Who needs IoT security?

Marc Witteman

November 7, 2018

D&E event

Outline

1. What is IoT?
2. Is IoT security important?
3. Case study
4. What's next?

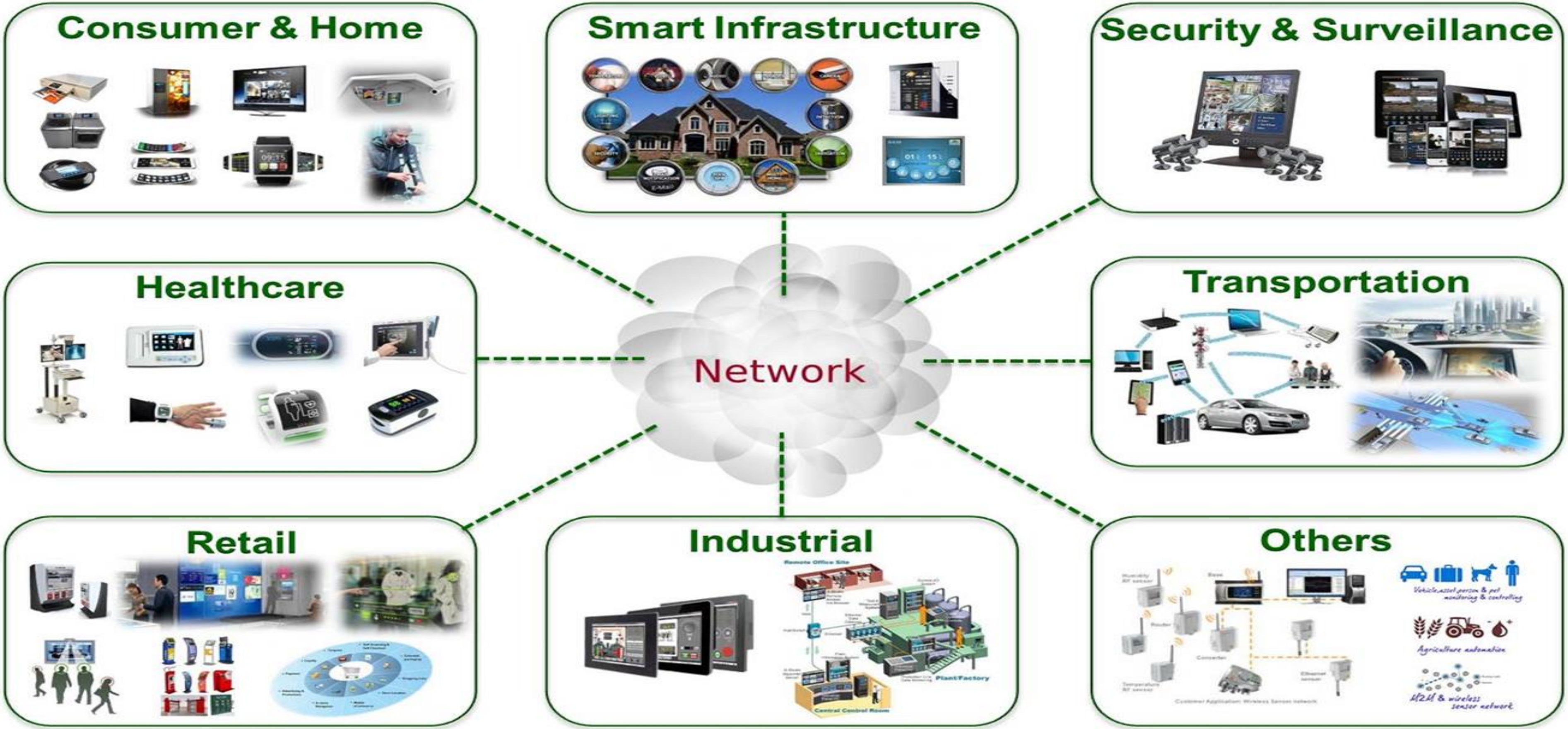
What’s new in internet?

- **Traditional internet**
  - connects people with machines
  - shares data that people create

- **IoT (Internet of Things)**
  - connects machines to machines
  - shares data that machines create

Public

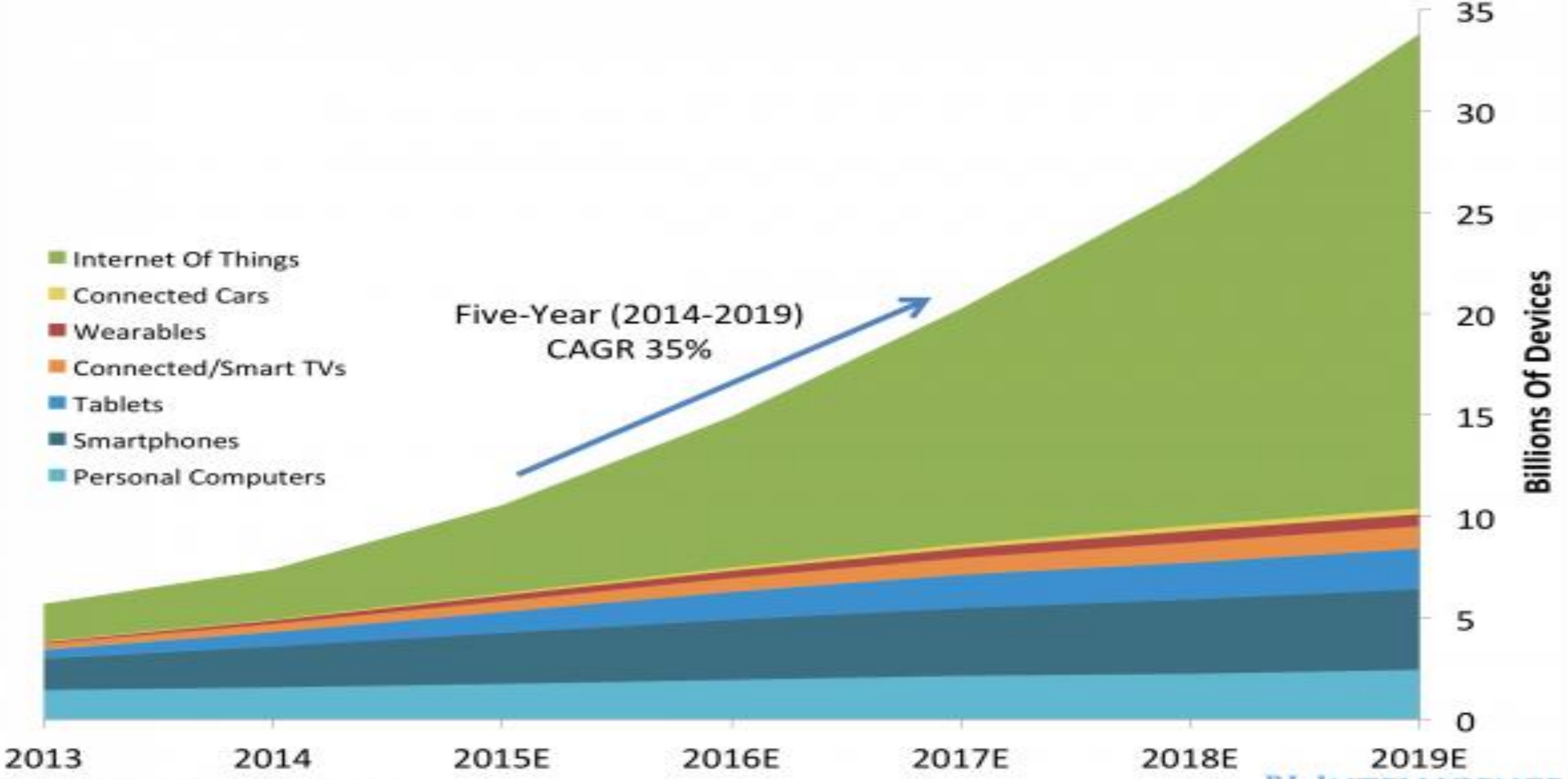
What is the Internet of Things?



Restricted

Source: Vivante

Number Of Devices In The Internet Of Everything

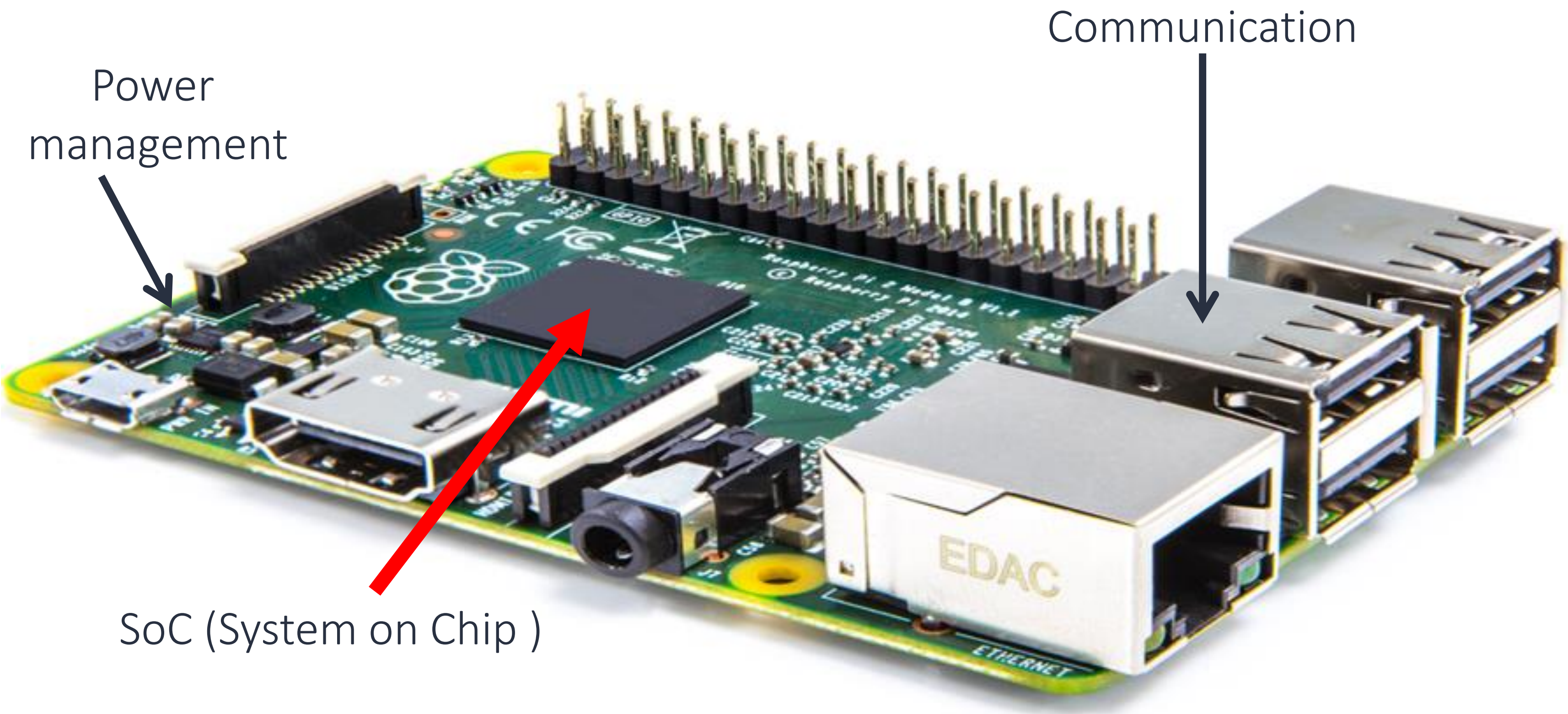


Five-Year (2014-2019)
CAGR 35%

Source: BI Intelligence Estimates

BI INTELLIGENCE

IoT example

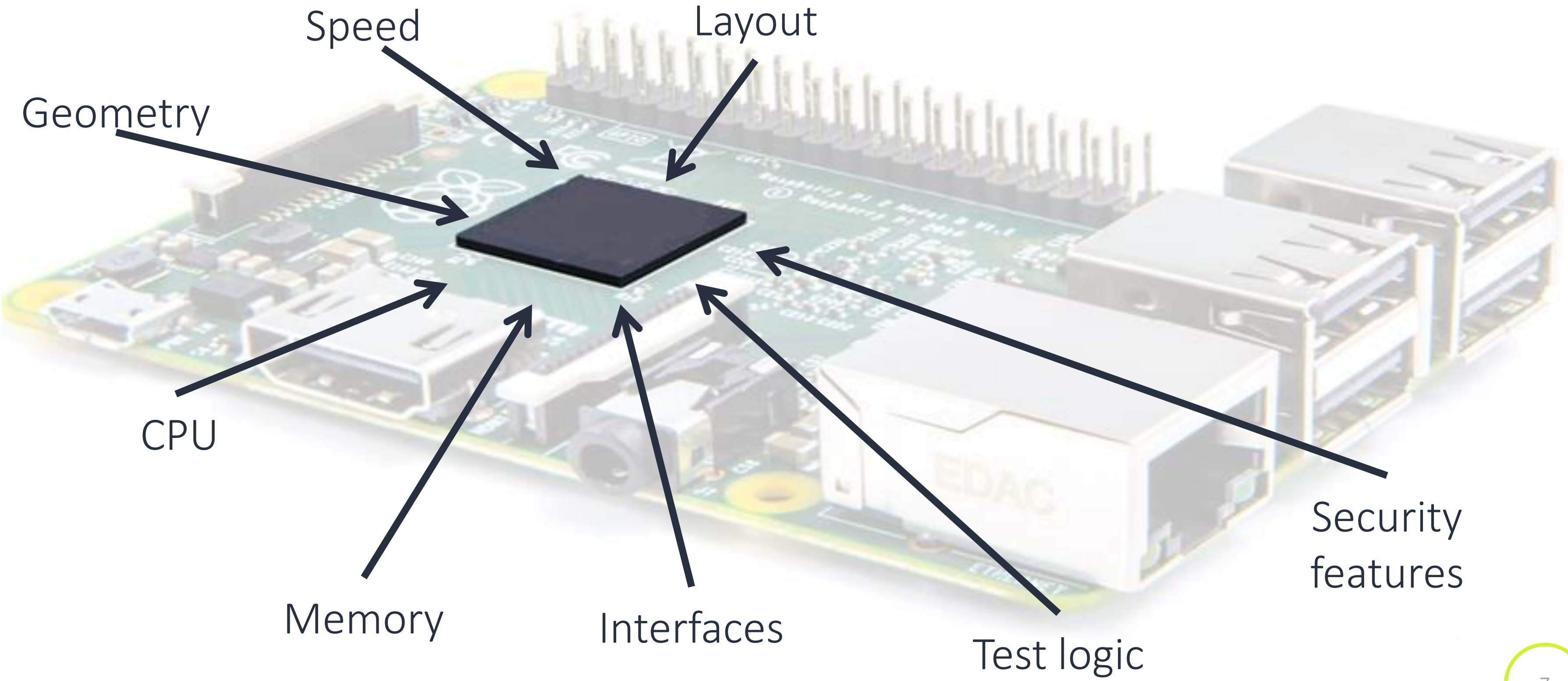


Communication

Power management

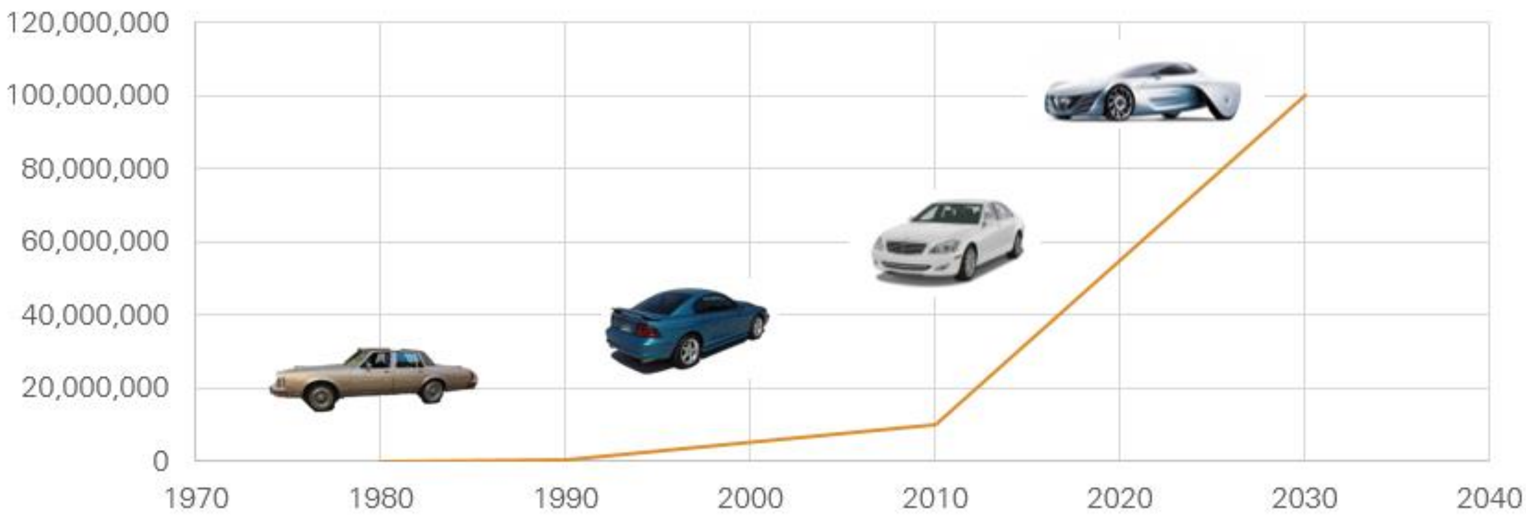
SoC (System on Chip)

Security is all about the chip



SOFTWARE COMPLEXITY IN AUTOMOTIVE

Lines of Code



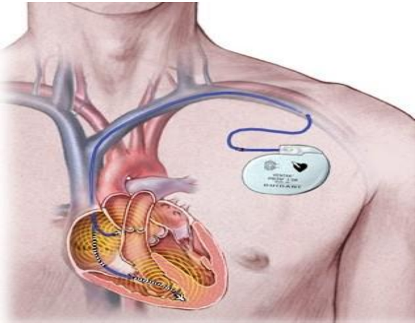
Outline

1. What is IoT?
2. Is IoT security important?
3. Case study
4. What's next?

Is IoT security important?

Remote car hijack

Medical device disturbance



Smart lock bypass

Identity theft

Premium content theft

CROSSING AN INTERSECTION IN 2028

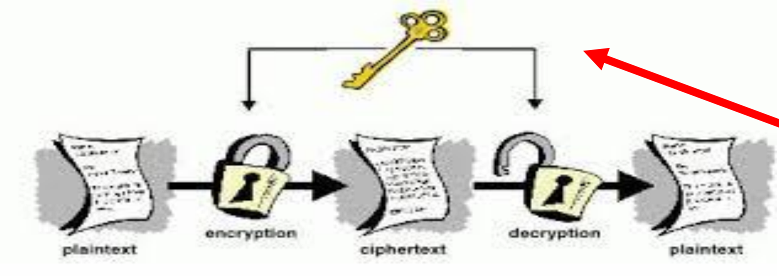
How does Information Security work?

What to protect?

- Confidentiality
- Integrity
- Availability

How to protect?

- Cryptography



- Access control

Primary targets
For attackers

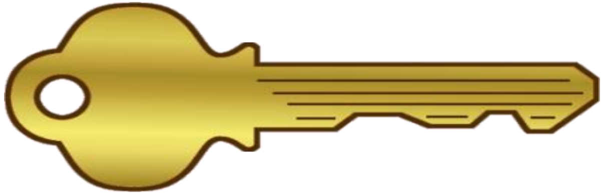
Are IoT devices sensitive to attacks?

- Fast growing market with new unexperienced entrants

- Operate in an uncontrolled (hostile) environment

- Pressure on time-to-market and cost

How does an attacker get access?



Find the key

or

Break the lock

Public

How do attackers work?

Outline

1. What is IoT?
2. Is IoT security important?
3. Case study
4. What’s next?

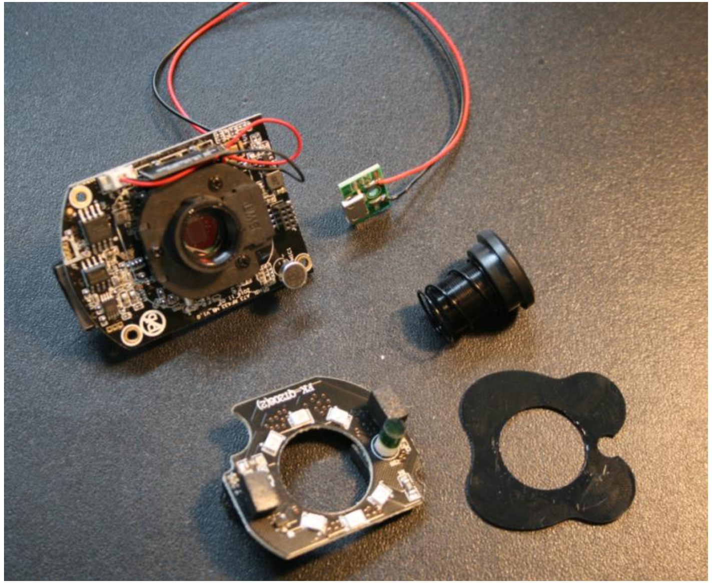
Case study: IoT camera

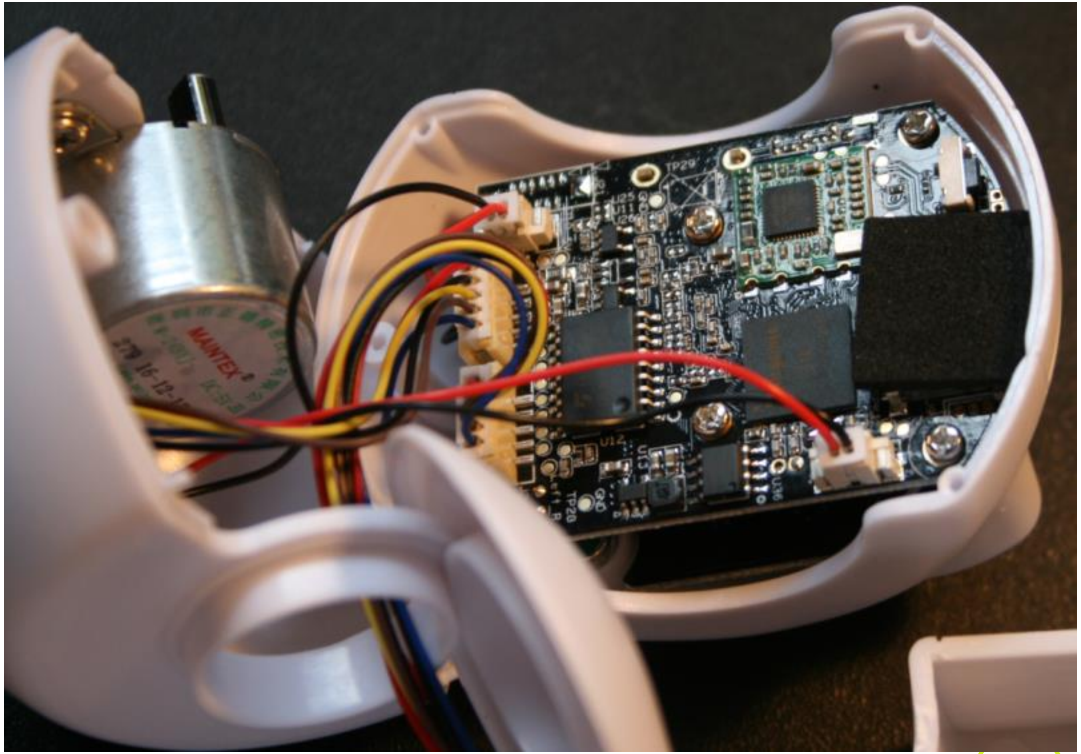
- IoT camera bought from China
- 17 euros
- Many features
  - Wi-Fi connection
  - 2-way audio
  - HD image
  - Motors for rotating the camera
  - IR light for night imaging
  - Logs data to microSD card
  - Phone app for Android & iOS
  - ….

What can go wrong?

Let’s look inside…

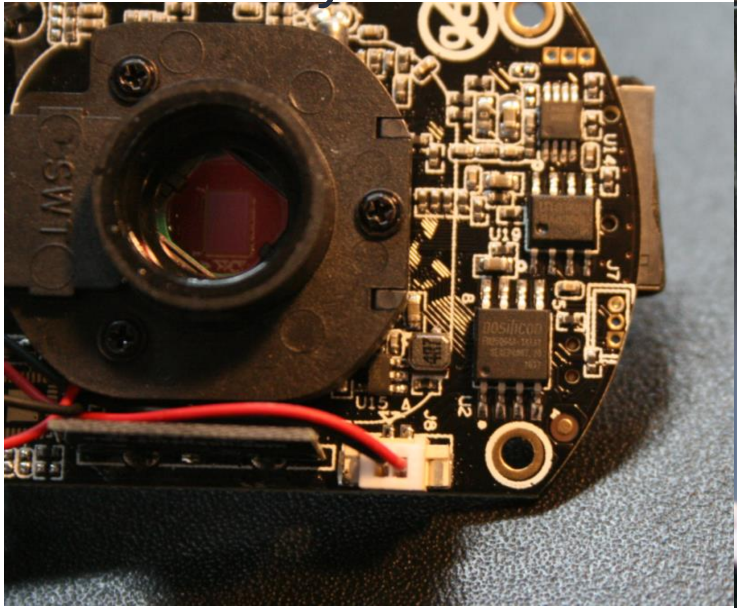
Let’s open the camera and identify interfaces

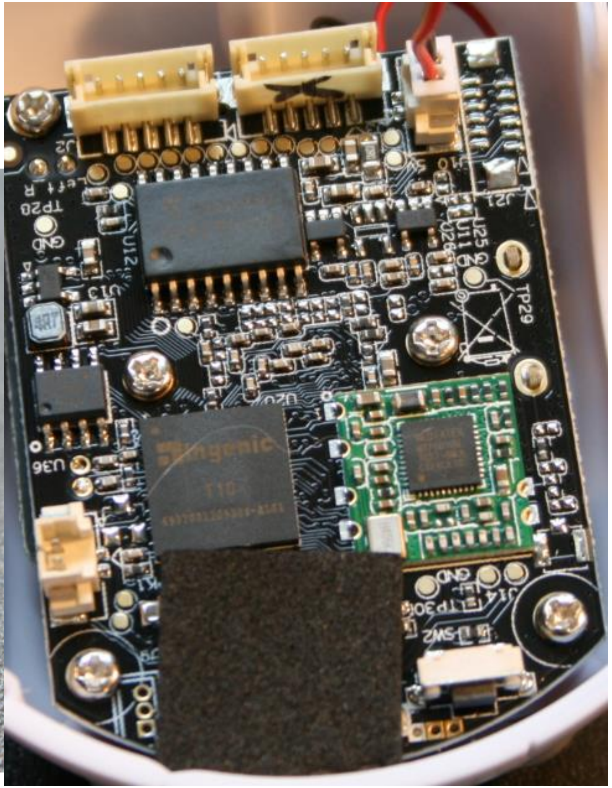




Inspecting the PCB…

Let’s open the camera and identify interfaces



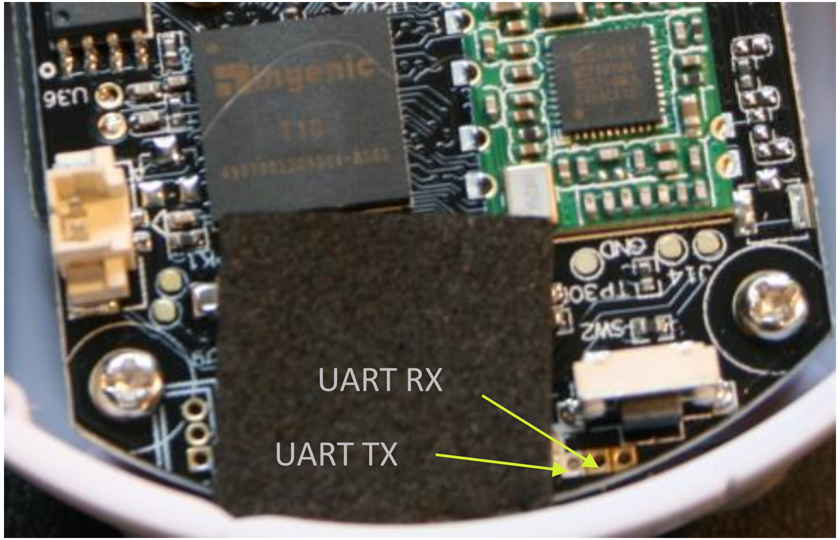


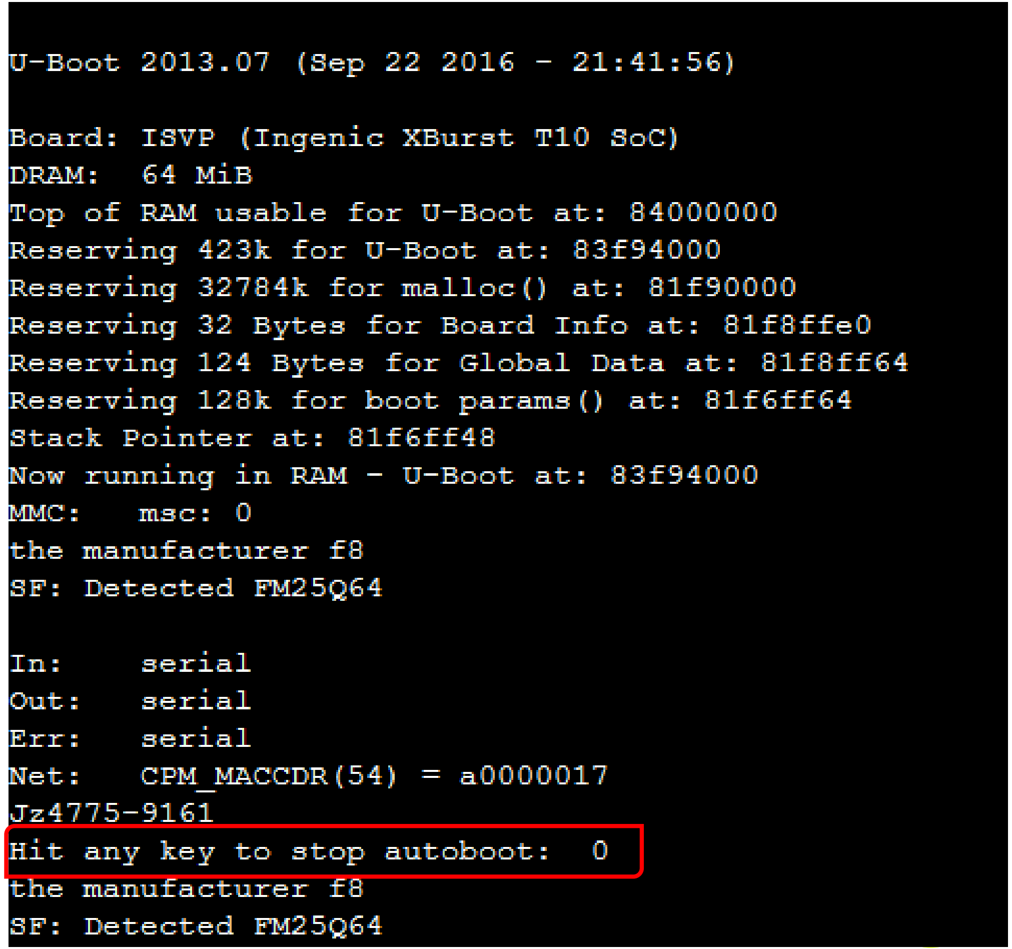
Google + a bit of RE:

- Ingenic T10 SoC
  - Heart of the system
- MediaTek MT7601 SoM
  - Wifi comms
- DoSilicon FM25Q64A
  - Storage for OS (linux)
- Atmel AT24C02 I2C flash
  - Storing camera model
  - MAC address
- Transistor array
  - Powering the motors

We found a way in…

- Most embedded systems still have a UART
- Of course, this camera too



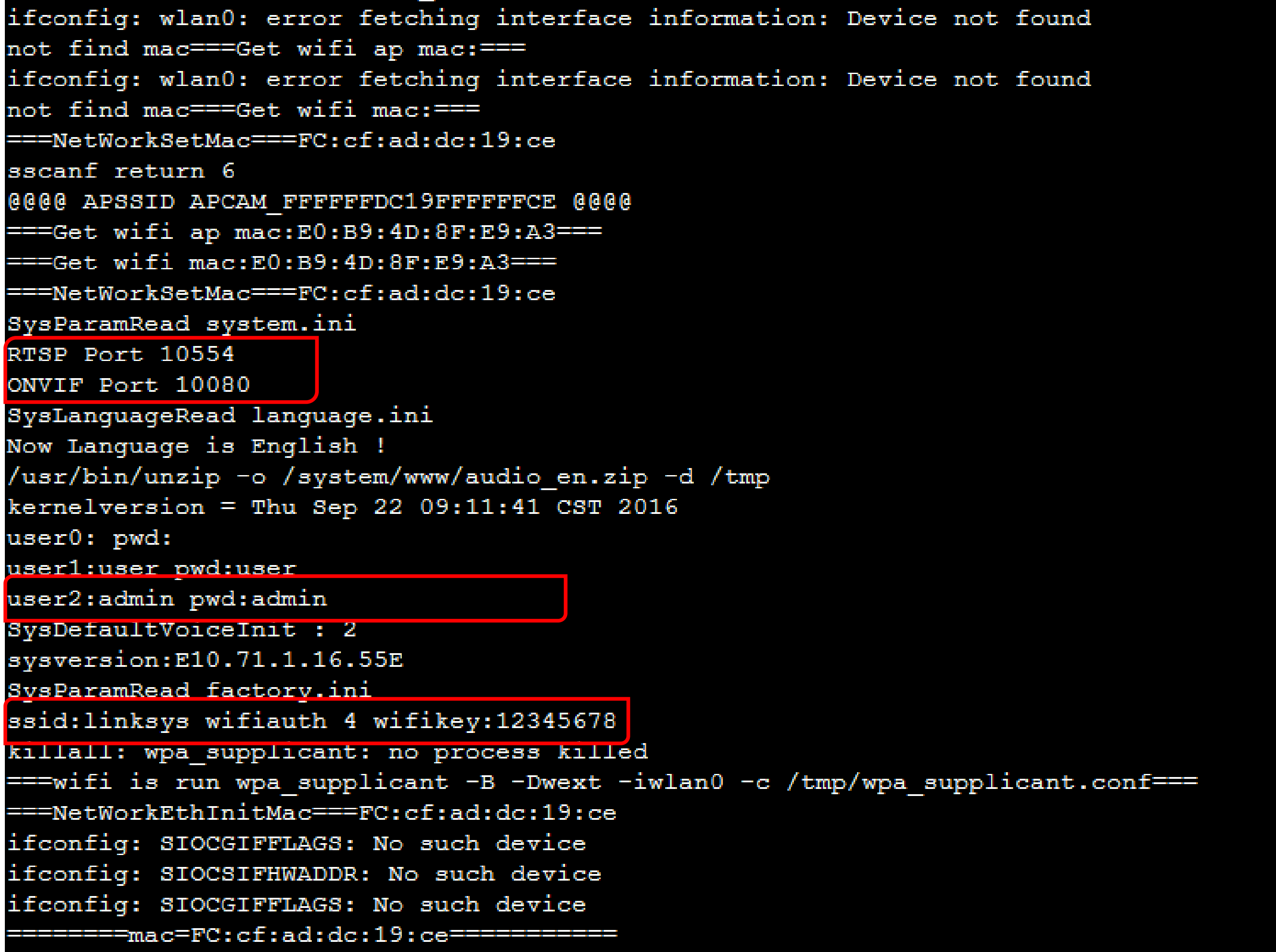


```
U-Boot 2013.07 (Sep 22 2016 - 21:41:56)

Board: ISVP (Ingenic XBurst T10 SoC)
DRAM:  64 MiB
Top of RAM usable for U-Boot at: 84000000
Reserving 423k for U-Boot at: 83f94000
Reserving 32784k for malloc() at: 81f90000
Reserving 32 Bytes for Board Info at: 81f8ffe0
Reserving 124 Bytes for Global Data at: 81f8ff64
Reserving 128k for boot params() at: 81f6ff64
Stack Pointer at: 81f6ff48
Now running in RAM - U-Boot at: 83f94000
MMC:   msc: 0
the manufacturer f8
SF: Detected FM25Q64

In:    serial
Out:   serial
Err:   serial
Net:   CPM_MACCDR(54) = a0000017
Jz4775-9161
Hit any key to stop autoboot:  0
the manufacturer f8
SF: Detected FM25Q64
```

Oops??!!

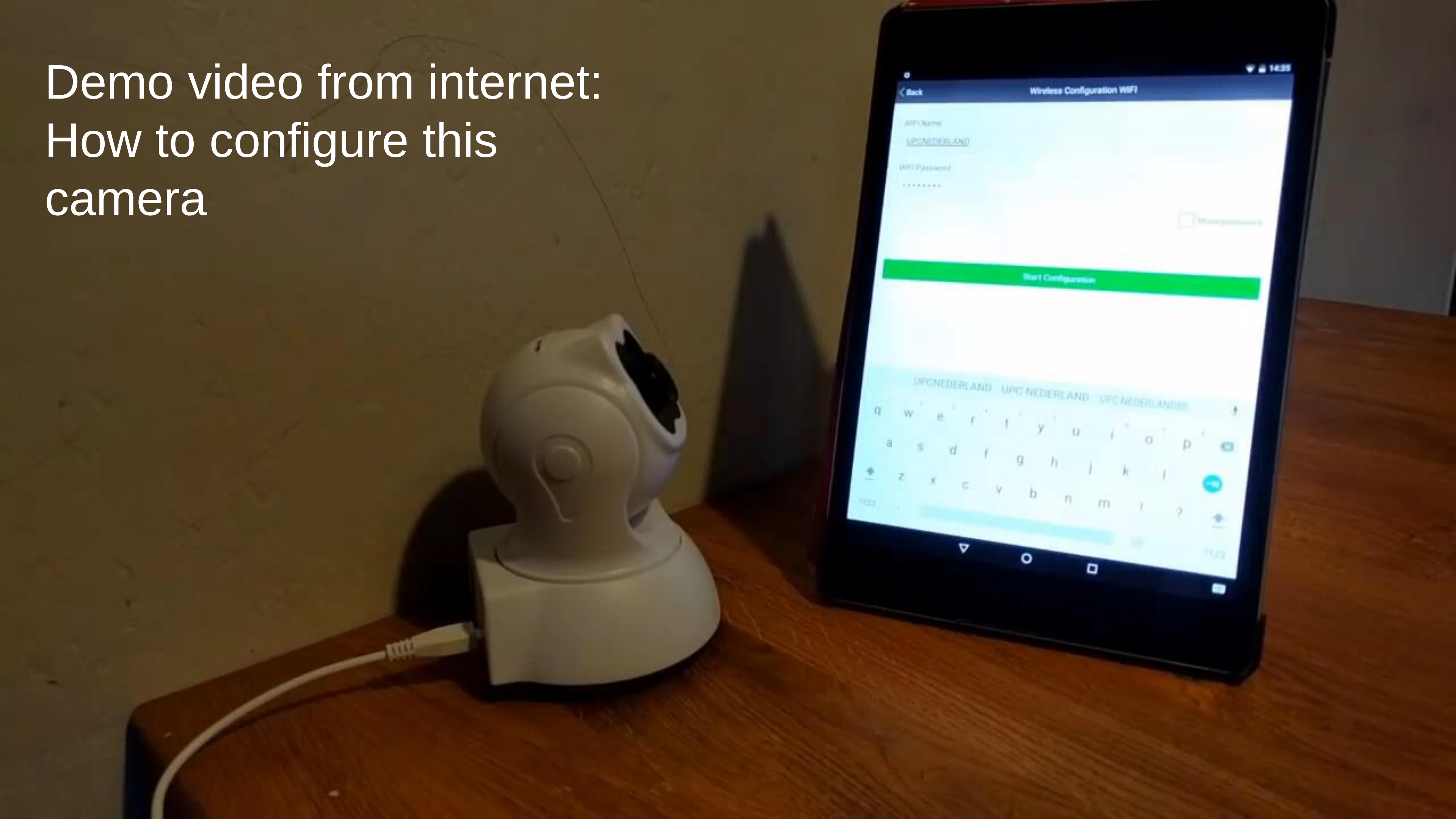
This camera prints all sorts of debug information through serial port

- Ports of the camera, configuration files…
- Users of camera
  - And passwords ☹
- Wifi configuration
  - SSID + password ☹



```
ifconfig: wlan0: error fetching interface information: Device not found
not find mac===Get wifi ap mac:===
ifconfig: wlan0: error fetching interface information: Device not found
not find mac===Get wifi mac:===
===NetWorkSetMac===FC:cf:ad:dc:19:ce
sscanf return 6
@@@@ APSSID APCAM_FFFFFFDC19FFFFFFCE @@@@
===Get wifi ap mac:E0:B9:4D:8F:E9:A3===
===Get wifi mac:E0:B9:4D:8F:E9:A3===
===NetWorkSetMac===FC:cf:ad:dc:19:ce
SysParamRead system.ini
RTSP Port 10554
ONVIF Port 10080
SysLanguageRead language.ini
Now Language is English !
/usr/bin/unzip -o /system/www/audio_en.zip -d /tmp
kernelversion = Thu Sep 22 09:11:41 CST 2016
user0: pwd:
user1:user pwd:user
user2:admin pwd:admin
SysDefaultVoiceInit : 2
sysversion:E10.71.1.16.55E
SysParamRead factory.ini
ssid:linksys wifiauth 4 wifikey:12345678
killall: wpa_supplicant: no process killed
===wifi is run wpa_supplicant -B -Dwext -iwlan0 -c /tmp/wpa_supplicant.conf===
===NetWorkEthInitMac===FC:cf:ad:dc:19:ce
ifconfig: SIOCGIFFLAGS: No such device
ifconfig: SIOCSIFHWADDR: No such device
ifconfig: SIOCGIFFLAGS: No such device
========mac=FC:cf:ad:dc:19:ce===========
```

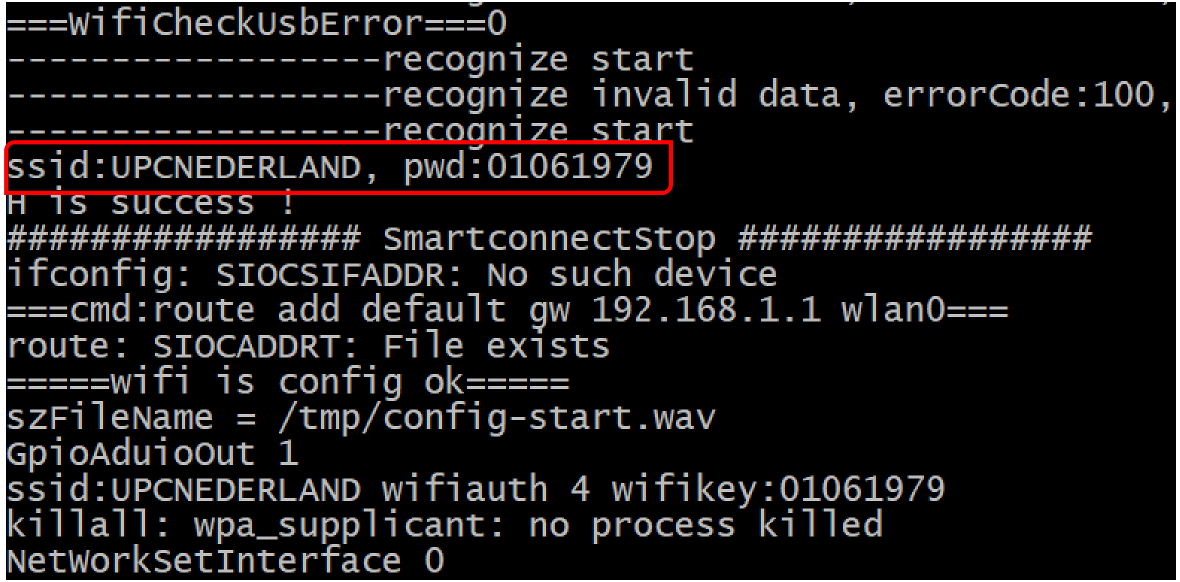
Demo video from internet: How to configure this camera



Oops??!!

This camera prints all sorts of debug information through serial port

- Even the configuration of the SSID from youtube videos ☹



```
===WifiCheckUsbError===0
--------------------recognize start
--------------------recognize invalid data, errorCode:100,
--------------------recognize start
ssid:UPCNEDERLAND, pwd:01061979
H is success !
################## SmartconnectStop ##################
ifconfig: SIOCSIFADDR: No such device
===cmd:route add default gw 192.168.1.1 wlan0===
route: SIOCADDRT: File exists
=====wifi is config ok=====
szFileName = /tmp/config-start.wav
GpioAduioOut 1
ssid:UPCNEDERLAND wifiauth 4 wifikey:01061979
killall: wpa_supplicant: no process killed
NetWorkSetInterface 0
```

Can we also get access to the OS?

Camera has a root password for Linux ☺
But all cameras have the same root password ☹
This thing has U-boot: can we still boot?

- Stop u-boot procedure (hit any key), and print bootargs using **`printenv`**
- Then append to the bootargs ***init=/bin/sh*** :

  ```
  $ setenv bootargs 'console=ttyS1,115200n8 mem=39M@0x0
  ispmem=5M@0x2700000 rmem=20M@0x2c00000 init=/linuxrc rootfstype=squashfs
  rw root=/dev/mtdblock2 rw mtdparts=jz_sfc:256k(boot),2176k(kernel),
  3584k(rootfs),2176k(system) init=/bin/sh'
  ```

-
  ```
  $ boot
  ```

And you boot without password ☹

Can we recover the password?

Reverse engineering on several cameras show they all have same configuration

Interesting files:

- /etc/password

```
root:$1$ybdHbPDn$ii9aEIFNiolBbM9QxW9mr0:0:0::/root:/bin/sh
```

- /etc/shadow does not exist → hash above is a MD5 hash → collision fun

Use any password cracking program to crack the salt$hash string (or google the string)
`ybdHbPDn$ii9aEIFNiolBbM9QxW9mr0 =` md5(“ybdHbPDn” + “**hslwificam**”)

We have the root access password on all cameras

Can we get access to other services?

We have local root: let’s login and see what is the camera exposing to internet…
Telnetd is running: default backdoor on all cameras ☹☹

But wait… **there is a RTSP port in 10554 published by the camera…**
What happens if you try to access it directly?

rstp://ip.of.the.cam:10554/tcp/av0_0
User: admin, no pass == access camera stream ☹☹☹

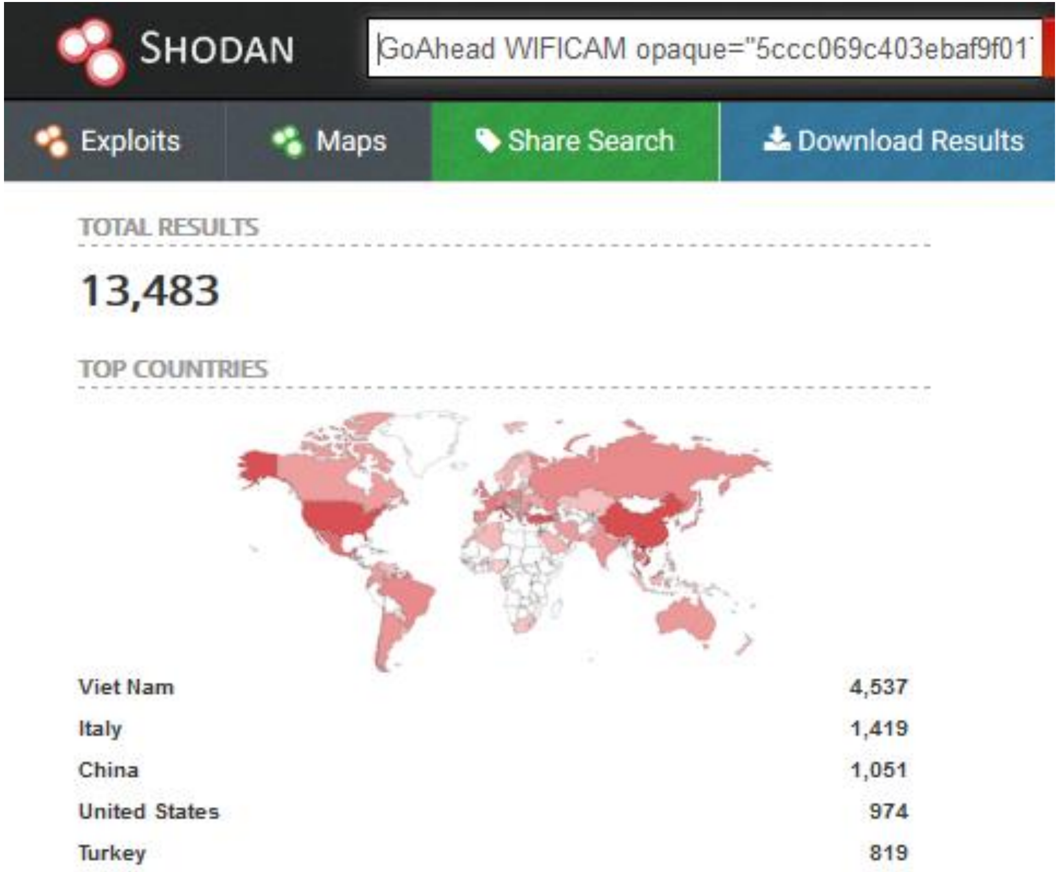
And in port 81: http / ONVIF interface (you can even move the camera) ☹☹☹

We can listen in to video broadcasted by all cameras of this type

So, where are the cameras?

Can we go global? Let’s search for http header strings in Shodan.io

- **Loads of cameras connected**
- **Thousands of houses offer free spying…**



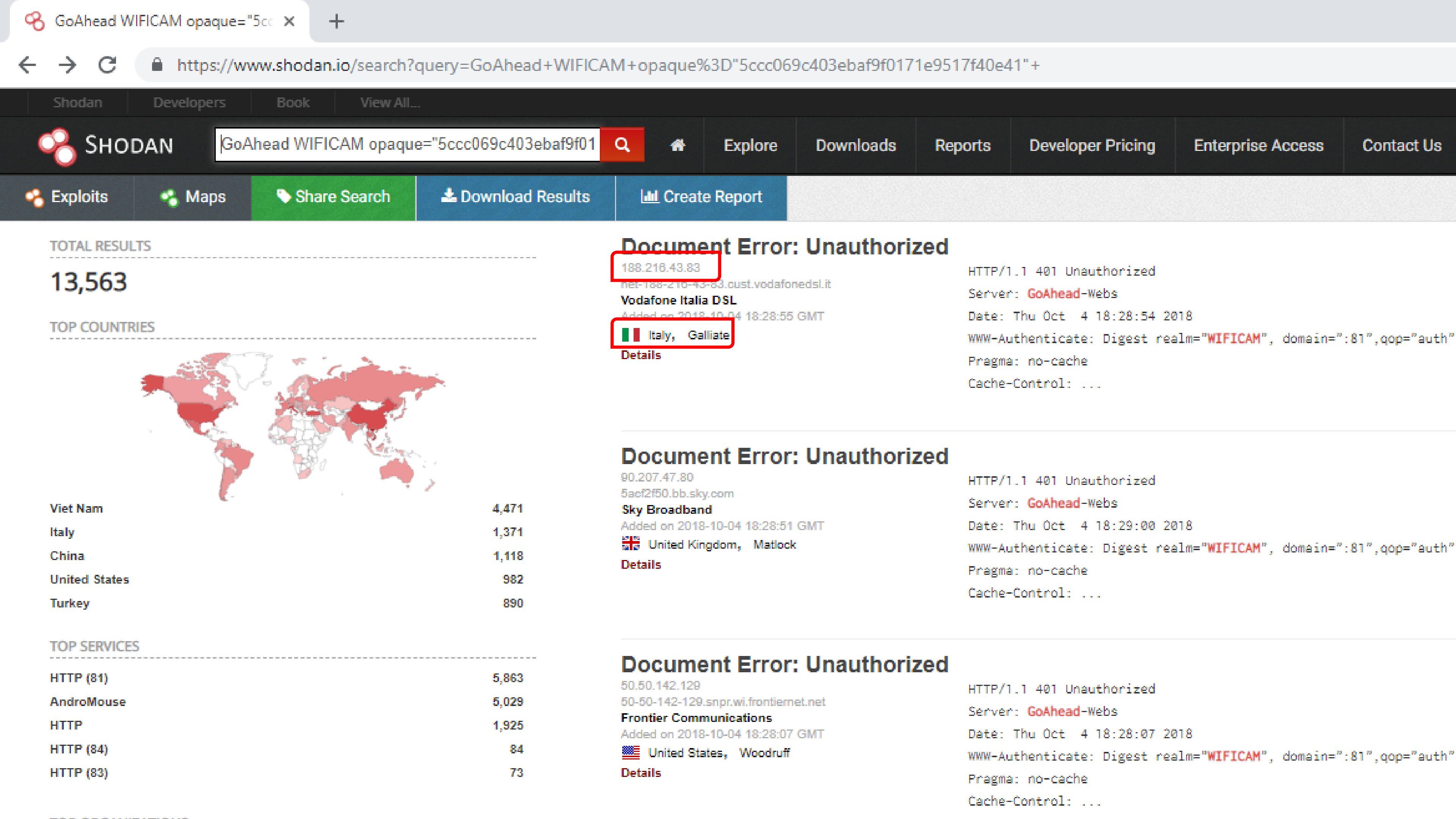
GoAhead WIFICAM opaque="5ccc069c403ebaf9f01

TOTAL RESULTS

13,483

TOP COUNTRIES

Viet Nam	4,537
Italy	1,419
China	1,051
United States	974
Turkey	819


GoAhead WIFICAM opaque="5cc
https://www.shodan.io/search?query=GoAhead+WIFICAM+opaque%3D"5ccc069c403ebaf9f0171e9517f40e41"+
Shodan
Developers
Book
View All...
SHODAN
GoAhead WIFICAM opaque="5ccc069c403ebaf9f01
Explore
Downloads
Reports
Developer Pricing
Enterprise Access
Contact Us
Exploits
Maps
Share Search
Download Results
Create Report

TOTAL RESULTS

13,563

TOP COUNTRIES

Viet Nam	4,471
Italy	1,371
China	1,118
United States	982
Turkey	890

TOP SERVICES

HTTP (81)	5,863
AndroMouse	5,029
HTTP	1,925
HTTP (84)	84
HTTP (83)	73

Document Error: Unauthorized

188.216.43.83
net-188-216-43-83.cust.vodafonedsl.it
Vodafone Italia DSL
Added on 2018-10-04 18:28:55 GMT
Italy, Galliate
Details

```
HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Thu Oct  4 18:28:54 2018
WWW-Authenticate: Digest realm="WIFICAM", domain=":81",qop="auth"
Pragma: no-cache
Cache-Control: ...
```

Document Error: Unauthorized

90.207.47.80
5acf2f50.bb.sky.com
Sky Broadband
Added on 2018-10-04 18:28:51 GMT
United Kingdom, Matlock
Details

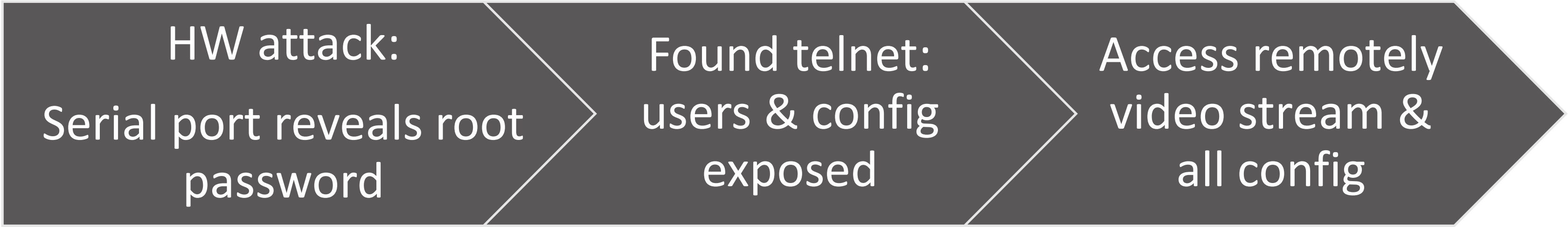
```
HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Thu Oct  4 18:29:00 2018
WWW-Authenticate: Digest realm="WIFICAM", domain=":81",qop="auth"
Pragma: no-cache
Cache-Control: ...
```

Document Error: Unauthorized

50.50.142.129
50-50-142-129.snpr.wi.frontiernet.net
Frontier Communications
Added on 2018-10-04 18:28:07 GMT
United States, Woodruff
Details

```
HTTP/1.1 401 Unauthorized
Server: GoAhead-Webs
Date: Thu Oct  4 18:28:07 2018
WWW-Authenticate: Digest realm="WIFICAM", domain=":81",qop="auth"
Pragma: no-cache
Cache-Control: ...
```

Attack recap



HW attack:

Serial port reveals root password

Found telnet: users & config exposed

Access remotely video stream & all config

Camera security fully bypassed & backdoor for free

- These cameras are used typically as baby monitors: privacy violation
- Linux system: can be used for illicit activities, e.g. bitcoin miners
- IoT botnet Mirai almost brought down DNS in parts of the world

Lessons learned

Takeaway 1: bad security practices + hardware attack == scalability

- Use hardened OS, close ports, protect services
- Need unique passwords
- Run firewalls

Takeaway 2: flawed IoT devices == stepping stone for bigger attacks

- It’s not just about the device itself, the eco system is at risk

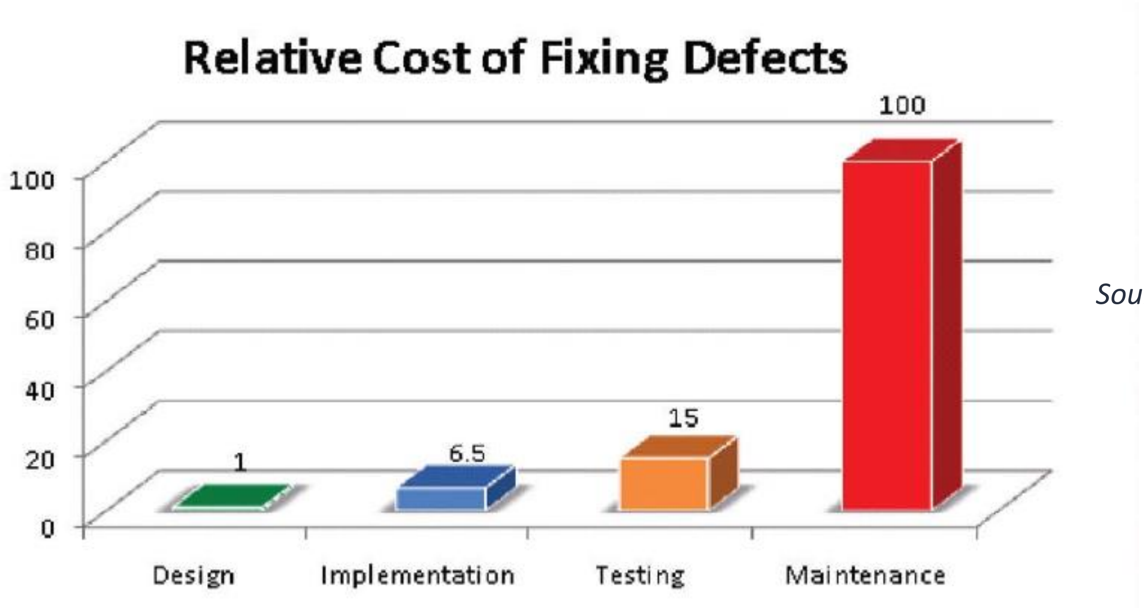
Takeaway 3: proper security is not free

- Independent review and testing really helps exposing weaknesses and improve security

Outline

1. What is IoT?
2. Is IoT security important?
3. Case study
4. What’s next?

When should we fix our bugs?



Source: NASA, IBM

- Cost of fixing goes rapidly up
- Prevention is better than cure

EU CYBERSECURITY ACT

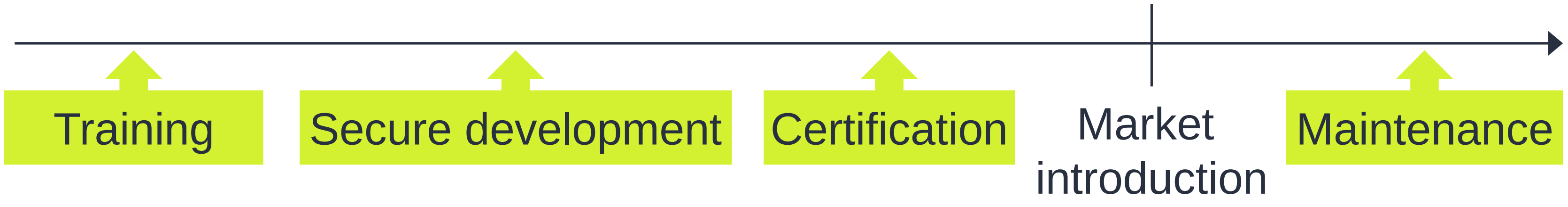
- European cybersecurity certification
- Certificates valid in all EU countries
- Certification will be voluntary, unless ...
- Verify data confidentiality and integrity
- Assurance levels:
  - Basic → documentation review
  - Substantial → functional security testing
  - High →penetration testing

Your products may need security certification by 2020

- Because EU mandates it, or
- Customers demand it, or
- Competitors get it

Are you ready?

How to make a secure product?

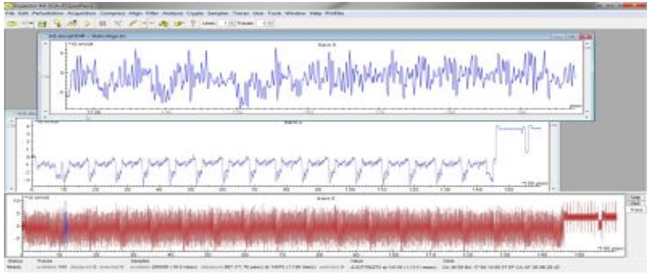


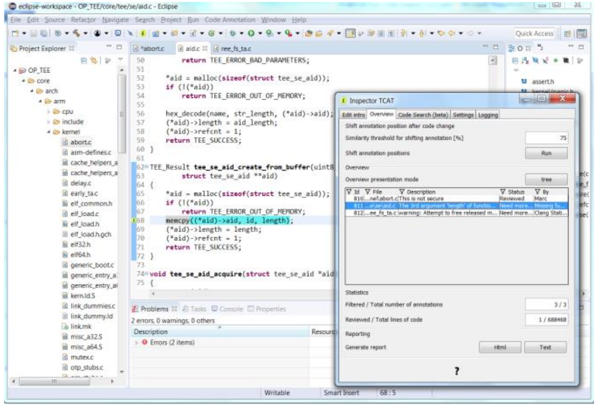
- Training increases security awareness and brings security capabilities
- Secure development is about secure process, design, and coding
- Certification involves testing and provides assurance that the product is secure
- Maintenance keeps an evolving product secure

Riscure support for making secure products

- Training & Coaching

- Tools for code analysis & security penetration testing





```
        return TEE_ERROR_BAD_PARAMETERS;

    *aid = malloc(sizeof(struct tee_se_aid));
    if (!(*aid))
        return TEE_ERROR_OUT_OF_MEMORY;

    hex_decode(name, str_length, (*aid)->aid);
    (*aid)->length = aid_length;
    (*aid)->refcnt = 1;
    return TEE_SUCCESS;
}

TEE_Result tee_se_aid_create_from_buffer(uint8
        struct tee_se_aid **aid)
{
    *aid = malloc(sizeof(struct tee_se_aid));
    if (!(*aid))
        return TEE_ERROR_OUT_OF_MEMORY;
    memcpy((*aid)->aid, id, length);
    (*aid)->length = length;
    (*aid)->refcnt = 1;
    return TEE_SUCCESS;
}

void tee_se_aid_acquire(struct tee_se_aid *aid
{
```

2 errors, 0 warnings, 0 others

Description | Resource
Errors (2 items)

Shift annotation position after code change

Similarity threshold for shifting annotation [%]: 75

Shift annotation positions: Run

Overview

Overview presentation mode: tree

Id	File	Description	Status	By
810	...nel\abort.c	This is not secure	Reviewed	Marc
811	...e\se\aid.c	The 3rd argument 'length' of functio...	Need more...	Missing fu...
812	...ee_fs_ta.c	warning: Attempt to free released m...	Need more...	Clang Stati...

Statistics

Filtered / Total number of annotations: 3 / 3

Reviewed / Total lines of code: 1 / 688468

Reporting

Generate report: Html Text

- Evaluation & Certification

Common Criteria

Takeaways

- IoT will be everywhere
- Software is getting huge and hard to verify
- Security no longer a nice-to-have
- Certification needs secure development
- Solutions exist to make better products

Riscure B.V.
Frontier Building, Delftechpark 49
2628 XJ Delft
The Netherlands
Phone: +31 15 251 40 90
www.riscure.com

Riscure North America
550 Kearny St., Suite 330
San Francisco, CA 94108 USA
Phone: +1 650 646 99 79
inforequest@riscure.com

Riscure China
Room 2030-31, No. 989, Changle Road, Shanghai 200031
China
Phone: +86 21 5117 5435
inforcn@riscure.com

riscure

Challenge your security

Visit us at the exhibition
Learn about security training & tooling