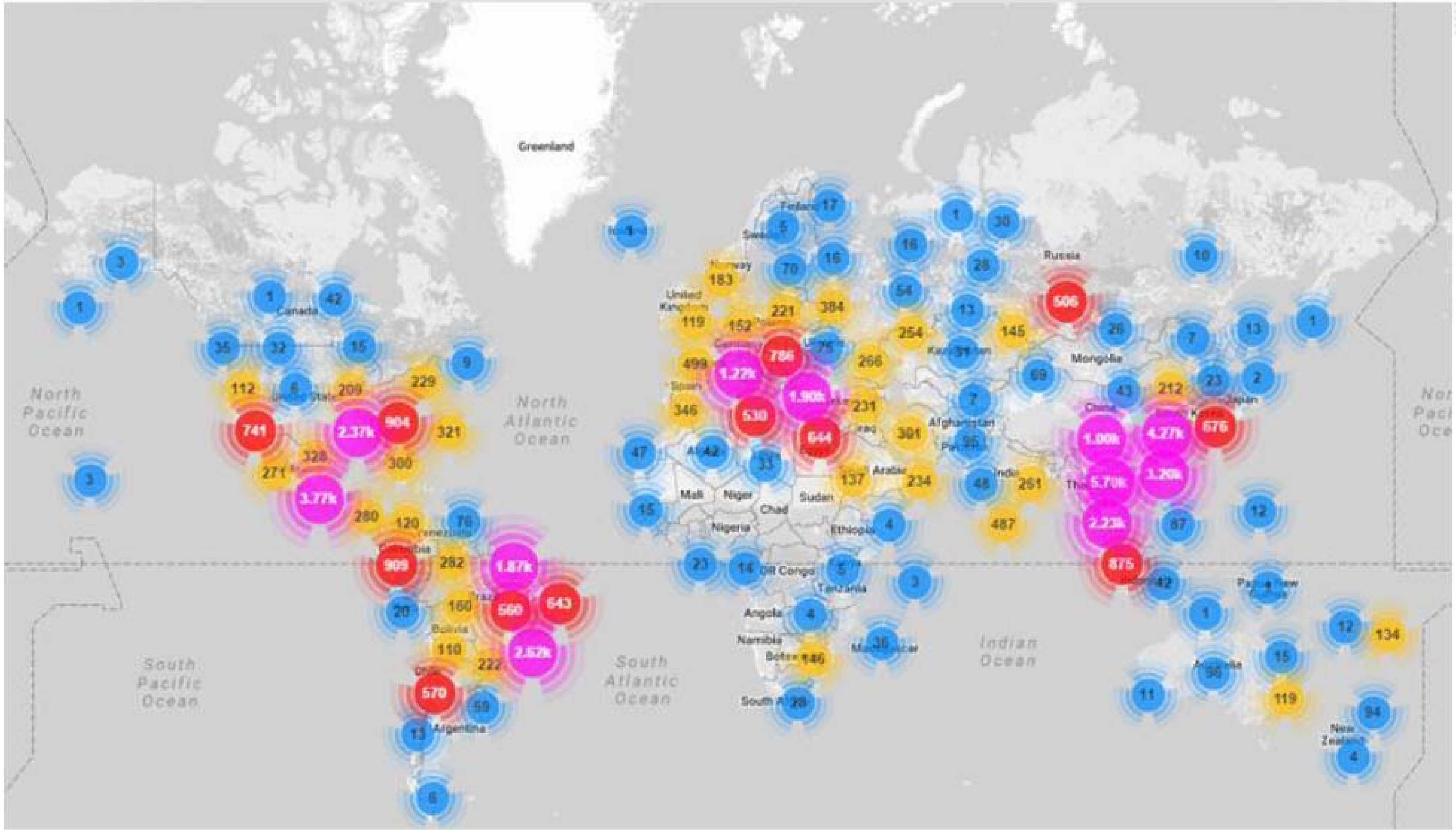
- Mirai is a piece of malware designed to launch multiple types of DDoS attacks
- The malware scans the internet for telnet servers then attempts to log in and infect them using a list of hard-coded passwords (most of which correspond to internet connected CCTV systems and routers)
- A botnets using the Mirai malware was responsible for the largest DDoS attack ever recorded, which peaked at 1.1 Tbps
- It exploits well-known hardcoded login credentials in IoT devices
- It uses segmented command-and-control which allows the botnet to launch simultaneous DDoS attacks against multiple, unrelated targets

Mirai Botnet



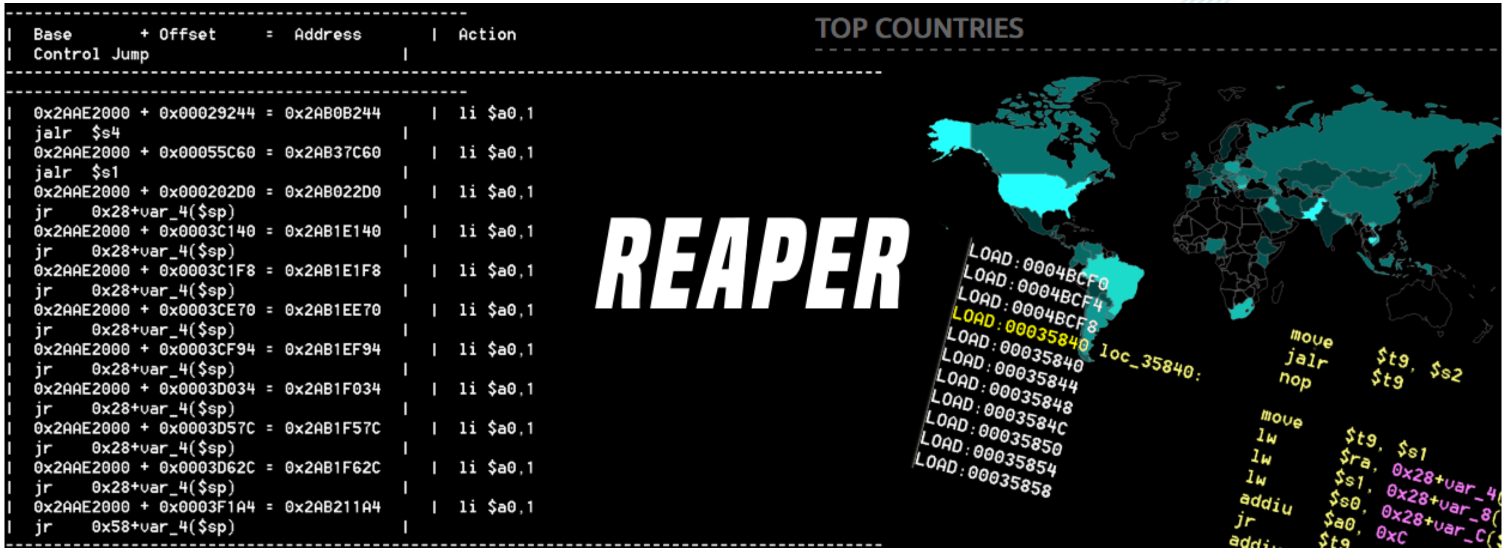
USER:	PASS:	USER:	PASS:
-----	-----	-----	-----
root	xc3511	admin1	password
root	vizxv	administrator	1234
root	admin	666666	666666
admin	admin	888888	888888
root	888888	ubnt	ubnt
root	xmhdipc	root	klv1234
root	default	root	Zte521
root	juantech	root	hi3518
root	123456	root	jvbzd
root	54321	root	anko
support	support	root	zlxx.
root	(none)	root	7ujMko0vizxv
admin	password	root	7ujMko0admin
root	root	root	system
root	12345	root	ikwb
user	user	root	dreambox
admin	(none)	root	user
root	pass	root	realtek
admin	admin1234	root	00000000
root	1111	admin	1111111
admin	smcadmin	admin	1234
admin	1111	admin	12345
root	666666	admin	54321
root	password	admin	123456
root	1234	admin	7ujMko0admin
root	klv123	admin	1234
Administrator	admin	admin	pass
service	service	admin	meinsm
supervisor	supervisor	tech	tech
guest	guest	mother	fucker
guest	12345		
guest	12345		

Geo-Locations of Mirai infected IoT Devices



The Reaper Botnet

- A new Botnet relying on more sophisticated takeover techniques
  - Spreads via nine different IoT vulnerabilities
- At least partially based on Mirai code
- Reports of up to 3.5 million infected devices
- Currently dormant: intention unknown
- Reaper includes an update mechanism



```
----------------------------------------------
|  Base       + Offset     =  Address       |  Action
|  Control Jump                            |
----------------------------------------------------------------------------------------
----------------------------------------------
|  0x2AAE2000 + 0x00029244 = 0x2AB0B244     |  li $a0,1
|  jalr  $s4                               |
|  0x2AAE2000 + 0x00055C60 = 0x2AB37C60     |  li $a0,1
|  jalr  $s1                               |
|  0x2AAE2000 + 0x000202D0 = 0x2AB022D0     |  li $a0,1
|  jr     0x28+var_4($sp)                  |
|  0x2AAE2000 + 0x0003C140 = 0x2AB1E140     |  li $a0,1
|  jr     0x28+var_4($sp)                  |
|  0x2AAE2000 + 0x0003C1F8 = 0x2AB1E1F8     |  li $a0,1
|  jr     0x28+var_4($sp)                  |
|  0x2AAE2000 + 0x0003CE70 = 0x2AB1EE70     |  li $a0,1
|  jr     0x28+var_4($sp)                  |
|  0x2AAE2000 + 0x0003CF94 = 0x2AB1EF94     |  li $a0,1
|  jr     0x28+var_4($sp)                  |
|  0x2AAE2000 + 0x0003D034 = 0x2AB1F034     |  li $a0,1
|  jr     0x28+var_4($sp)                  |
|  0x2AAE2000 + 0x0003D57C = 0x2AB1F57C     |  li $a0,1
|  jr     0x28+var_4($sp)                  |
|  0x2AAE2000 + 0x0003D62C = 0x2AB1F62C     |  li $a0,1
|  jr     0x28+var_4($sp)                  |
|  0x2AAE2000 + 0x0003F1A4 = 0x2AB211A4     |  li $a0,1
|  jr     0x58+var_4($sp)                  |
----------------------------------------------------------------------------------------
```

```
LOAD:0004BCF0
LOAD:0004BCF4
LOAD:0004BCF8
LOAD:00035840 loc_35840:
LOAD:00035840                 move
LOAD:00035844                 jalr     $t9, $s2
LOAD:00035848                 nop      $t9
LOAD:0003584C
LOAD:00035850                 move
LOAD:00035854                 lw       $t9, $s1
LOAD:00035858                 lw       $ra, 0x28+var_4(
                              lw       $s1, 0x28+var_8(
                              addiu    $s0, 0x28+var_C(
                              jr       $a0, 0xC
                              addi     $t9
```

VPNFilter: New Router Malware with Destructive Capabilities

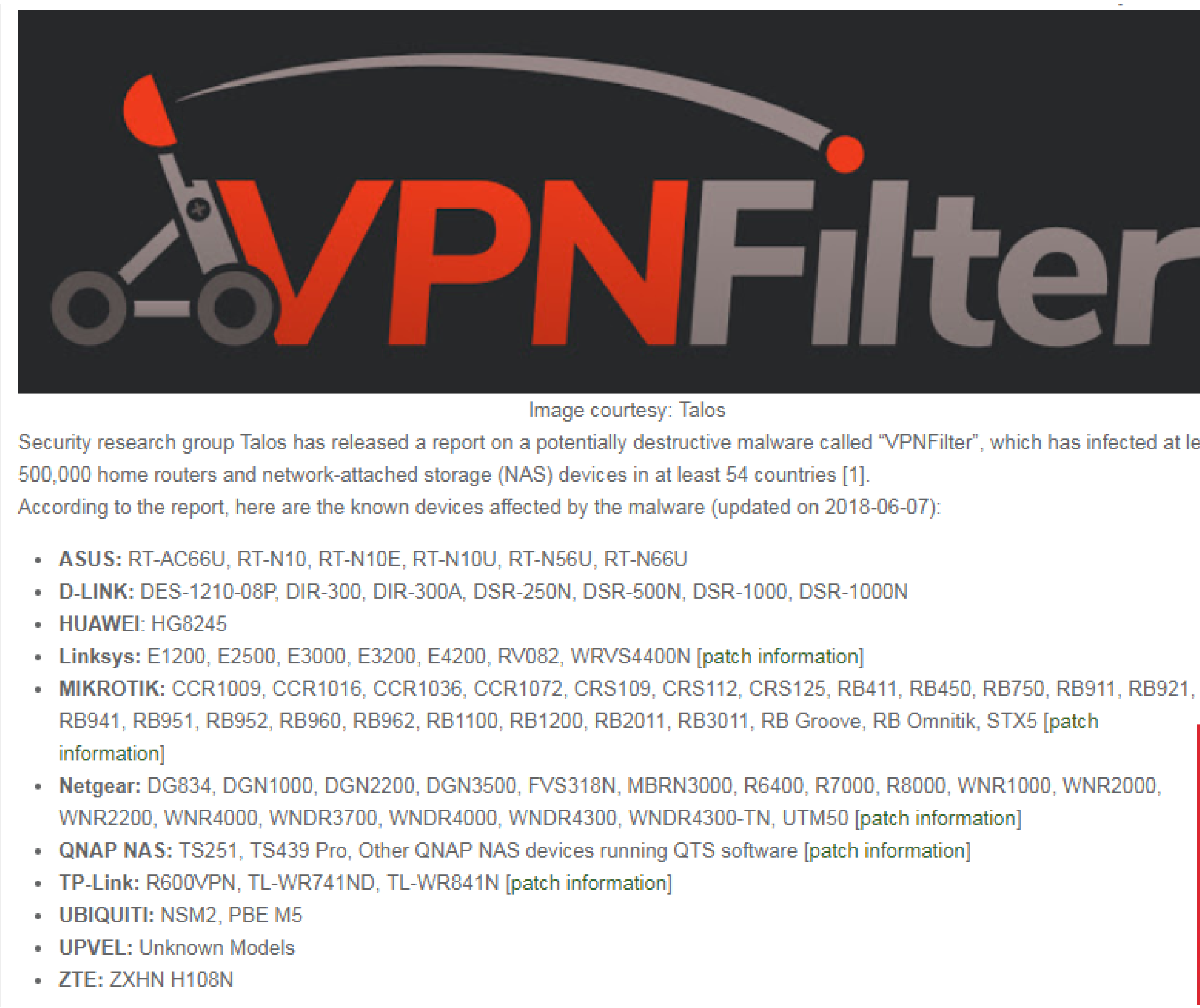


Image courtesy: Talos

Security research group Talos has released a report on a potentially destructive malware called "VPNFilter", which has infected at least 500,000 home routers and network-attached storage (NAS) devices in at least 54 countries [1].

According to the report, here are the known devices affected by the malware (updated on 2018-06-07):

- **ASUS:** RT-AC66U, RT-N10, RT-N10E, RT-N10U, RT-N56U, RT-N66U
- **D-LINK:** DES-1210-08P, DIR-300, DIR-300A, DSR-250N, DSR-500N, DSR-1000, DSR-1000N
- **HUAWEI**: HG8245
- **Linksys:** E1200, E2500, E3000, E3200, E4200, RV082, WRVS4400N [patch information]
- **MIKROTIK:** CCR1009, CCR1016, CCR1036, CCR1072, CRS109, CRS112, CRS125, RB411, RB450, RB750, RB911, RB921, RB941, RB951, RB952, RB960, RB962, RB1100, RB1200, RB2011, RB3011, RB Groove, RB Omnitik, STX5 [patch information]
- **Netgear:** DG834, DGN1000, DGN2200, DGN3500, FVS318N, MBRN3000, R6400, R7000, R8000, WNR1000, WNR2000, WNR2200, WNR4000, WNDR3700, WNDR4000, WNDR4300, WNDR4300-TN, UTM50 [patch information]
- **QNAP NAS:** TS251, TS439 Pro, Other QNAP NAS devices running QTS software [patch information]
- **TP-Link:** R600VPN, TL-WR741ND, TL-WR841N [patch information]
- **UBIQUITI:** NSM2, PBE M5
- **UPVEL:** Unknown Models
- **ZTE:** ZXHN H108N

Why IoT Devices are so vulnerable?

- There’s poor or non-existent security built into the device itself
- The device is directly exposed to the Internet because of poor network segmentation
- There’s un-needed functionality left in OS based on generic and often Linux-derivative hardware & software
- Default credentials are often hard coded
- Security patches deployment is difficult

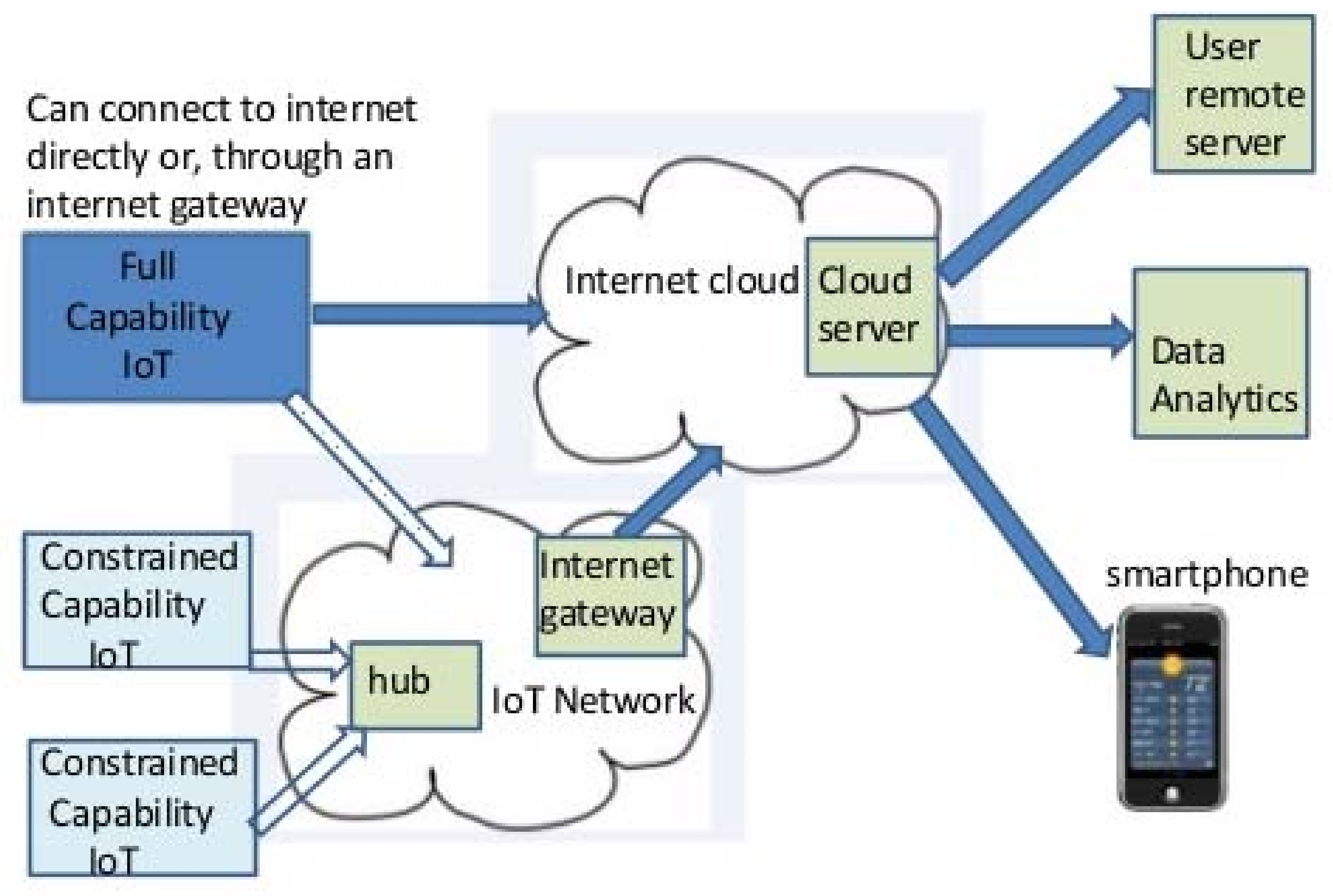
Consumers and Business - How to Protect IoTs

- Evaluate if the devices you are bringing into your network really need to be smart. It's better to treat IoT tech as hostile by default.
- Segment the network
- Change the default credentials
- Apply patches and update whenever possible

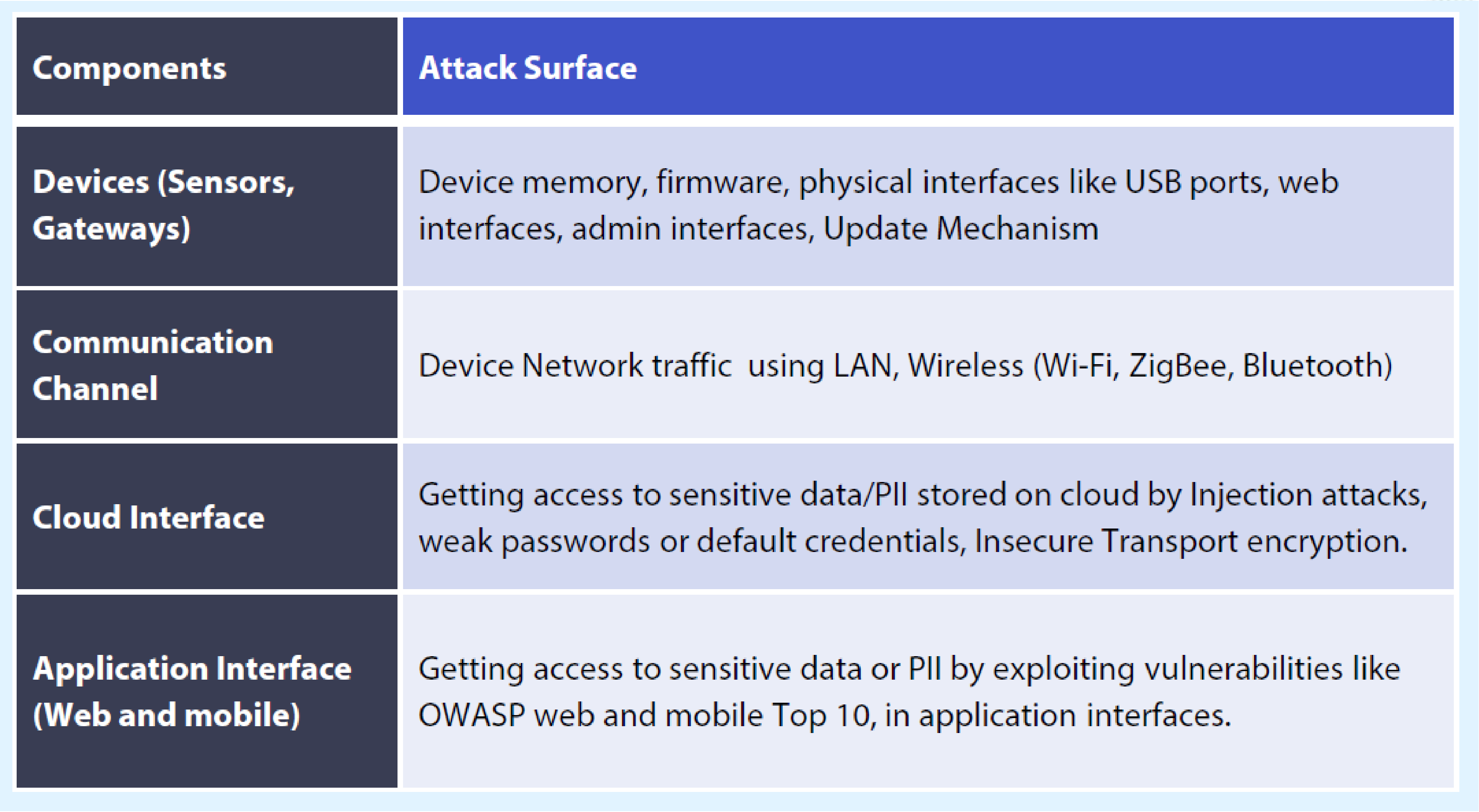
Developer Actions to Protect IoTs

- Have a red team audit the devices prior to commercial release.
- Force a credential change at the point of setup. (i.e., Devices will not work unless the default credentials are modified.)
- Require https if there’s web access
- Remove unneeded functionality
- Provide mechanism for product update
- Security by design

A Simplified IoT Architecture



IoT Components Attack Surface



Components	Attack Surface
Devices (Sensors, Gateways)	Device memory, firmware, physical interfaces like USB ports, web interfaces, admin interfaces, Update Mechanism
Communication Channel	Device Network traffic using LAN, Wireless (Wi-Fi, ZigBee, Bluetooth)
Cloud Interface	Getting access to sensitive data/PII stored on cloud by Injection attacks, weak passwords or default credentials, Insecure Transport encryption.
Application Interface (Web and mobile)	Getting access to sensitive data or PII by exploiting vulnerabilities like OWASP web and mobile Top 10, in application interfaces.

OWASP IoT Project

- OWASP - Open community organization focused on improving security of software
- Internet of Things project
  - –Help manufacturers, developers, and consumers better understand the security issues associated with IoT
  - –Enable users in any context to make better security decisions when building, deploying, or assessing IoT technologies
  - –https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- Provides Information on:
  - –Attack Surface Areas, Testing Guides, Principles of IoT Security, Security Guidance, IoT Vulnerabilities, Firmware Analysis, Design Principles, ICS/SCADA Software Weaknesses, etc.

OWASP IoT Top 10

Category	IoT Security Consideration	Recommendations
I1: Insecure Web Interface	•Ensure that any web interface coding is written to prevent the use of weak passwords …	When building a web interface consider implementing lessons learned from web application security. Employ a framework that utilizes security …
I2: Insufficient Authentication/Authorization	•Ensure that applications are written to require strong passwords where authentication is needed …	Refer to the OWASP Authentication Cheat Sheet
I3: Insecure Network Services	•Ensure applications that use network services don't respond poorly to buffer overflow, fuzzing …	Try to utilize tested, proven, networking stacks and interfaces that handle exceptions gracefully...
I4: Lack of Transport Encryption	•Ensure all applications are written to make use of encrypted communication between devices…	Utilize encrypted protocols wherever possible to protect all data in transit…
I5: Privacy Concerns	•Ensure only the minimal amount of personal information is collected from consumers …	Data can present unintended privacy concerns when aggregated…
I6: Insecure Cloud Interface	•Ensure all cloud interfaces are reviewed for security vulnerabilities (e.g. API interfaces and cloud-based web interfaces) …	Cloud security presents unique security considerations, as well as countermeasures. Be sure to consult your cloud provider about options for security mechanisms…
I7: Insecure Mobile Interface	•Ensure that any mobile application coding is written to disallows weak passwords …	Mobile interfaces to IoT ecosystems require targeted security. Consult the OWASP Mobile …
I8: Insufficient Security Configurability	•Ensure applications are written to include password security options (e.g. Enabling 20 character passwords or enabling two-factor authentication)…	Security can be a value proposition. Design should take into consideration a sliding scale of security requirements…
I9: Insecure Software/Firmware	•Ensure all applications are written to include update capability and can be updated quickly …	Many IoT deployments are either brownfield and/or have an extremely long deployment cycle...
I10: Poor Physical Security	•Ensure applications are written to utilize a minimal number of physical external ports (e.g. USB ports) on the device…	Plan on having IoT edge devices fall into malicious hands...

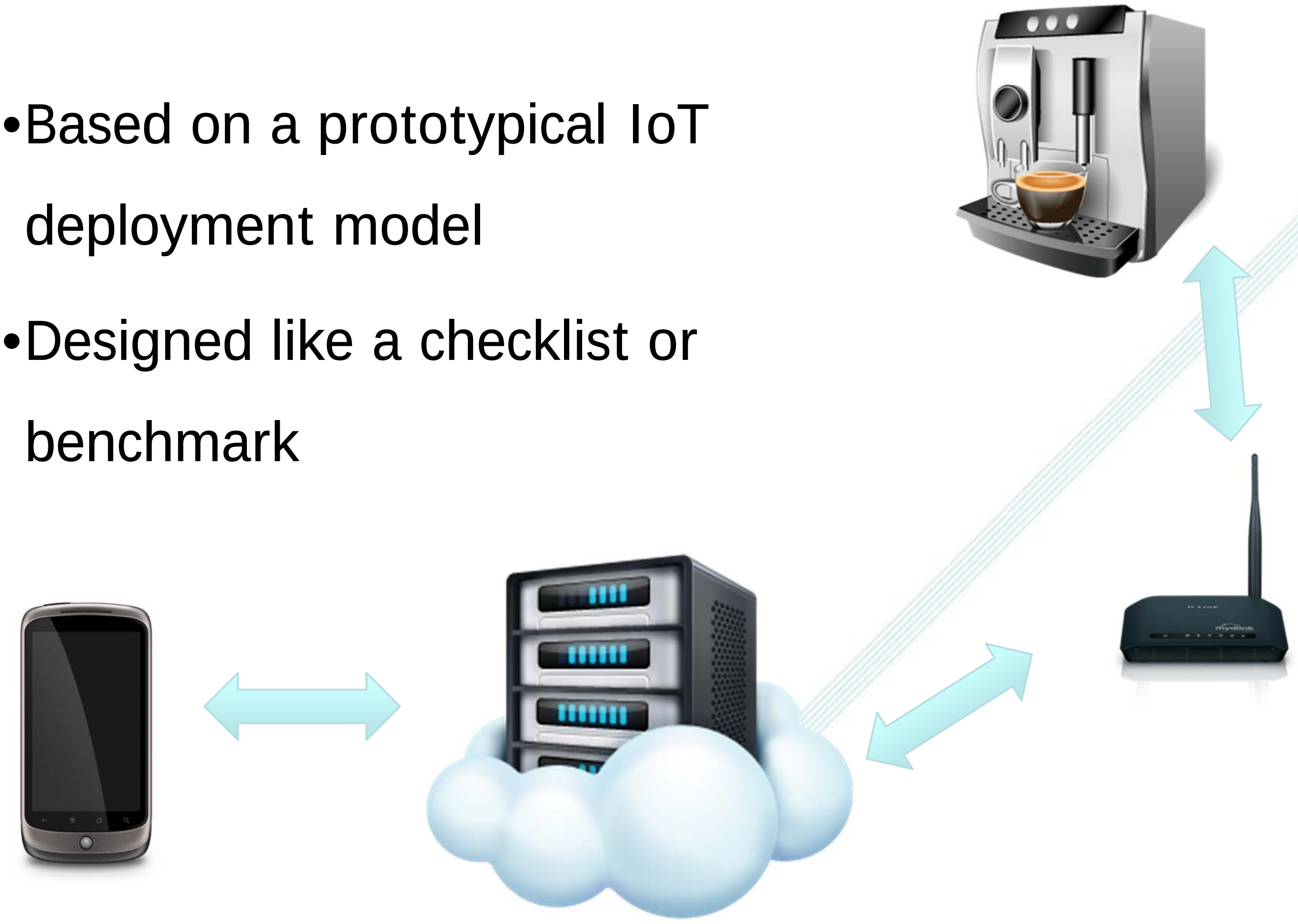
Principles of IoT Security

- Assume a hostile edge
- Test for scale
- Internet of lies
- Exploit autonomy
- Expect isolation
- Protect uniformly
- Encryption is tricky
- System hardening

- Limit what you can
- Lifecycle support
- Data in aggregate is unpredictable
- Plan for the worst
- The long haul
- Attackers target weakness
- Transitive ownership
- N:N Authentication

Framework assessment

- Based on a prototypical IoT deployment model
- Designed like a checklist or benchmark



Example Edge Considerations

- Are communications encrypted?
- Is storage encrypted?
- How is logging performed?
- Is there an updating mechanism?
- Are there default passwords?
- What are the offline security features?
- Is transitive ownership addressed?

Example Gateway Considerations

- Is encryption interrupted?
- Is there replay and denial of service defensive capabilities?
- Is there local storage? Is it encrypted?
- Is there anomaly detection capability?
- Is there logging and alerting?

Example Cloud Considerations

- Is there a secure web interface?
- Is there data classification and segregation?
- Is there security event reporting?
- How are 3rd party components tracked/updated?
- Is there an audit capability?
- Is there interface segregation?
- Is there complex, multifactor authentication allowed?

Example Mobile Considerations

- What countermeasures are in place for theft or loss of device?
- Does the mobile authentication degrade other component security?
- Is local storage done securely?
- Is there an audit trail of mobile interactions?
- Can mobile be used to enhance authentication for other components?

Summary

- Internet of Things (IoT) attacks are expected to rise as number of IoT devices continue to grow in coming years
- Securing IoT devices may be difficult due to constraints of hardware & software
- Consumers and business need to consider their real needs in selecting IoT devices and secure the devices as far as possible
- IoT developers and manufacturers need to adopt a security by design approach
- There are needs for a framework and systematic approach of assessing IoT devices before launching in the market

Q&A

HKCERT Hotline: 81056060

www.hkcert.org