Hands-on security for DIY projects

A. Cervoise
antoine.cervoise@gmail.com

July 6, 2016

Summary

Antoine - @acervoise

- Pentester at NTT (Com) Security FR
- @_Univershell_
- @Fabelier Paris
- Cigars smoker
- Music lover

Who am I?

Current projects

- Hardware password bruteforce
- IoT/DIY vulnerability research
- Control cigars cave humidity with Arduinos
- LeakyStorage: USB key with Wi-Fi
- Having fun with WebDev

Summary

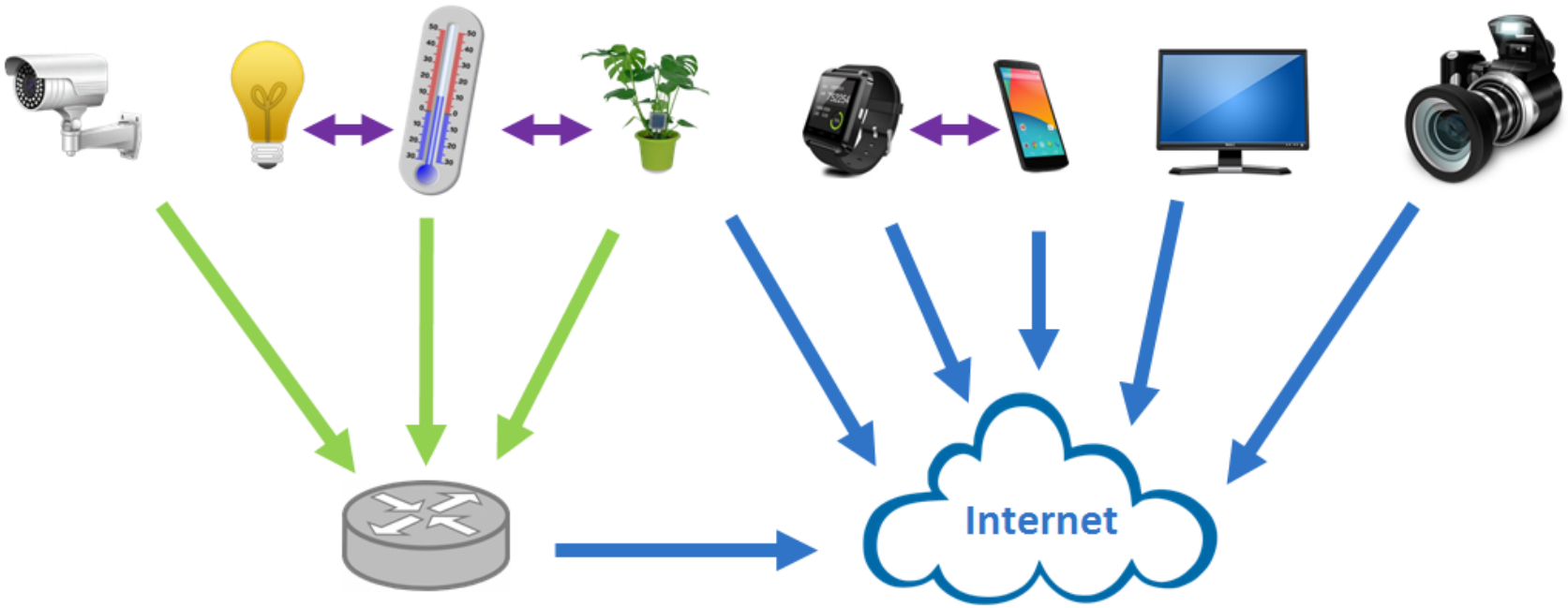
Internet of Things

The internet of things (IoT) is the network of physical devices, vehicles, buildings and other itemsembedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

Source: Wikipedia

https://en.wikipedia.org/wiki/Internet_of_things

Internet of Things



Internet of Things

Internet of Threats

Pownable

- Fast development process
- People with hardware background, not software
- Security is done at the end (if there is still some times)

Internet of Threats

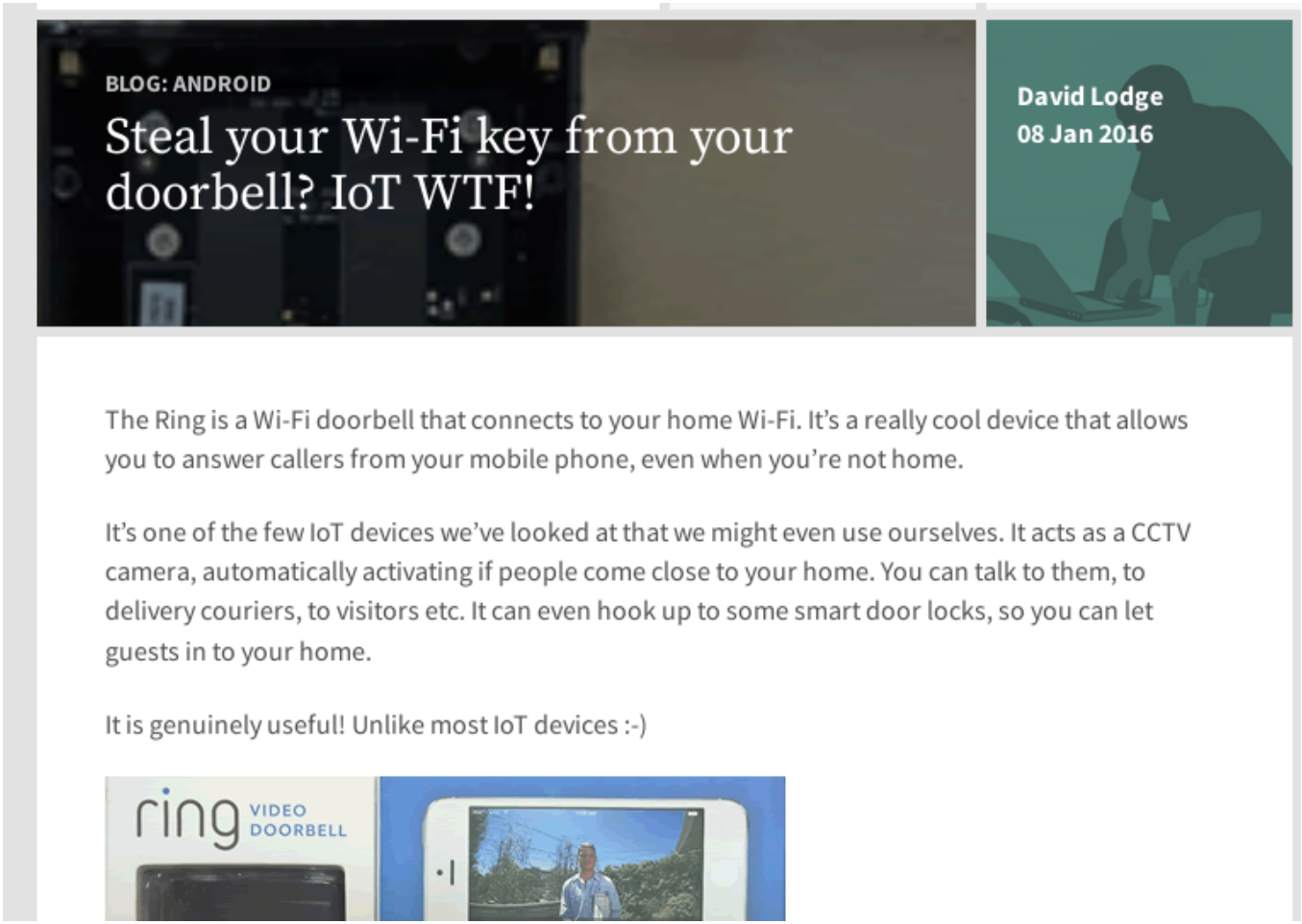
Black Hat USA 2015: The full story of how that Jeep was hacked

August 6, 2015 Alex Drozhzhin Featured Post, News, Security, Threats

Recently we wrote about the now-famous hack of a Jeep Cherokee. At Black Hat USA 2015, a large security conference, researchers Charlie Miller and Chris Valasek finally explained in detail, how exactly that hack happened.

https://blog.kaspersky.com/blackhat-jeep-cherokee-hack-explained/9493/

Internet of Threats



BLOG: ANDROID

Steal your Wi-Fi key from your doorbell? IoT WTF!

David Lodge
08 Jan 2016

The Ring is a Wi-Fi doorbell that connects to your home Wi-Fi. It's a really cool device that allows you to answer callers from your mobile phone, even when you're not home.

It's one of the few IoT devices we've looked at that we might even use ourselves. It acts as a CCTV camera, automatically activating if people come close to your home. You can talk to them, to delivery couriers, to visitors etc. It can even hook up to some smart door locks, so you can let guests in to your home.

It is genuinely useful! Unlike most IoT devices :-)

https://www.pentestpartners.com/blog/steal-your-wi-fi-key-from-your-doorbell-iot-wtf/

Internet of Threats

Technology

VTech hack: Parents complain of Christmas disappointment

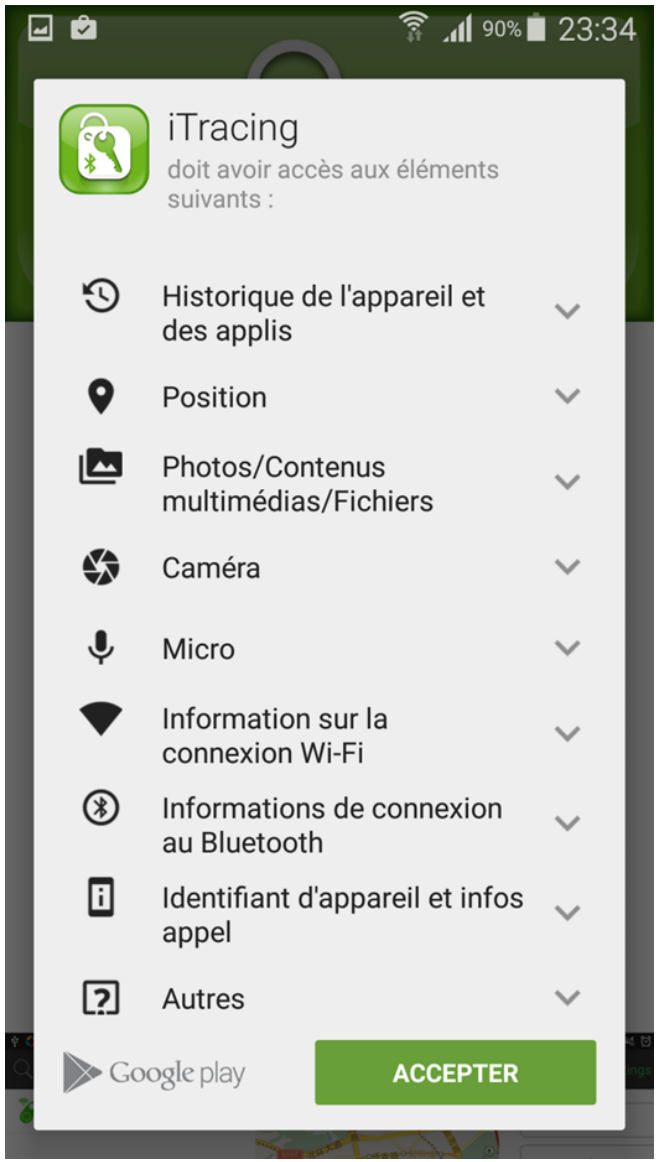
By Kevin Rawlinson
BBC News

5 January 2016 | Technology

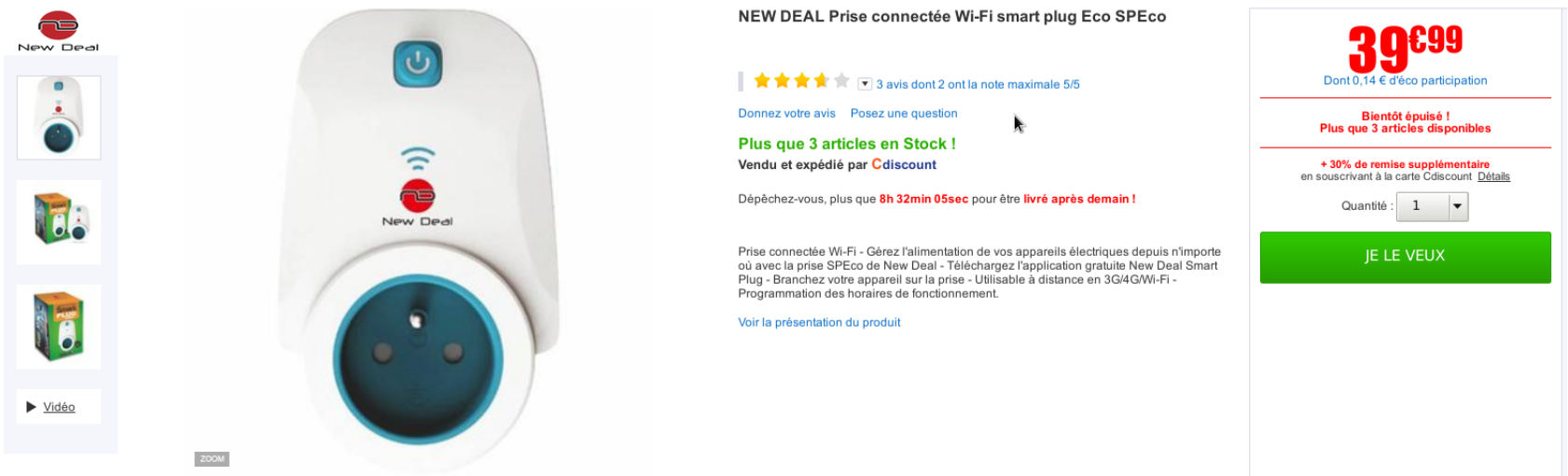
Share

http://www.bbc.com/news/technology-35232469

Internet of Threats



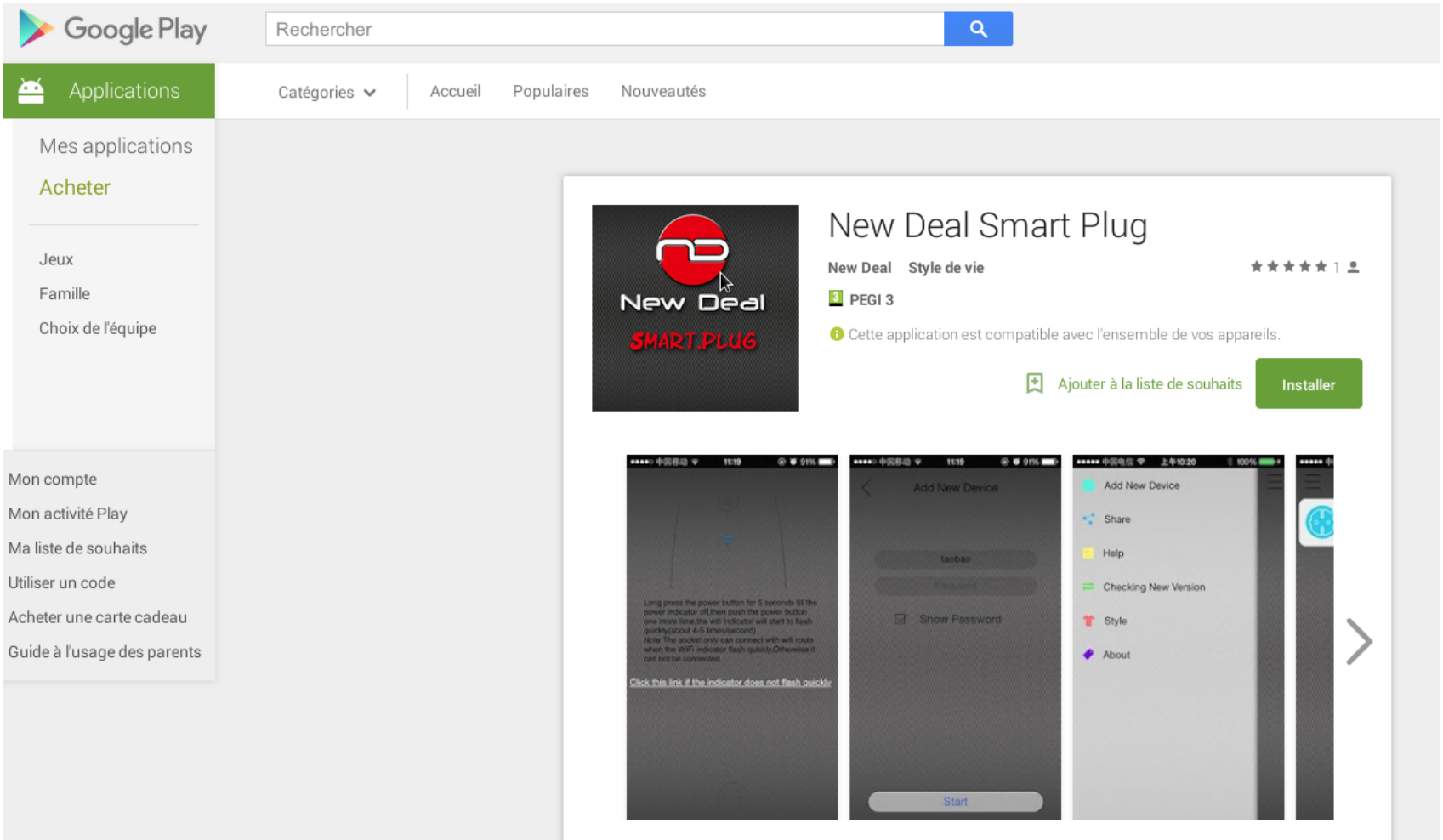
Internet of Threats



Internet of Things

Internet of Threats

Internet of Threats



Notre attaque

```
$ ls SmartDeal/u/aly
aa.java  ai.java  ap.java  ax.java  bf.java  bm.java
ab.java  a.java   aq.java  ay.java  bg.java  bn.java
ac.java  aj.java  ar.java  az.java  bh.java  bo.java
ad.java  ak.java  as.java  ba.java  bi.java  bp.java
ae.java  al.java  at.java  bb.java  b.java   bq.java
af.java  am.java  au.java  bc.java  bj.java  br.java
ag.java  an.java  av.java  bd.java  bk.java  bs.java
ah.java  ao.java  aw.java  be.java  bl.java  bt.java
```

Notre attaque

```
$ cat SmartDeal/u/aly/ap.java

public static ap a(int paramInt)
{
    switch (paramInt)
    {
        default:
            return null;
        case 0:
            return a;
        case 1:
        return b;
    }
    return c;
}
```

Internet of Threats

virustotal

SHA256: fa789cd6357e1bb2ac84e55dd7c36a2691d5a603132b0716bd3b9d4f4fe6e630

Nom du fichier : base.apk

Ratio de détection : 11 / 55

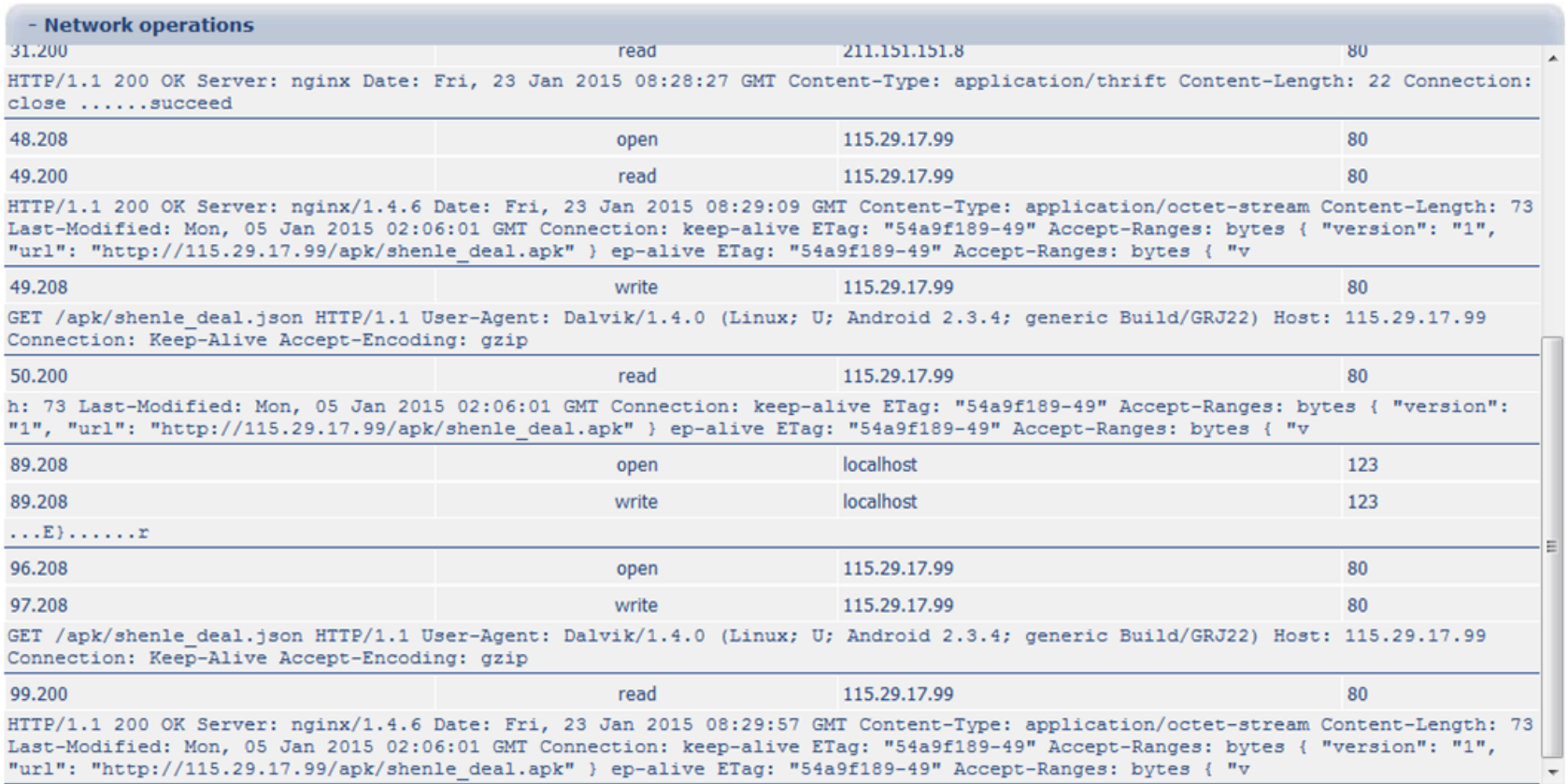
Date d'analyse : 2016-06-23 14:38:53 UTC (il y a 3 minutes)

Analyse | File detail | Informations supplémentaires | Commentaires | Votes | Informations comportementales

Antivirus	Résultat	Mise à jour
AVG	Android/Deng.PDS	20160623
AVware	Trojan.AndroidOS.Generic.A	20160623
AegisLab	Spr.Andr.Dianjin.Alc	20160623
Antiy-AVL	Trojan/AndroidOS.TSGeneric	20160623
Bkav	Android.Adware.Dowgin.75DA	20160623
CAT-QuickHeal	Android.Dianjin.A3cd (AdWare)	20160623
Cyren	AndroidOS/GenPua.769524B3!Olympus	20160623
ESET-NOD32	a variant of Android/Dianjin.B potentially unsafe	20160623
Ikarus	AdWare.AndroidOS.Dianjin	20160623
McAfee	Artemis!769524B3BF44	20160623
McAfee-GW-Edition	Artemis!769524B3BF44	20160623

https://www.virustotal.com/fr/file/fa789cd6357e1bb2ac84e55dd7c36a2691d5a603132b0716bd3b9d4f4fe6e630/analysis/1466692733/

Internet of Threats



- Network operations

31.200	read	211.151.151.8	80
HTTP/1.1 200 OK Server: nginx Date: Fri, 23 Jan 2015 08:28:27 GMT Content-Type: application/thrift Content-Length: 22 Connection: close ......succeed			
48.208	open	115.29.17.99	80
49.200	read	115.29.17.99	80
HTTP/1.1 200 OK Server: nginx/1.4.6 Date: Fri, 23 Jan 2015 08:29:09 GMT Content-Type: application/octet-stream Content-Length: 73 Last-Modified: Mon, 05 Jan 2015 02:06:01 GMT Connection: keep-alive ETag: "54a9f189-49" Accept-Ranges: bytes { "version": "1", "url": "http://115.29.17.99/apk/shenle_deal.apk" } ep-alive ETag: "54a9f189-49" Accept-Ranges: bytes { "v			
49.208	write	115.29.17.99	80
GET /apk/shenle_deal.json HTTP/1.1 User-Agent: Dalvik/1.4.0 (Linux; U; Android 2.3.4; generic Build/GRJ22) Host: 115.29.17.99 Connection: Keep-Alive Accept-Encoding: gzip			
50.200	read	115.29.17.99	80
h: 73 Last-Modified: Mon, 05 Jan 2015 02:06:01 GMT Connection: keep-alive ETag: "54a9f189-49" Accept-Ranges: bytes { "version": "1", "url": "http://115.29.17.99/apk/shenle_deal.apk" } ep-alive ETag: "54a9f189-49" Accept-Ranges: bytes { "v			
89.208	open	localhost	123
89.208	write	localhost	123
...E}......r			
96.208	open	115.29.17.99	80
97.208	write	115.29.17.99	80
GET /apk/shenle_deal.json HTTP/1.1 User-Agent: Dalvik/1.4.0 (Linux; U; Android 2.3.4; generic Build/GRJ22) Host: 115.29.17.99 Connection: Keep-Alive Accept-Encoding: gzip			
99.200	read	115.29.17.99	80
HTTP/1.1 200 OK Server: nginx/1.4.6 Date: Fri, 23 Jan 2015 08:29:57 GMT Content-Type: application/octet-stream Content-Length: 73 Last-Modified: Mon, 05 Jan 2015 02:06:01 GMT Connection: keep-alive ETag: "54a9f189-49" Accept-Ranges: bytes { "version": "1", "url": "http://115.29.17.99/apk/shenle_deal.apk" } ep-alive ETag: "54a9f189-49" Accept-Ranges: bytes { "v			

Internet of Threats

- Started Services	
32.210	com.android.music.MediaPlaybackService
32.210	com.android.music.MediaPlaybackService
36.207	com.android.music.MediaPlaybackService
38.208	com.android.music.MediaPlaybackService
43.210	com.android.music.MediaPlaybackService
44.206	com.android.music.MediaPlaybackService
77.208	com.android.mms.transaction.SmsReceiverService
77.208	com.android.mms.transaction.SmsReceiverService

Summary

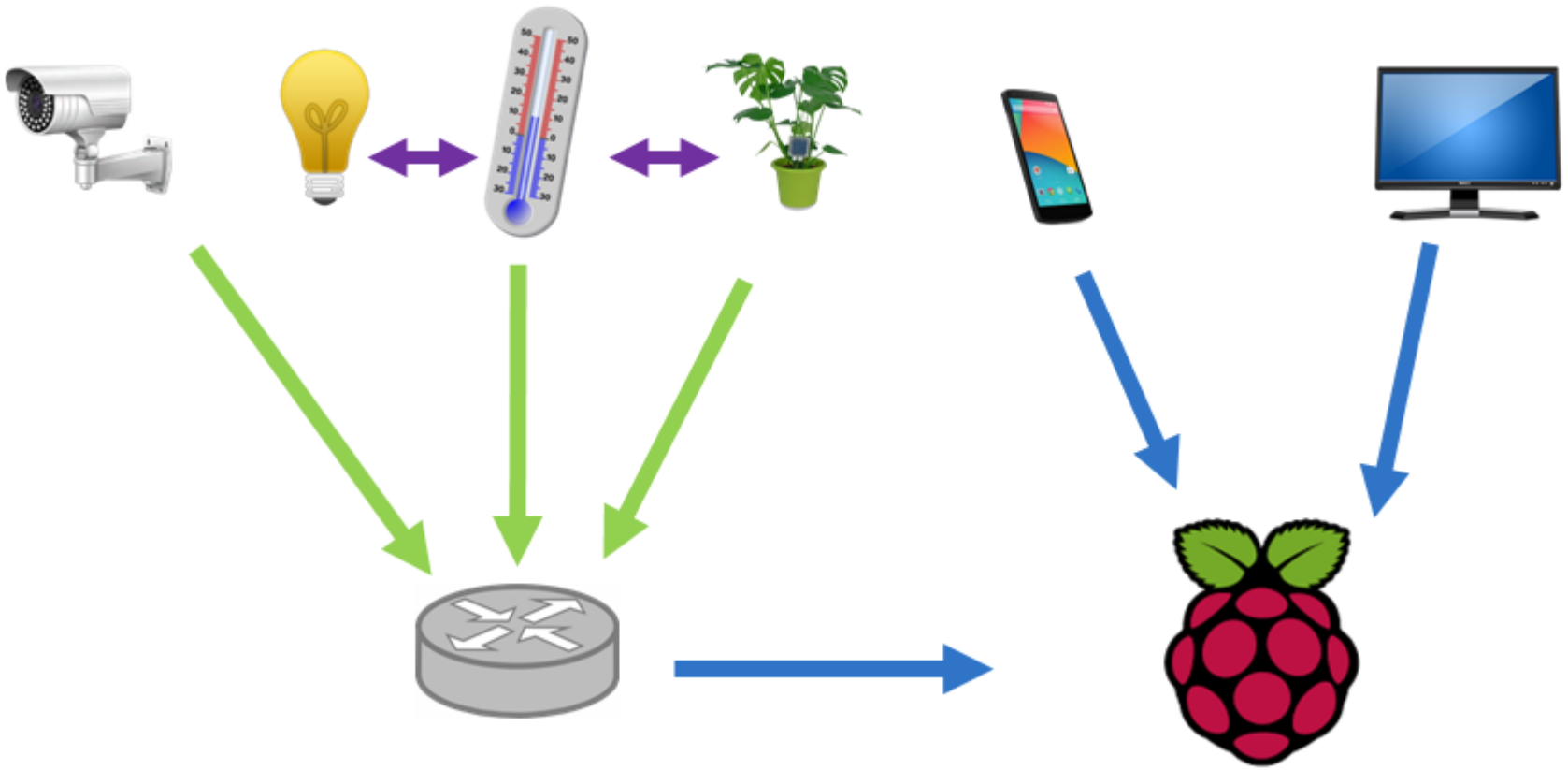
DIY IoT

Not the subject

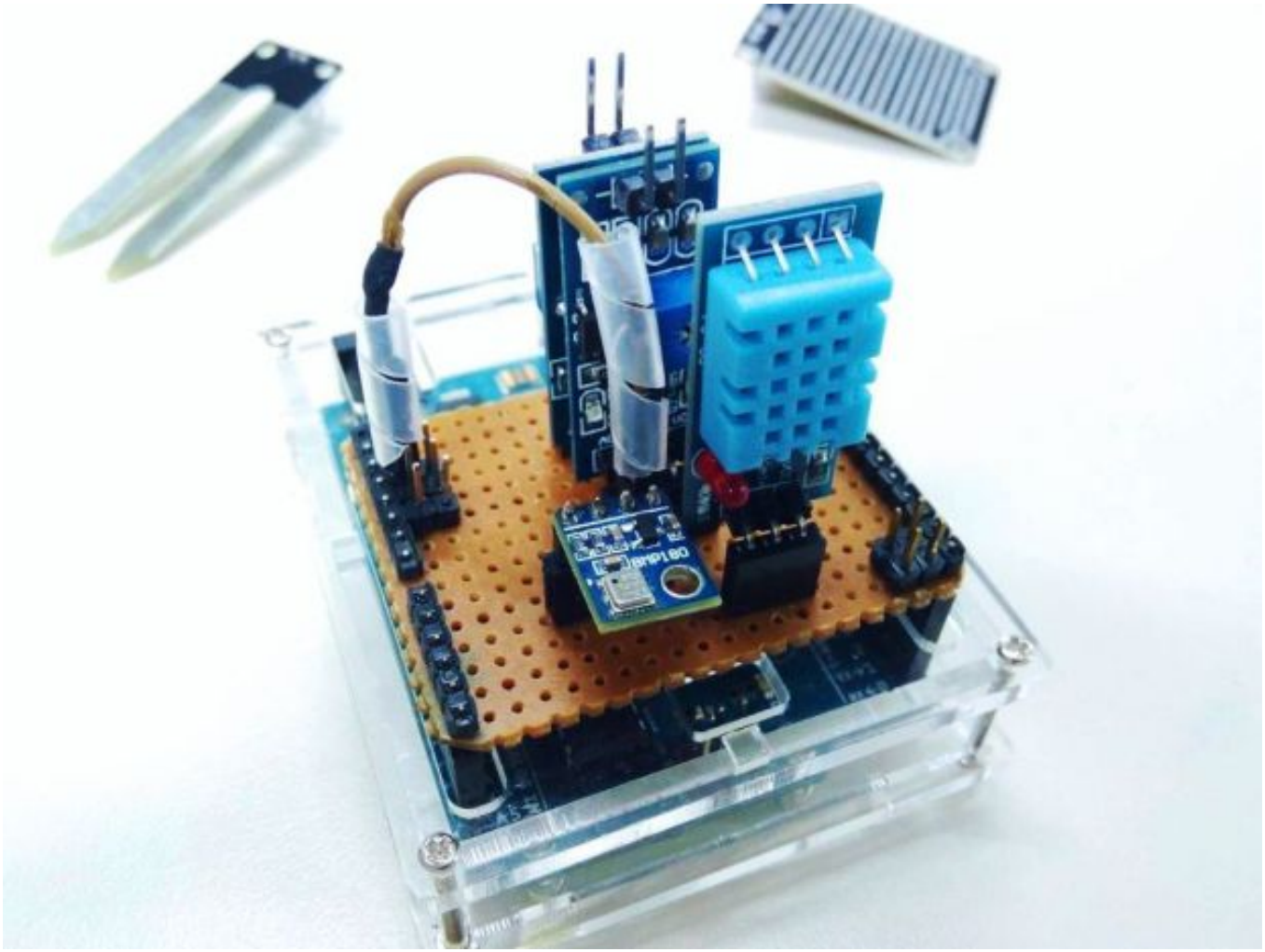
Commercial product with

- Central controller
- Hardware modules
- Smartphone apps

DIY IoT



DIY IoT



http://makezine.com/2015/11/20/build-your-own-arduino-weather-station/

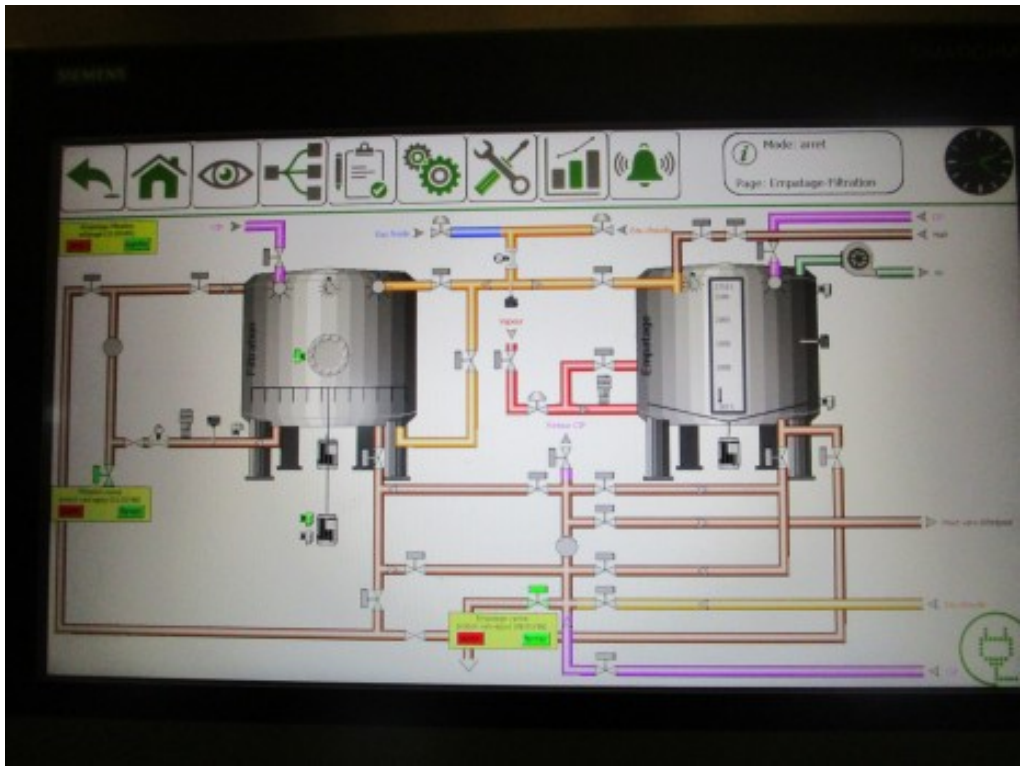
DIY "ICS"

Let's brew beer

- Control beer process
- Industrials use ICS (Industrial Control System)
- Homebrewers use BrewPi

DIY "ICS"

Siemens ICS for *Brasserie de Meaux*

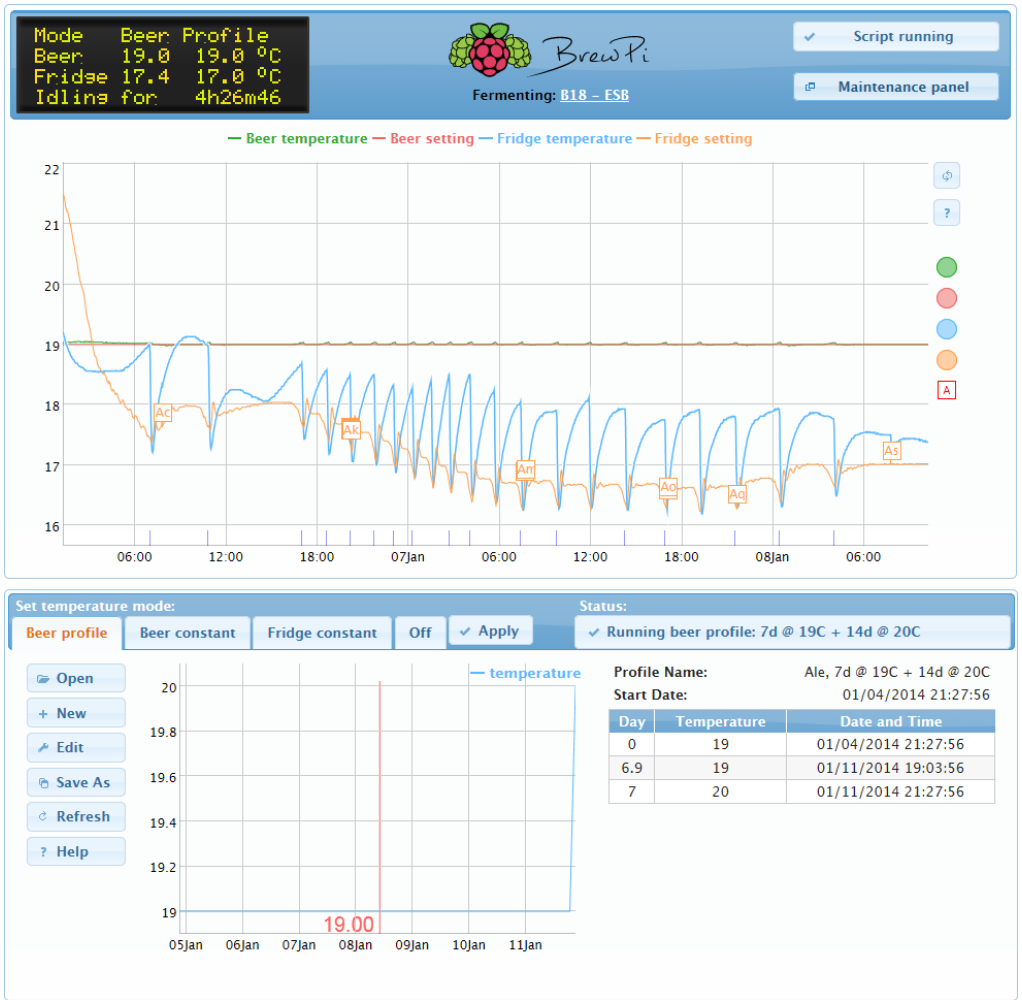


DIY "ICS"

BrewPi

- Hack a fridge
- Solder BrewPi
- Assembly case
- Install software

BrewPi (without authentication) web interface



Pull request for authentication by nzjoel1234: https://github.com/BrewPi/brewpi-www/pull/61

DIY IoT

Bad examples through

- Blogs
- Magazines
- Vendors

And control points to improve your DIY projects

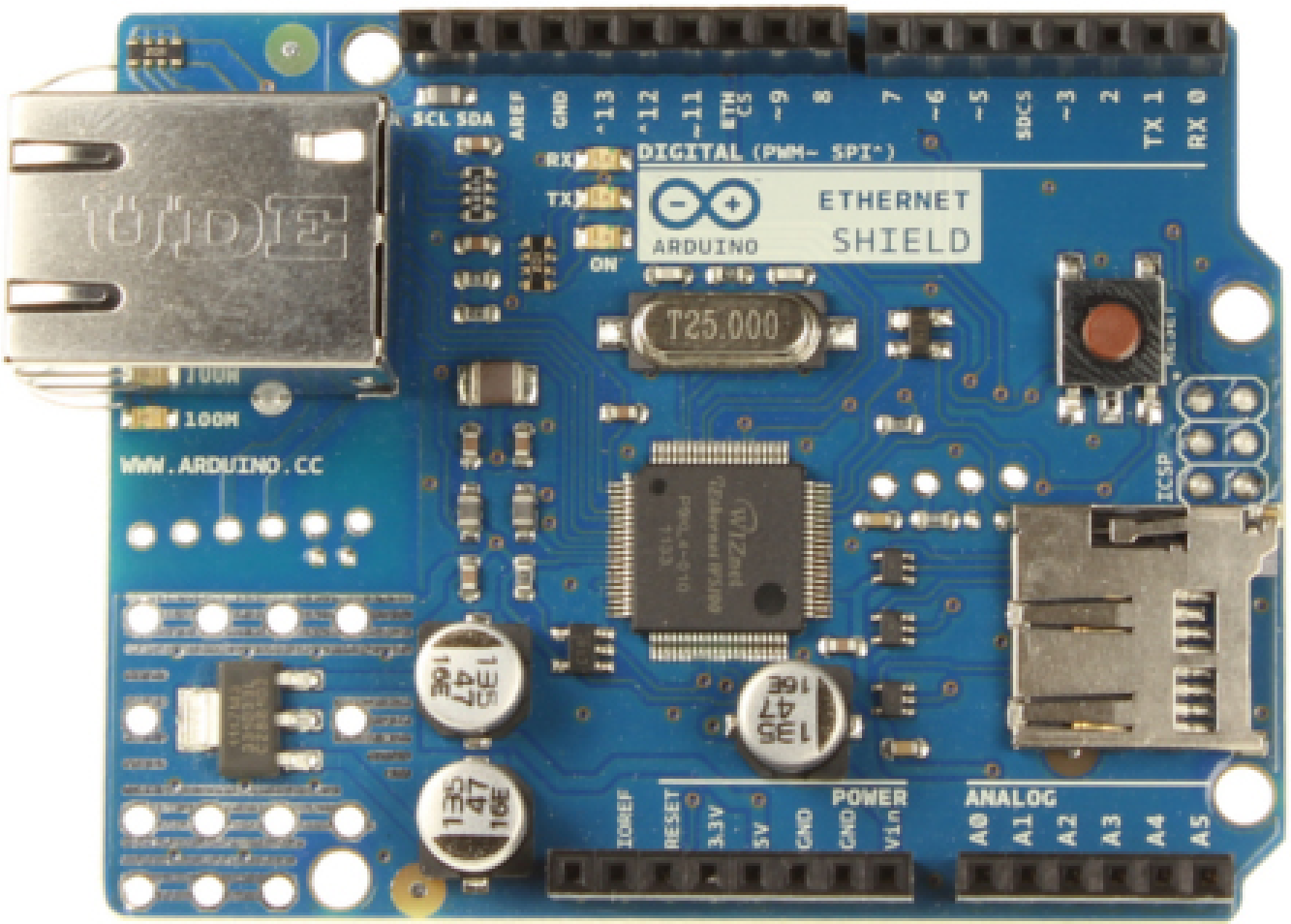
Summary

Let's add network

Example

- Ethernet
- Wi-Fi
- Using USB

Ethernet shield



Ethernet shield

Problems

- HTTPS not supported
- HTTP server: Developers generally do not implement authentication
- TCP/IP stack allowing IDLE Scan
- Weird behaviour as a server?

Ethernet shield

```
# hping3 -SA 192.168.100.2 -p 80 -c 1
HPING 192.168.100.2 (eno1 192.168.100.2): SA set,
 40 headers + 0 data bytes
len=46 ip=192.168.100.2 ttl=128 DF id=5 sport=80
 flags=SA seq=0 win=2048 rtt=3.9 ms

--- 192.168.100.2 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
```

Ethernet shield

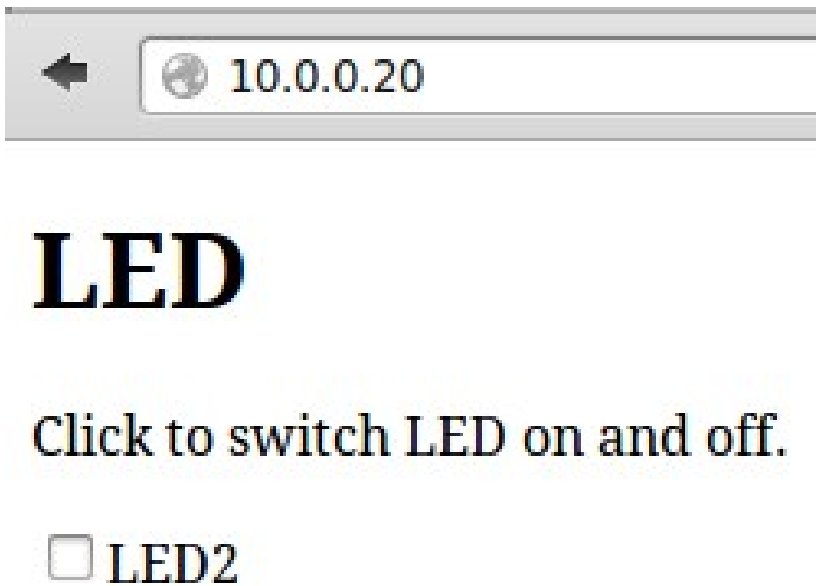
```
# hping3 -c 5 -p 80 192.168.100.2
HPING 192.168.100.2 (eno1 192.168.100.2): NO FLAGS are set,
 40 headers + 0 data bytes
len=46 ip=192.168.100.2 ttl=128 DF id=6 sport=80 flags=R
 seq=0 win=0 rtt=3.9 ms
len=46 ip=192.168.100.2 ttl=128 DF id=7 sport=80 flags=R
 seq=1 win=0 rtt=3.8 ms
len=46 ip=192.168.100.2 ttl=128 DF id=8 sport=80 flags=R
 seq=2 win=0 rtt=3.8 ms
len=46 ip=192.168.100.2 ttl=128 DF id=9 sport=80 flags=R
 seq=3 win=0 rtt=3.8 ms
len=46 ip=192.168.100.2 ttl=128 DF id=10 sport=80 flags=R
 seq=4 win=0 rtt=3.7 ms
```

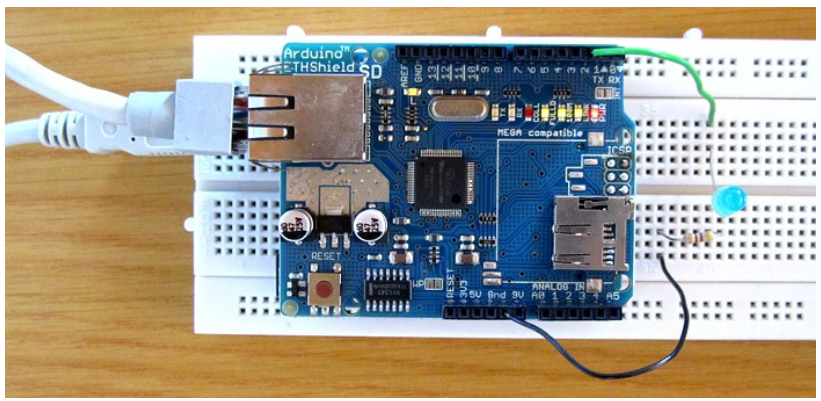
Ethernet shield

Having fun

- MiTM
- nmap
- Nessus

Wi-fi





https://startingelectronics.org/tutorials/arduino/ethernet-shield-web-server-tutorial/web-server-LED-control/

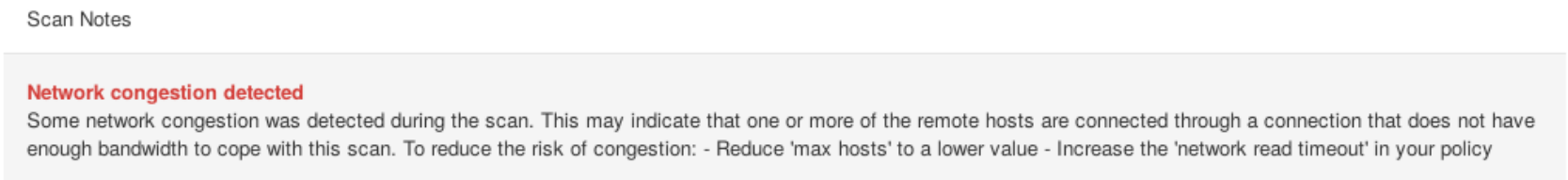
Ethernet shield

Having fun

- MiTM: it works
- nmap: it works
- Nessus: it works but...

Ethernet shield

First scan: classic policy



Ethernet shield

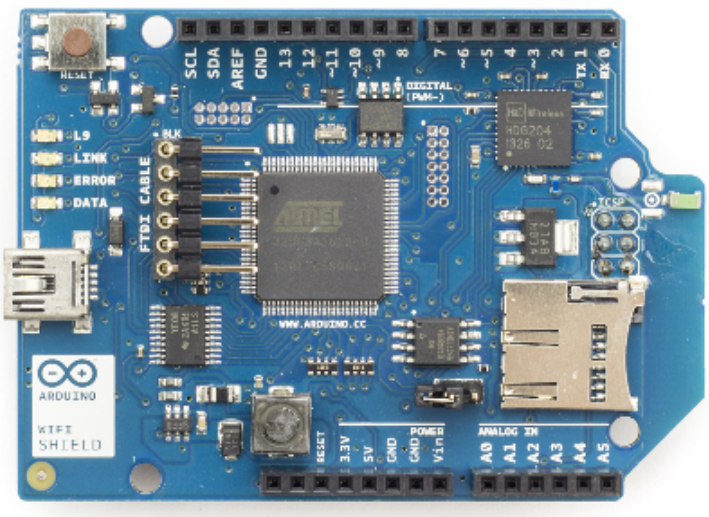
Second scan: customized policy

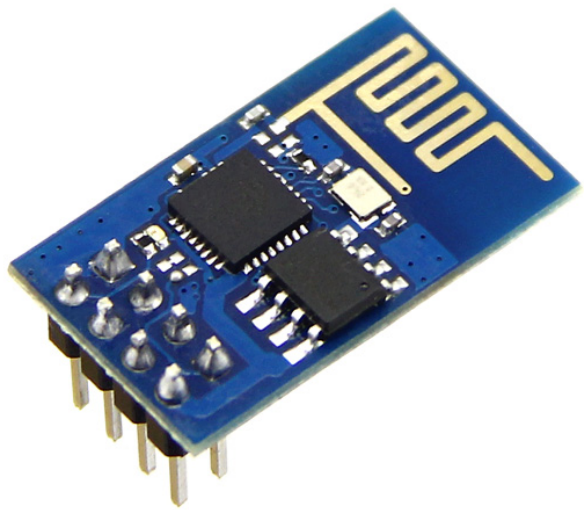
Ethernet shield

After Nessus

- MCU was hot
- Arduino program was not loading
- Arduino worked back after re-uploading the sketch

Wi-Fi


RESET
SCL
SDA
AREF
GND
DIGITAL (PWM~)
L9
LINK
ERROR
DATA
FTDI CABLE
WWW.ARDUINO.CC
ARDUINO
WIFI SHIELD
POWER
ANALOG IN



Wi-Fi

Problems

- As for the Ethernet Shield (not tried yet)
- Store a (your?) Wi-Fi key

Wi-Fi

Read the ihex

```
$ cd arduino-1.6.9/hardware/tools/avr/bin
$ ./avrdude_bin -p m328p -P /dev/ttyACM0 -c arduino
 -U flash:r:unicorn-diy-project.hex:i
 -C ../etc/avrdude.conf
```

Convert to bin

Notes about *avrdude*

Use -C option

```
$ cd arduino-1.6.9/hardware/tools/avr/bin
$ ./avrdude_bin -p m328p -P /dev/ttyACM0 -c arduino
-U flash:r:unicorn-diy-project.hex:i
avrdude: can't open config file "/home/jenkins/jenkins/
 jobs/toolchain-avr-linux64/ workspace/objdir/etc/
 avrdude.conf": No such file or directory
avrdude: error reading system wide configuration file "
 /home/jenkins/jenkins/ jobs/toolchain-avr-linux64/
 workspace/objdir/etc/avrdude.conf"
```

Notes about *avrdude*

Extracted file is Intel HEX format, conversion to bin

```
import bincopy

f = bincopy.File()
with open("unicorn-diy-project.hex", "r") as fin:
f.add_ihex(fin)

print f.as_binary()
```

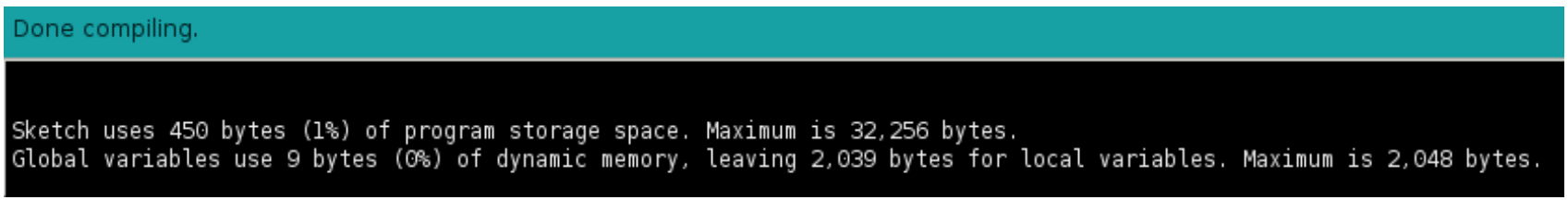
https://pypi.python.org/pypi/bincopy

Wi-Fi

```
$ strings unicorn-diy-project.bin
!P1
/_?O
N__Oa
/_?O
N__Oa
f'x/
[...]
yourHiddenKey
yourSSID
Attempting to connect to WPA network...
Couldn't get a wifi connection
```

Wi-Fi

When uploading a new program, flash is not fully erased



Wi-Fi

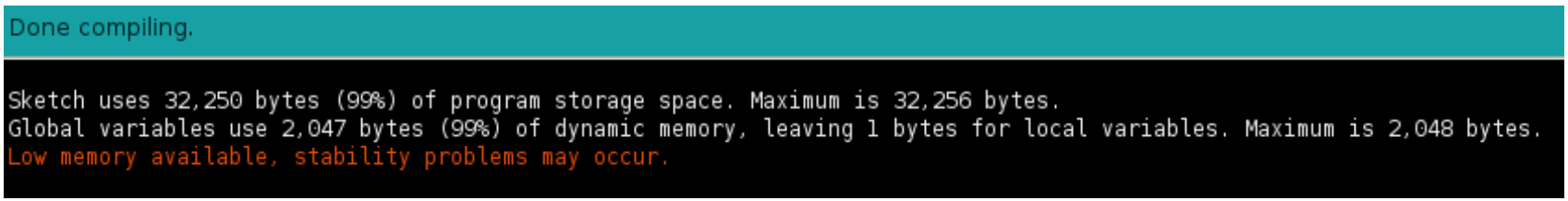
bin file

```
!P1
/_?O
N__Oa
/_?O
N__Oa
f'x/
[...]
yourHiddenKey
yourSSID
Attempting to connect
 to WPA network...
Couldn't get a wifi
 connection
```

reprogrammed bin file

```
!P1
/_?O
N__Oa
/_?O
N__Oa
f'x/
[...]
yourHiddenKey
yourSSID
Attempting to connect to
 WPA network...
Couldn't get a wifi
 connection
```

Let's full memory



Protection

Memory Lock Bits			
Mode	LB1	LB2	Protection Type
1	1	1	Unprogrammed, no protection enabled
2	0	1	Further Programming disabled, Read back possible
3	0	0	Further programming and read back is disabled

This may be bypass using *Goodfet*

http://electronics.stackexchange.com/questions/53282/protecting-avr-flash-from-reading-through-isp

"Free" network "shield"

A computer using Processing

http://playground.arduino.cc/Interfacing/Processing

"Free" network "shield"

Example - Connected light bulb

- From: Getting Started with Arduino: The Open Source Electronics Prototyping Platform (Make)
- Changing bulb color depending of peace, love and arduino words occurency on a blog
- Internet access through serial with Processing

"Free" network "shield"

Problems

- Do not let default *pi* accounts
- On Linux users need to be in *dialout* group

"Free" network "shield"

Do not

```
sudo processing
```

Do

```
sudo usermod -a -G dialout YouUsername
```

Summary

Remote control/Authentication

Example

- Infra Red
- Radio
- RFID

Infrared

From **An Introduction to Infrared Technology: Applications in the Home, Classroom, Workplace, and Beyond ...**

IR Advantages:

4. Higher security: directionality of the beam helps ensure that data isn't leaked or spilled to nearby devices as it's transmitted

http://trace.wisc.edu/docs/ir_intro/ir_intro.htm

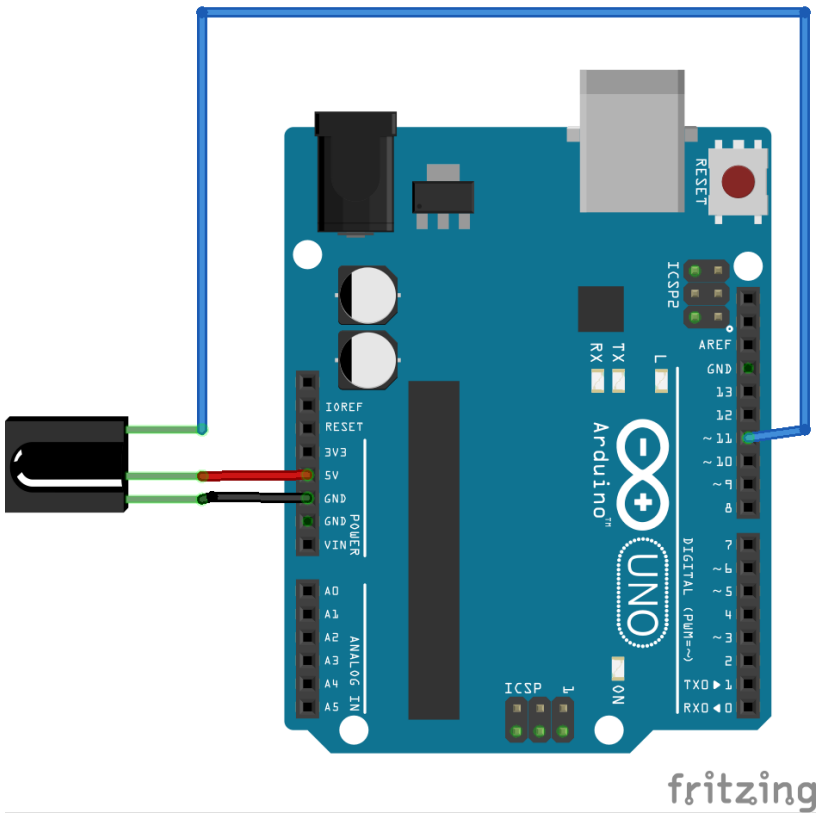
Infrared

From **Major Malfunction - DEFCON 13**

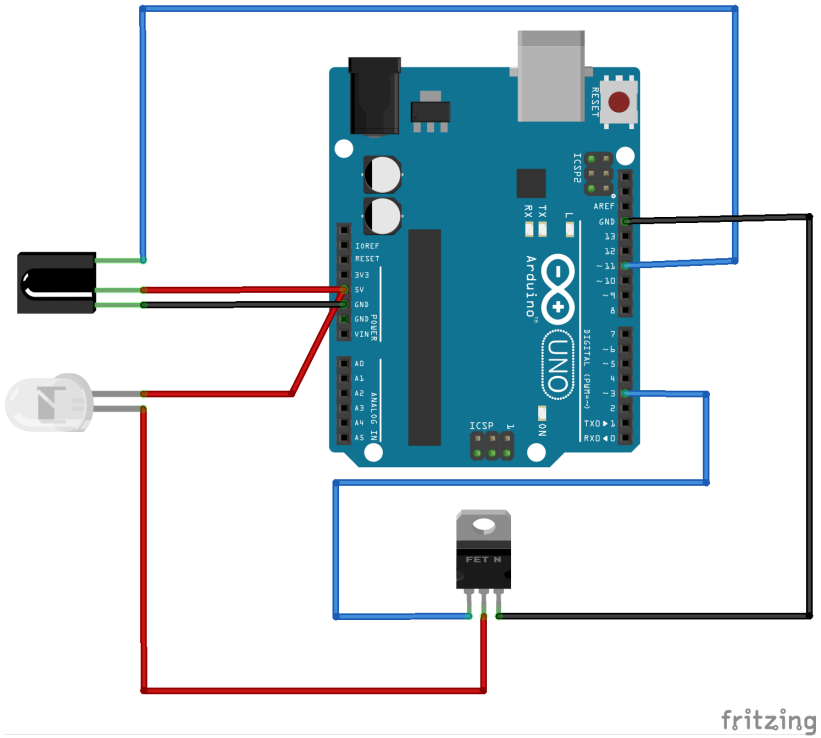
IR is the ultimate in 'security by obscurity'
https://www.defcon.org/images/defcon-13/dc13-presentations/DC_13-MajorMalfunction.pdf

Infrared

Receive data (30 €)



Replay data (30 €)



Infra Red

So what?

- Easy to read
- Easy to replay
- Easy to fuzz

Low cost 433 MHz

Vous en avez un à vendre ? Vendez le vôtre

433Mhz RF Module Émetteur Récepteur Télécommande Pour Projet Arduino ARM MCU

Etat : **Neuf**

Quantité : 1

Plus de 10 disponibles
295 objets déjà vendus

1,00 EUR

Achat immédiat

Ajouter au panier

Ajouter à votre liste d'Affaires à suivre
Ajouter à la collection
Suivi par 13 personnes

Plus de 67 % vendus | Quantité disponible limitée | Livraison gratuite

Ajouter à votre liste d'Affaires à suivre

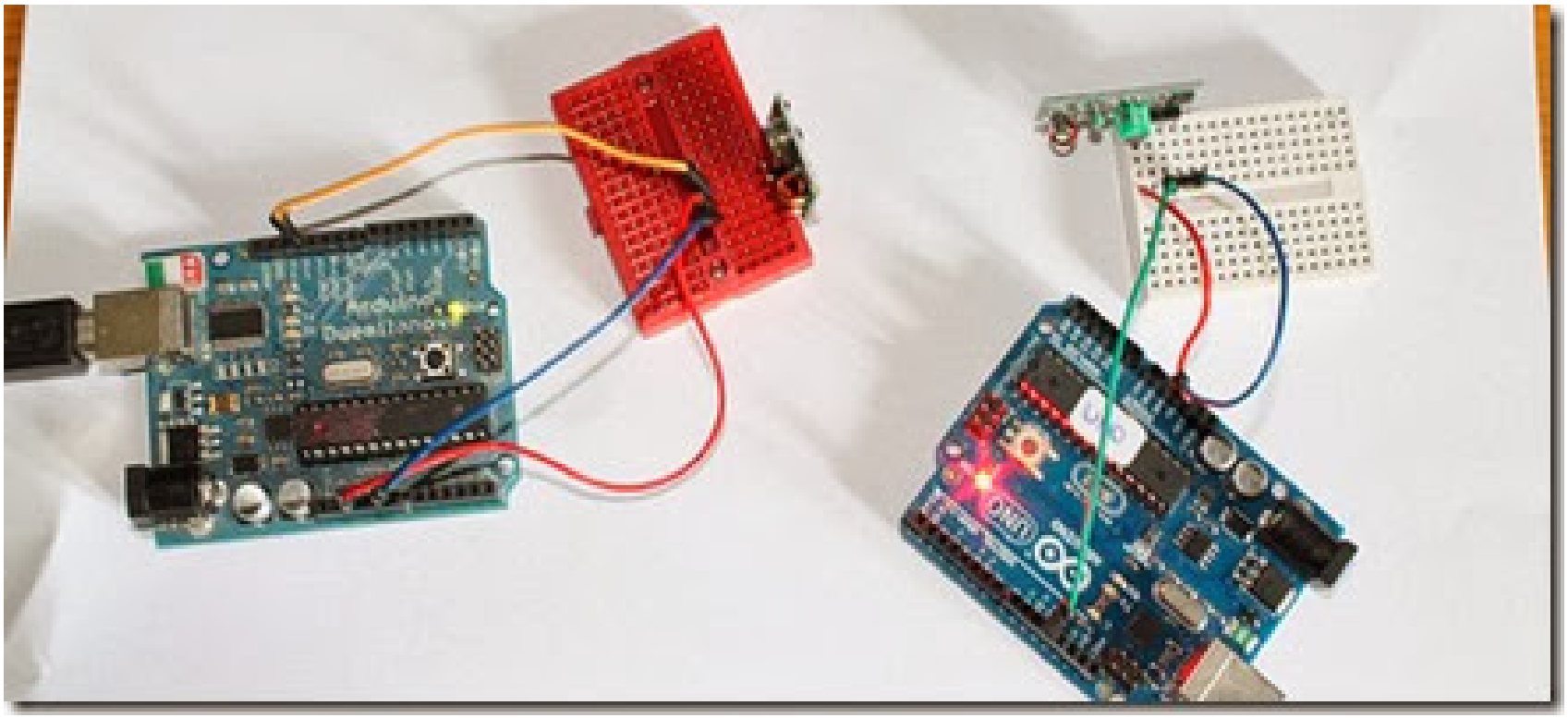
Détails sur le vendeur
gamesalor (349237) Perso
97,1% Evaluations positives
S'abonner à ce vendeur
Afficher les autres objets
Visiter la Boutique : gamesalor
Inscrit comme vendeur professionnel

Livraison : **GRATUIT** Autres | Détails
Cliquez ici pour plus de détails sur la livraison internationale.
Lieu où se trouve l'objet : **Hongkong, Hong Kong**
Lieu de livraison : **France** Afficher les exclusions

Délai de livraison : Estimé entre le **mer. 13 juil. et le mer. 17 août**

Paiements : PayPal CB Maestro VISA MasterCard

Radio



http://myhowtosandprojects.blogspot.fr/2014/01/arduino-rf-transmitter-receiver-mx-fs.html

Radio

Record

```
hackrf_transfer -r unicorn -f 433930000 -s 20
```

Replay

```
hackrf_transfer -t unicorn -f 433930000 -s 20 -x 10
```

RFID

Remember

- ID card is not unique
- Cards also have vulnerabilities (MIFARE 1K)

Summary

Case

Physical access

- USB port
- PIN
- Video port
- SD Card

Case

USB

- Dump the flash (*avrdude*)
- Plug keyboard, network...

Case - Adding USB

CIRCLean
USB Sanitizer

https://www.circl.lu/projects/CIRCLean/
https://github.com/CIRCL/Circlean

Case - Adding keyboard

Adding keyboard to CIRCLean

```
/usr/bin/timidity /opt/midi/sepultura-refuse_resist.mid &
echo $! > /tmp/music.pid
pmount /dev/sda1
cd /media/sda1
mkdir -p FROM_PARTITION_1/logs
echo '2015-02... > FROM_PARTITION_1/logs/processing.log
echo '2015-02... >> /FROM_PARTITION_1/logs/processing.log
echo 'MALICIOUS' > FROM_PARTITION_1/safe_pdf.pdf.html
pumount /dev/sda1
kill -9 $(cat /tmp/music.pid)
```

Case - Adding network

Adding USB Ethernet on CIRCLean

```
Nmap scan report for 192.168.100.89
Host is up (0.00064s latency).
PORT   STATE  SERVICE
22/tcp closed ssh
MAC Address: 00:09:72:83:62:58 (Securebase)
```

Case

PIN

- Dump the flash
- Flash firmware

Case

Video port (on screen)

- Can be used for display unapropriated content
- (not DIY specific) examples:
  - 2015/08: Hackers broadcast porn on TV screens at Brazil bus depot (www.i24news.tv/en/news/international/americas/81400-150808-hackers-broadcast-porn-on-tv-screens-at-brazil-bus-depot)
  - 2015/10: Target stores attacked by pornographic pranksters (http://www.bbc.com/news/technology-34556644)

Case

SD card

- Sensitive data: encryption
- Prevent your code from crashing if the card is removed

Summary

Android - Developing its own App

- Allow unsigned apk installation
- Enable Debug Mode

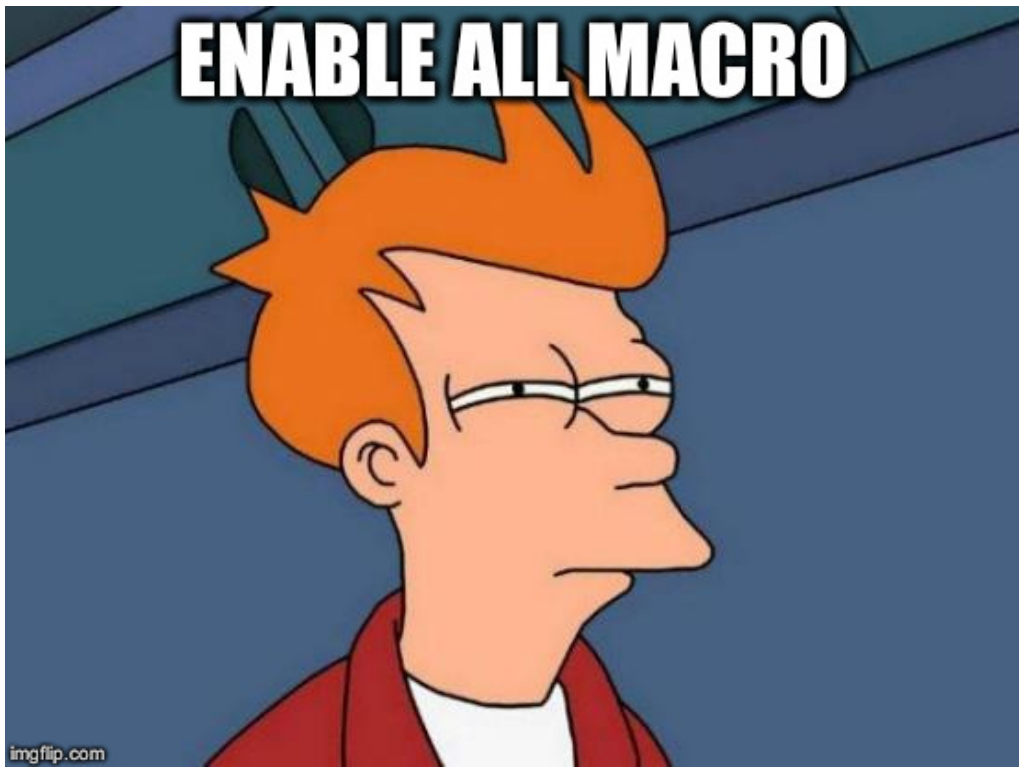
App

Excel

- PLX-DAQ: Excel Macro receiving data from Arduino
- OpenDaqCalc: For LibreOffice Calc

http://electroniqueamateur.blogspot.fr/2014/10/transmettre-les-donnees-darduino-vers.html

App



Summary

Cloud

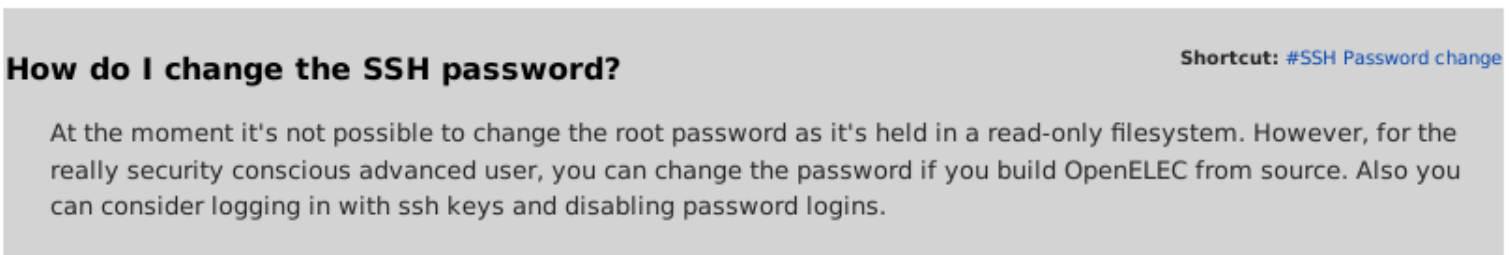
What could go wrong?

- Default password / no password
- No encryption
- Vulnerabilities in software
- Scripts/Software running as *root*

Default password

OpenElec

- SSH password cannot be changed
- SSH disabled by default since 3.0.6 (15 June 2013)



How do I change the SSH password?

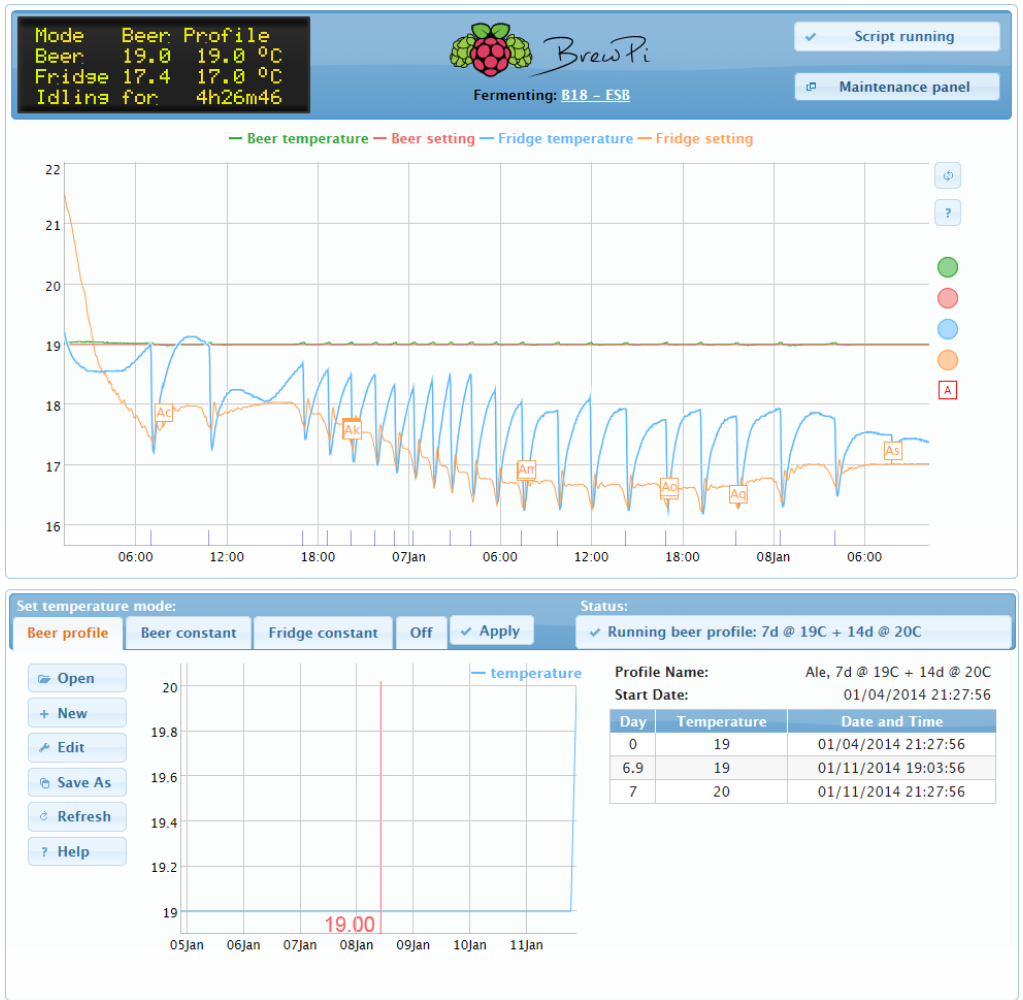
Shortcut: #SSH Password change

At the moment it's not possible to change the root password as it's held in a read-only filesystem. However, for the really security conscious advanced user, you can change the password if you build OpenELEC from source. Also you can consider logging in with ssh keys and disabling password logins.

http://wiki.openelec.tv/index.php/OpenELEC_FAQ

No password

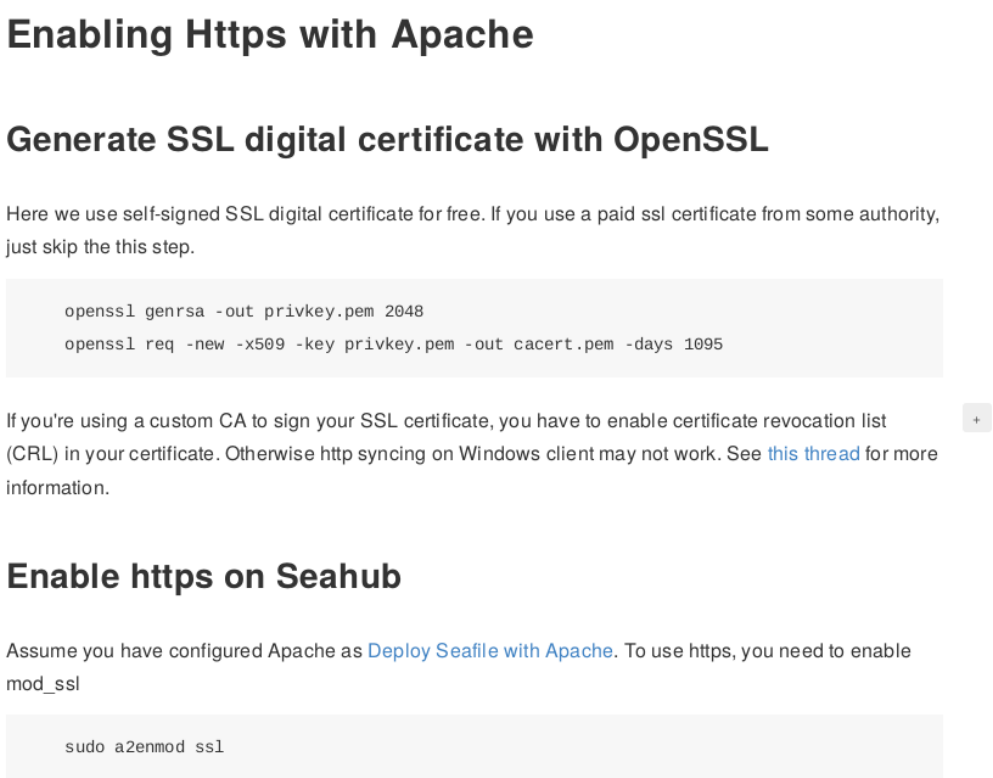
BrewPi (without authentication) web interface



Pull request for authentication bynzjoel1234: https://github.com/BrewPi/brewpi-www/pull/61

No encryption

Generally no by default, example Seafile



Enabling Https with Apache

Generate SSL digital certificate with OpenSSL

Here we use self-signed SSL digital certificate for free. If you use a paid ssl certificate from some authority, just skip the this step.

```
openssl genrsa -out privkey.pem 2048
openssl req -new -x509 -key privkey.pem -out cacert.pem -days 1095
```

If you're using a custom CA to sign your SSL certificate, you have to enable certificate revocation list (CRL) in your certificate. Otherwise http syncing on Windows client may not work. See this thread for more information.

Enable https on Seahub

Assume you have configured Apache as Deploy Seafile with Apache. To use https, you need to enable mod_ssl

```
sudo a2enmod ssl
```

http://manual.seafile.com/deploy/https_with_apache.html

Vulnerabilities in software

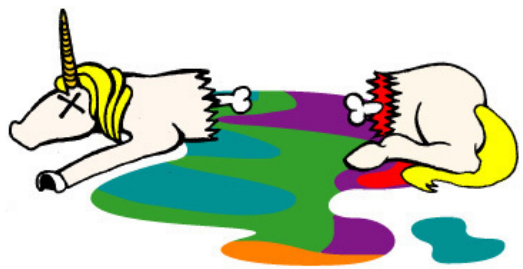
BrewPi: Flash the Arduino

Vulnerabilities in software

BrewPi: Flash the Arduino... Wait!

Vulnerabilities in software

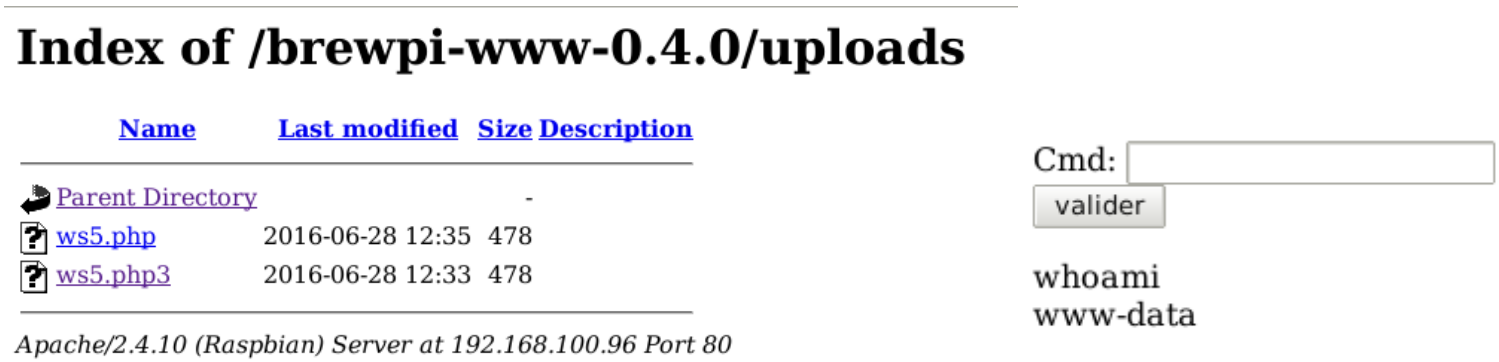
Remotely flashing controller



WITHOUT authentication

Vulnerabilities in software

BrewPi: Flash the Arduino



Summary

Control points

The DIY project

- Is it using secure protocols/channels?
- Who will have physical access to it?
- What logical entry points will it use?
- Will your board store sensitive data?
- Has your board stored sensitive data?
- Check for (security) updates and apply them.

Summary

Control points

Your network

- Which interaction with my network?
- Which (direct) interaction with my systems?
- Did I disabled some security features during installation?
- Check for (security) updates and apply them.

Control points

Your network

- Look there: https://2015.rmll.info/home-sweet-home
- And there: https://2015.rmll.info/let-s-talk-about-selks
- And also there (in French): http://static.sstic.org/rumps2016/SSTIC_2016-06-02_P12_RUMPS_11.mp4
- And also there (in English): https://workshop.netfilter.org/2016/wiki/index.php/File:Amsterdam.pdf

Questions?