

Hands-on security for DIY projects

A. Cervoise

antoine.cervoise@gmail.com



July 6, 2016

Summary

Introduction

Who am I?

IoT

DIY IoT

Bad examples (I played with)

Control points

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

Introduction

Who am I?

IoT

DIY IoT

Bad examples (I played with)

Control points

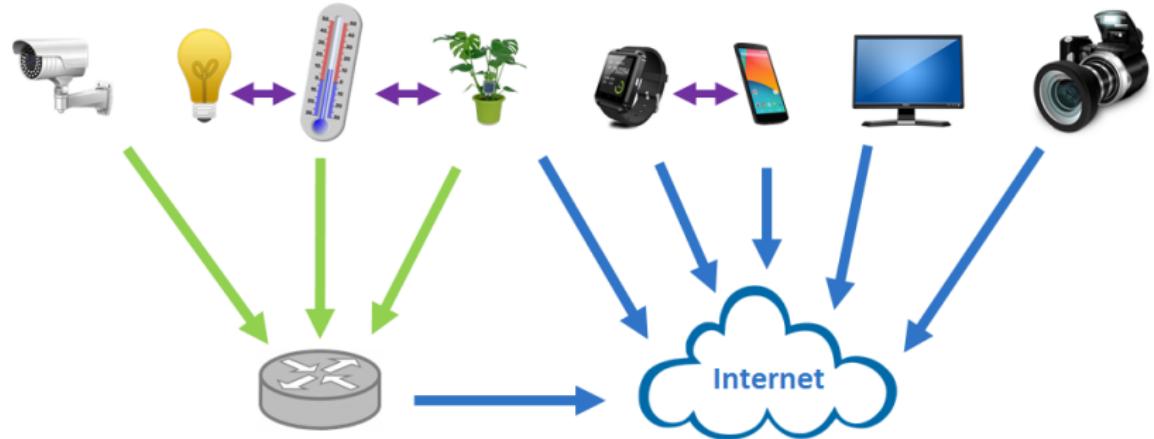
Internet of Things

The internet of things (IoT) is the network of physical devices, vehicles, buildings and other items embedded 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





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

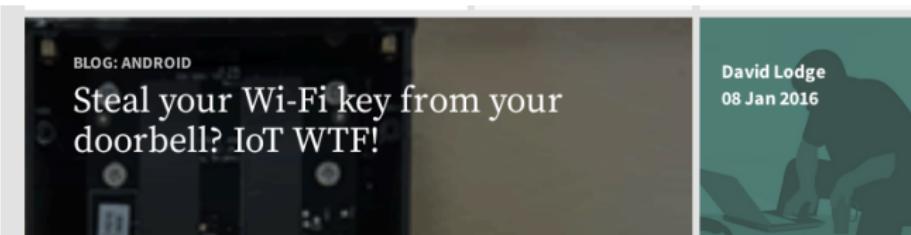
August 6, 2015 by Alex Drozhzin | Featured Post, News, Security, Threats

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



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/>

Technology

VTech hack: Parents complain of Christmas disappointment

By Kevin Rawlinson
BBC News

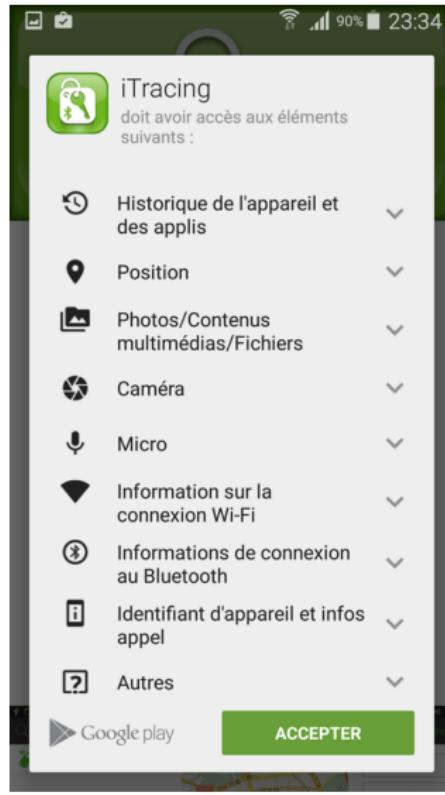
© 5 January 2016 | Technology

 Share



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

Internet of Threats



Internet of Threats



NEW DEAL Prise connectée Wi-Fi smart plug Eco SPEco

4 ★★★★☆ 3 avis dont 2 ont la note maximale 5/5

Donnez votre avis Poser une question

Plus que 3 articles en Stock !

Vendu et expédié par Colisdiscount

Dépêchez-vous, plus que **8h 32min 05sec** pour être livré après demain !

Prise connectée Wi-Fi - Garez l'allumage de vos appareils électriques depuis n'importe où avec la prise SPEco de New Deal - Téléchargez l'application gratuite New Deal Smart Plug - Branchez votre appareil sur la prise - Utilisable à distance en 3G/HG/Wi-Fi - Programmation des horaires de fonctionnement.

[Voir la présentation du produit](#)

39€99
Dont 0,14 € d'éco participation

Bien sûr épuisé !
Plus que 3 articles disponibles

+ 3% de remise supplémentaire
en souscrivant à la carte Colisdiscount [Détails](#)

Quantité :

JE LE VEUX

Internet of Things



Internet of Threats



A screenshot of a web browser window. The address bar shows the URL: `kdsldkfjslkdcom.s512.000pc.net/down/new_deal_smart_plug.apk`. The main content area displays a red warning message:

Page malveillante !

 La page web sur `kdsldkfjslkdcom.s512.000pc.net` a été signalée comme étant une page malveillante et a été bloquée sur la base de vos préférences de sécurité.

Les pages malveillantes essaient d'installer des programmes qui volent des informations personnelles, qui utilisent votre ordinateur pour en attaquer d'autres ou qui endommagent votre système.

Certaines pages distribuent intentionnellement des logiciels malveillants, mais beaucoup sont compromises sans la permission de leurs propriétaires ou sans qu'ils en aient connaissance.

[Sortir d'ici](#) | [Pourquoi cette page a-t-elle été bloquée ?](#)

[Ignorer cet avertissement](#)

Internet of Threats

The screenshot shows the Google Play Store interface. The left sidebar is visible with categories like Applications, Mes applications, Acheter, Jeux, Famille, Choix de l'équipe, Mon compte, Mon activité Play, Ma liste de souhaits, Utiliser un code, Acheter une carte cadeau, and Guide à l'usage des parents. The main content area displays the "New Deal Smart Plug" app page. The app icon features a red circle with a white 'n' and 'd' logo above the text "New Deal SMART.PLUG". The app details include the developer "New Deal", category "Style de vie", rating "PEGI 3", and a note that it's compatible with multiple devices. Three screenshots of the app's user interface are shown: one showing a power button instruction, another for device pairing, and a third showing a menu with options like "Add New Device", "Share", "Help", "Checking New Version", "Style", and "About".

New Deal Smart Plug

New Deal Style de vie

PEGI 3

Cette application est compatible avec l'ensemble de vos appareils.

Ajouter à la liste de souhaits

Installer

Long press the power button for 5 seconds till the power indicator starts to flash quickly. After one more touch the wi fi indicator will start to flash quickly for 5 seconds. Now the phone can connect with wi fi module when the WiFi indicator flashes quickly. Otherwise it can not be connected.

Click the icon if the indicator does not flash quickly.

Add New Device

Device

Password

Show Password

Add New Device

Share

Help

Checking New Version

Style

About

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



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: closesucceed			
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

Introduction

Who am I?

IoT

DIY IoT

Bad examples (I played with)

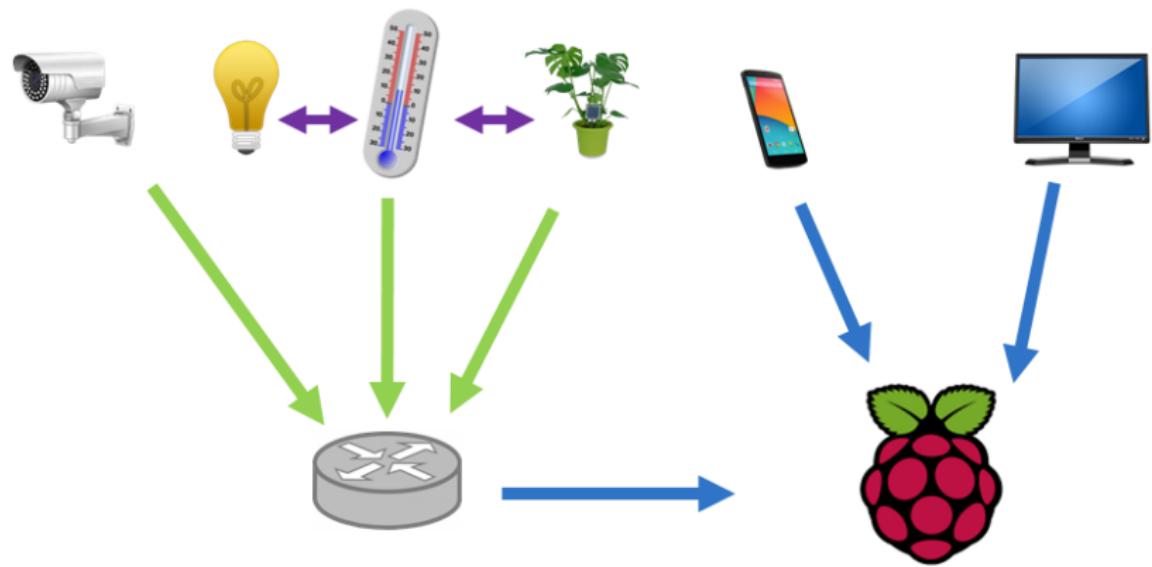
Control points

Not the subject

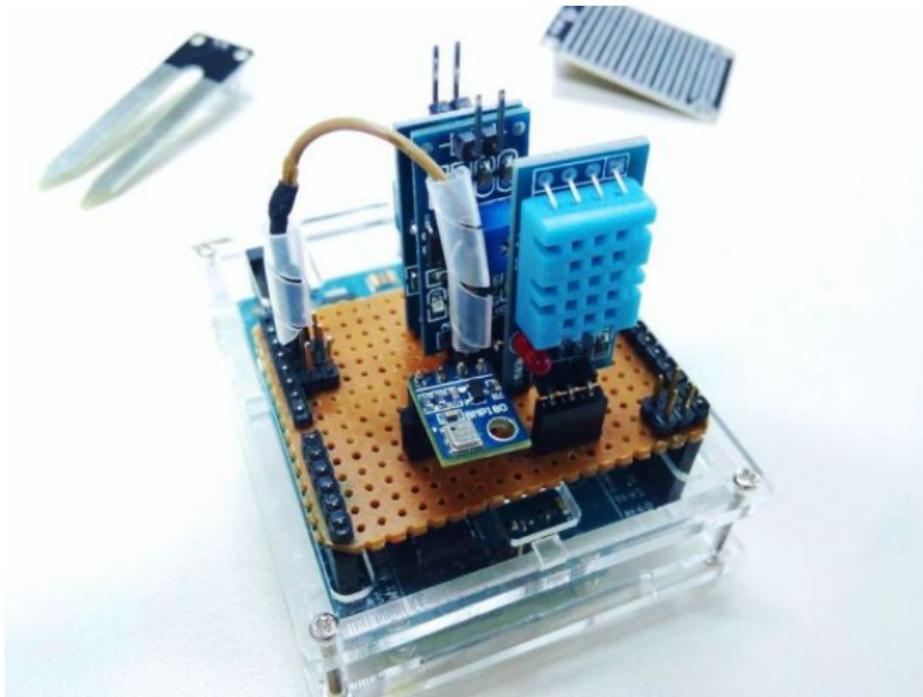
Commercial product with

- ▶ Central controller
- ▶ Hardware modules
- ▶ Smartphone apps

DIY IoT



DIY IoT



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

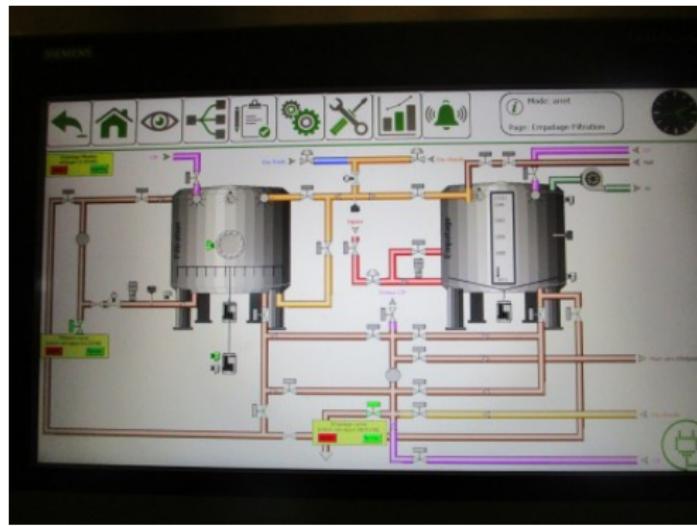
DIY "ICS"

Let's brew beer

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

DIY "ICS"

Siemens ICS for Brasserie de Meaux



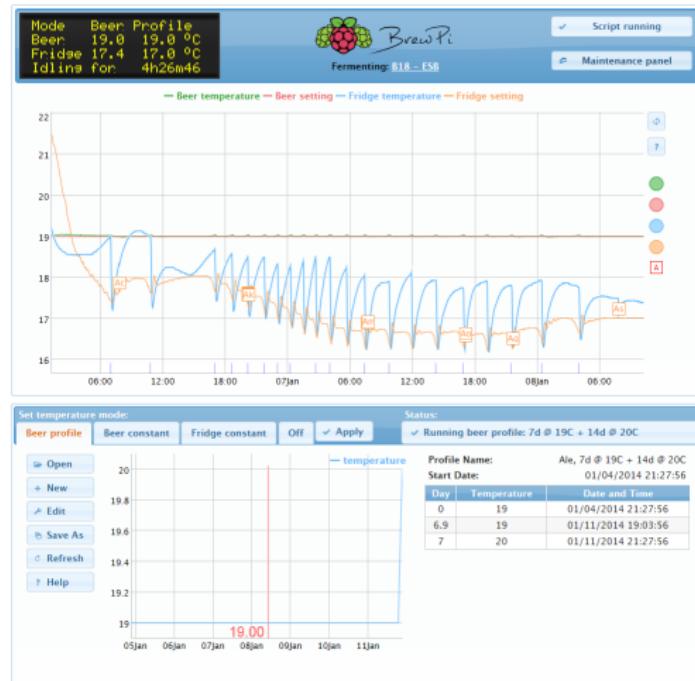
DIY "ICS"

BrewPi

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

DIY "ICS"

BrewPi (without authentication) web interface



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

Bad examples through

- ▶ Blogs
- ▶ Magazines
- ▶ Vendors

And control points to improve your DIY projects

Summary

Introduction

Bad examples (I played with)

Network

Remote control / Authentication

Case

App

Cloud

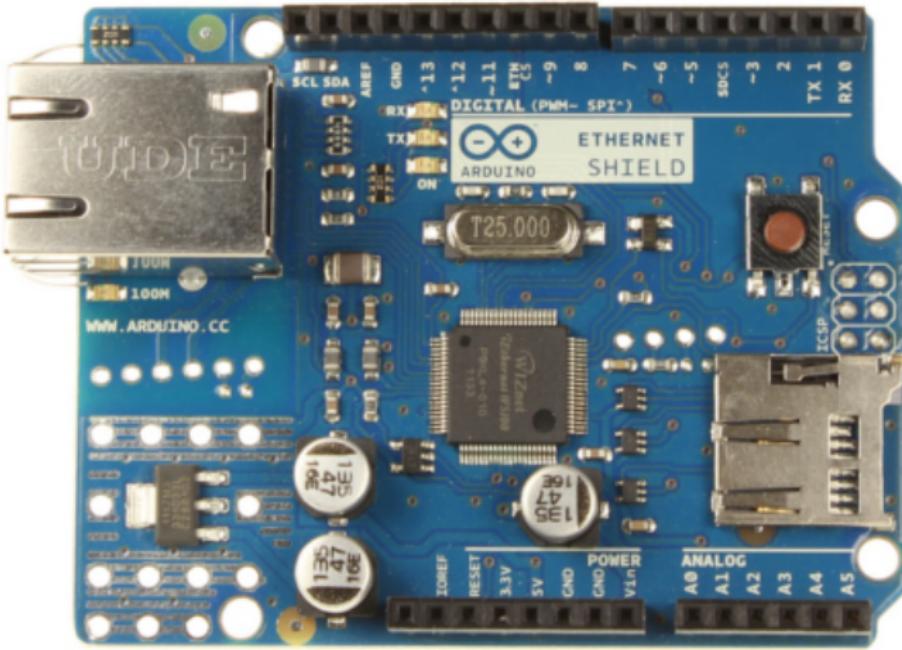
Control points

Let's add network

Example

- ▶ Ethernet
- ▶ Wi-Fi
- ▶ Using USB

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

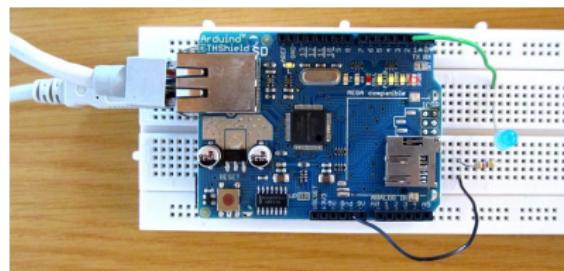


LED

Click to switch LED on and off.

LED2

<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

Scan Notes

Network congestion detected

Some network congestion was detected during the scan. This may indicate that one or more of the remote hosts are connected through a connection that does not have enough bandwidth to cope with this scan. To reduce the risk of congestion: - Reduce 'max hosts' to a lower value - Increase the 'network read timeout' in your policy

Ethernet shield

Second scan: customized policy

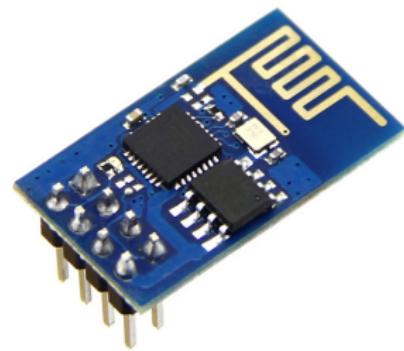
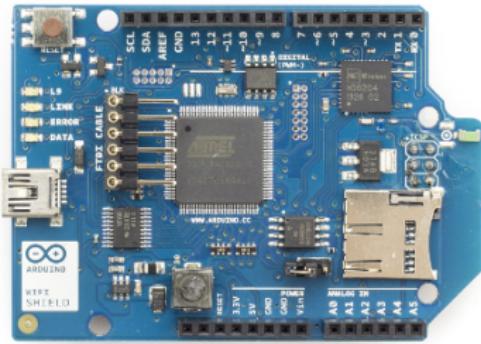


Ethernet shield

After Nessus

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

Wi-Fi



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 *avrduude*

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 *avrduude*

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
/_?0
N__0a
/_?0
N__0a
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

```
Done compiling.
```

```
Sketch uses 450 bytes (1%) of program storage space. Maximum is 32,256 bytes.  
Global variables use 9 bytes (0%) of dynamic memory, leaving 2,039 bytes for local variables. Maximum is 2,048 bytes.
```

Wi-Fi

bin file

```
!P1  
/_?0  
N__0a  
/_?0  
N__0a  
f'x/  
[...]  
yourHiddenKey  
yourSSID  
Attempting to connect  
to WPA network...  
Couldn't get a wifi  
connection
```

reprogrammed bin file

```
!P1  
/_?0  
N__0a  
/_?0  
N__0a  
f'x/  
[...]  
yourHiddenKey  
yourSSID  
Attempting to connect to  
WPA network...  
Couldn't get a wifi  
connection
```

Let's full memory

Done compiling.

Sketch uses 32,250 bytes (99%) of program storage space. Maximum is 32,256 bytes.
Global variables use 2,047 bytes (99%) of dynamic memory, leaving 1 bytes for local variables. Maximum is 2,048 bytes.
Low memory available, stability problems may occur.

Protection

Memory Lock Bits			Protection Type
Mode	LB1	LB2	
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

Introduction

Bad examples (I played with)

Network

Remote control / Authentication

Case

App

Cloud

Control points

Remote control/Authentication

Example

- ▶ Infra Red
- ▶ Radio
- ▶ RFID

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

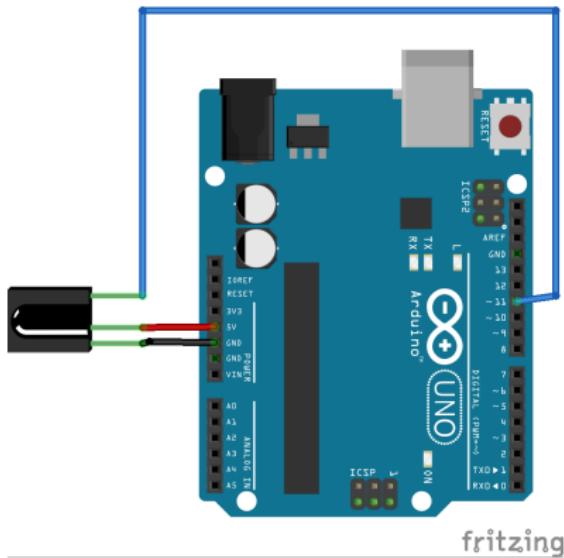
From Major Malfunction - DEFCON 13

IR is the ultimate in 'security by obscurity'

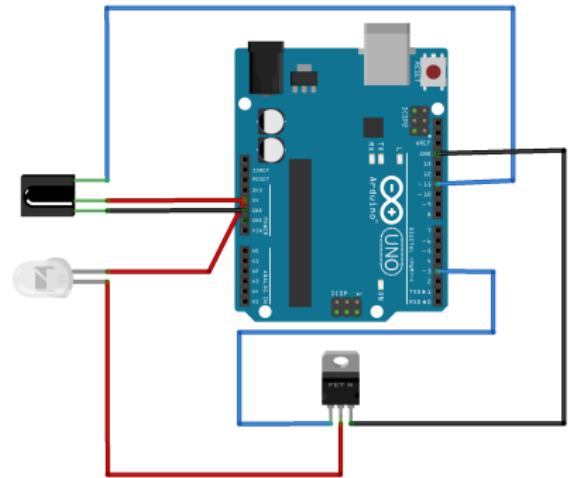
https://www.defcon.org/images/defcon-13/dc13-presentations/DC_13-MajorMalfunction.pdf

Infrared

Receive data (30 €)



Replay data (30 €)



fritzing

So what?

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

Radio

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)

97,1% Évaluations 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.

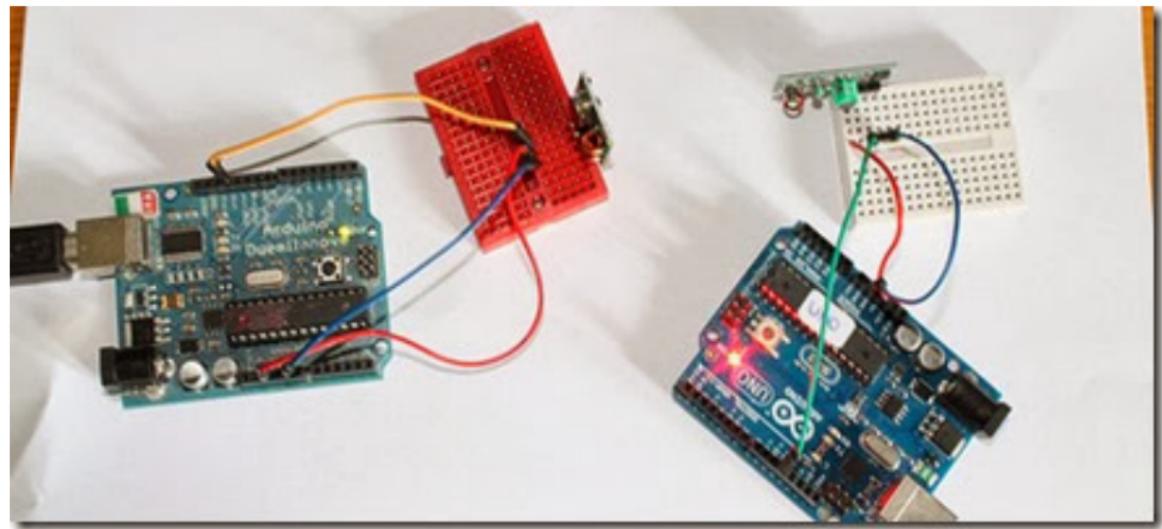
Lieu où se trouve l'objet : Hongkong, Hong Kong

Lieu de livraison : France [Afficher les expéditions](#)

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

Paiements :

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
```

Remember

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

Summary

Introduction

Bad examples (I played with)

Network

Remote control / Authentication

Case

App

Cloud

Control points

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/septultura-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

Video port (on screen)

- ▶ Can be used for display unappropriate 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

Introduction

Bad examples (I played with)

Network

Remote control / Authentication

Case

App

Cloud

Control points

Android - Developing its own App

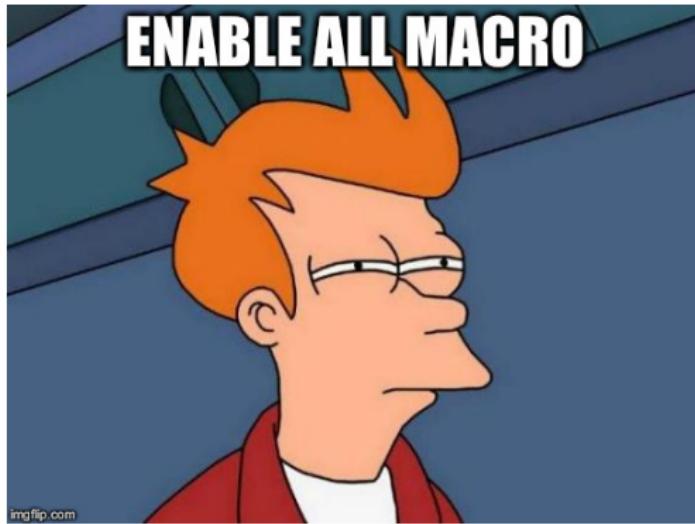
- ▶ Allow unsigned apk installation
- ▶ Enable Debug Mode

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

Introduction

Bad examples (I played with)

Network

Remote control / Authentication

Case

App

Cloud

Control points

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?

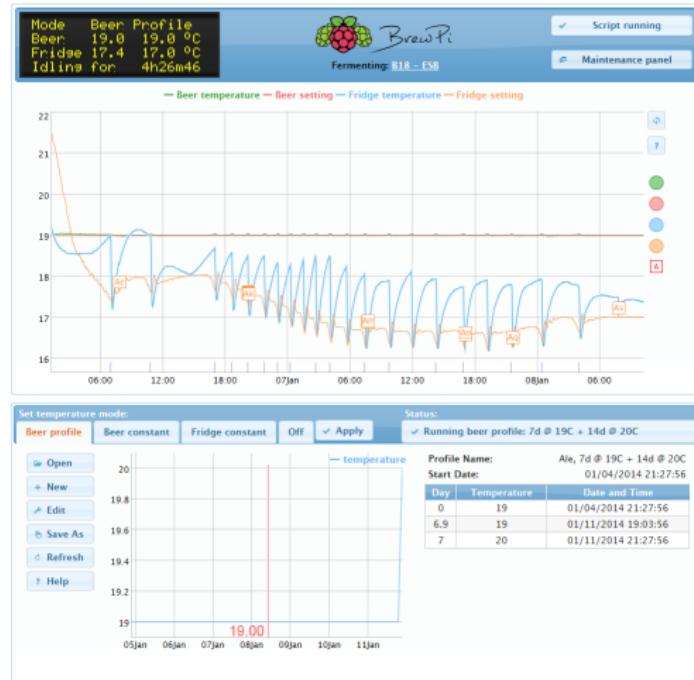
Shortcut: #SSH Password change

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 bynjoel1234: <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



Vulnerabilities in software

BrewPi: Flash the Arduino

Maintenance Panel X

Settings	View logs	Previous Beers	Control Algorithm	⚠ Script not running!
Device Configuration	Advanced Settings	Reprogram controller		

Here you can upload a firmware file which will be uploaded to the controller by the Python script. The script will automatically restart itself after programming. Just hit the back button on your browser to continue running BrewPi.

HEX file: **Program**

Board type:

Restore old settings after programming Yes No

Restore installed devices after programming Yes No

Vulnerabilities in software

BrewPi: Flash the Arduino... Wait!

Vulnerabilities in software

Remotely flashing controller



WITHOUT authentication

Vulnerabilities in software

BrewPi: Flash the Arduino

Index of /brewpi-www-0.4.0/uploads

Name	Last modified	Size	Description
 Parent Directory		-	
 ws5.php	2016-06-28 12:35	478	
 ws5.php3	2016-06-28 12:33	478	

Apache/2.4.10 (Raspbian) Server at 192.168.100.96 Port 80

Cmd:

whoami
www-data

Summary

Introduction

Bad examples (I played with)

The DIY project

Your network

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

Introduction

Bad examples (I played with)

The DIY project

Your network

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.

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?