

IRON-HID:

Create your own bad USB

Seunghun Han

Who am I ?



- Security researcher at NSR (National Security Research Institute of South Korea)
 - Operating system and firmware developer
- Author of the book series titled “64-bit multi-core OS principles and structure, Vol.1 & 2”
- a.k.a kkamagui (crow or raven in English)
 - @kkamagui1

Contents

- Background and Architecture of IRON-HID
- Hacking a Portable Charger
- Testing a Vulnerability of a Smartphones
- Testing a Vulnerability of a POS System and a PC
- Bonus

- Background and Architecture of IRON-HID
- Hacking a Portable Charger
- Testing a Vulnerability of the Smartphone
- Testing a Vulnerability of the POS System and the PC
- Bonus

IRON-HID Project?

IRON-HID

II

Human Interface Device
for making your tools

Features

- **Custom device + firmware + test agent program + Android smartphone program**
- **Various types of system exploitable**
 - POS (Point-of-Sale), PC, Android, etc.
- **Lightweight embedded hardware-based**
 - “Arduino” and “Teensy”
- **Open-source project!**
 - <https://github.com/kkamagui/IRON-HID>

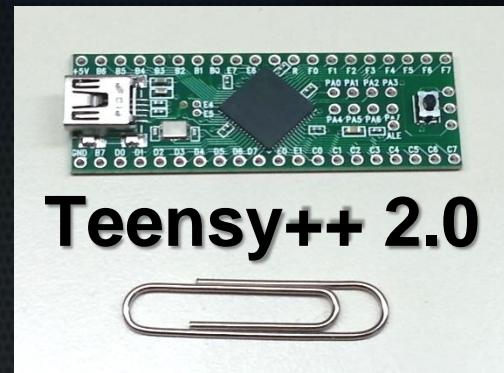
Arduino vs Teensy

Arduino



Arduino Mega

Teensy



Larger
(Palm size)

256KB Flash
(ATmega16U2 + ATmega2560)

60 I/O Pins

Smaller
(Paper-clip size)

128KB Flash
(AT90USB1286)

46 I/O Pins

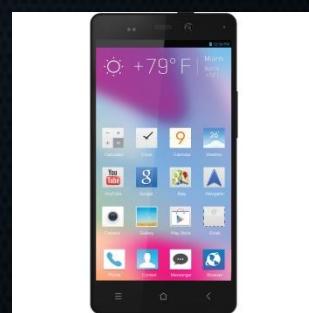
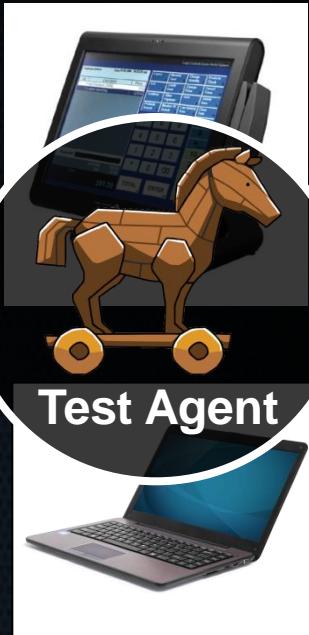
Arduino Sketch IDE is available!

Targets

Commander



Proxy Device



Attach



Custom Device

Target POS systems, PCs, smartphones

Test agent (TA) program

Send commands and events
Install a test agent program

Receive results of commands
(Results of shell, screens, files)

Custom device (in proxy devices)

IRON-HID firmware
(USB functions and a CD-ROM image)

Embedded hardware
(Low-powered hardware)

Wireless module
(WiFi, Bluetooth, Cellular, etc.)

Execute shell commands
Send keyboard events
Capture screens
Get files

Receive results of commands
Receive status of a proxy device

Security inspector' smartphone IRON-HID commander program

: IRON-HID component

IRON-HID Firmware

- Emulates **keyboard** and **mass-storage** device
 - It has one interrupt type endpoint for sending and logging keyboard events
 - It has two bulk type endpoints for installing the TA program
- Makes a custom **communication channel**
 - It has one control type endpoint for making a tunnel between the TA program and the Commander program

TA program and IRON-HID Commander

- TA program processes requests of Commander
 - Command Executions, Screen Captures, File Transfers
- Commander is an interface of pen-testers
 - It has control tab, command tab, key tab
 - Penetration tester uses each tab for testing security holes

Direction	Format	Description
Commander → TA program	C;<command>;	Commander requests that TA program executes a command and sends result to Commander
Commander → TA program	G;<filename>;	Commander requests that TA program sends a file to Commander
Commander → TA program	S;;	Commander requests that TA program captures a screenshot and sends it to Commander
TA program → Commander	F;;<64byte data>;	TA program sends results to Commander
Commander → Firmware	<Magic string 1>	Commander changes firmware's mode to command transfer mode
Commander → Firmware	<Magic string 2>	Commander changes firmware's mode to keyboard event mode
Commander → Firmware	<Magic string 3>	Commander requests that firmware installs TA program into host
Firmware → Commander	M;;<keyboard event>;	Firmware sends user's keyboard inputs to Commander
Firmware → Commander	D;;<debug message>;	Firmware sends debug messages to Commander

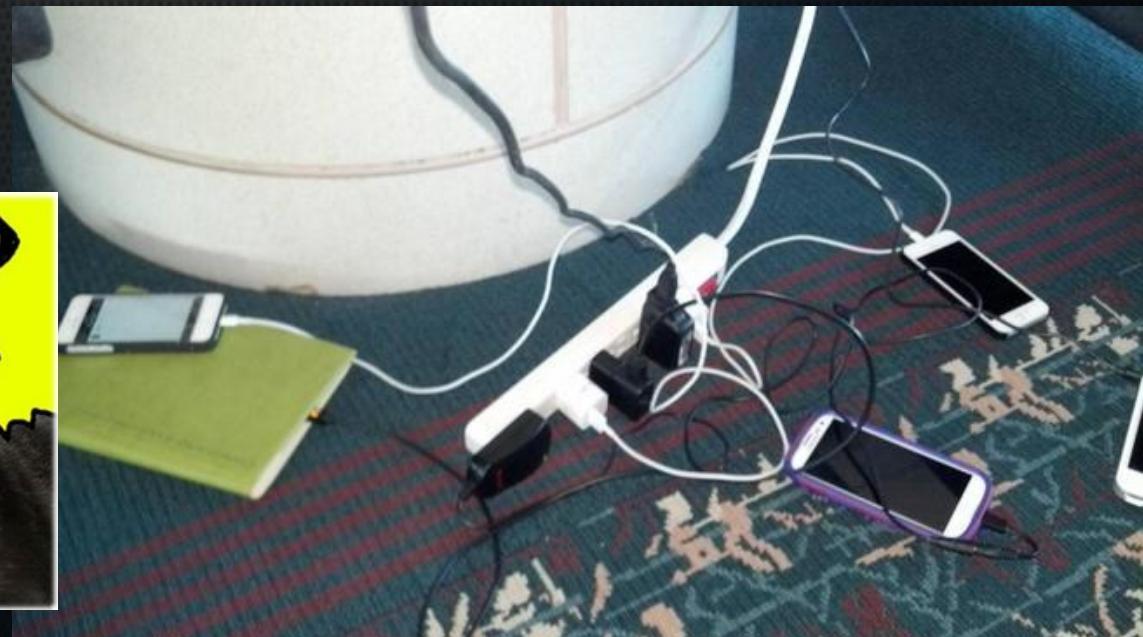
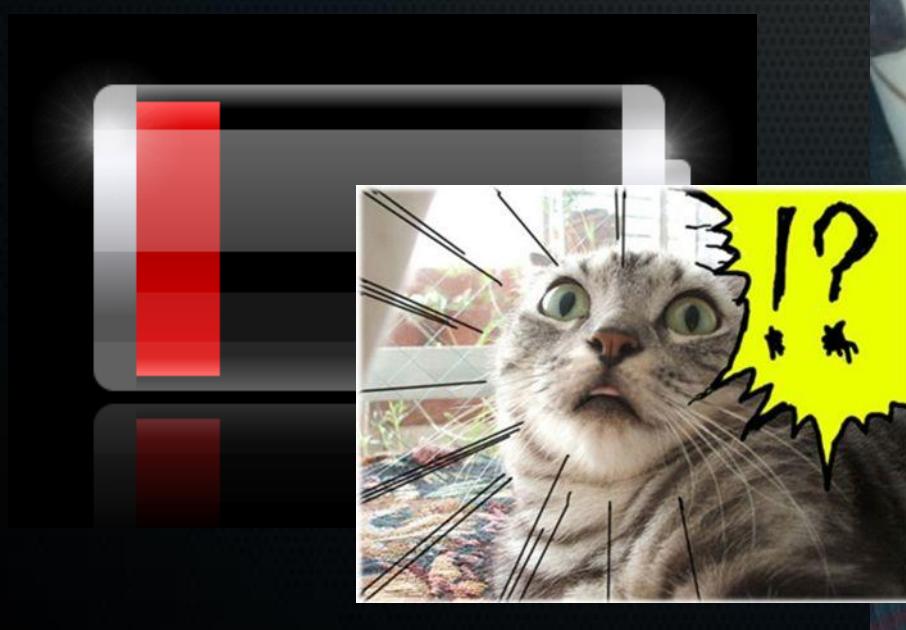
We are ready to launch!

Choose a target to

attach it

We want a portable charger

- **We use the smartphone everywhere!!**
 - We spend much time with the smartphone
 - But, it doesn't have enough battery
 - So, you should bring your charger or ...



So many portable chargers...



So many battery rental services...



Hey,

You totally believe
your portable charger?

PowerShock!!

- It is a portable charger, but not normal
 - It has **IRON-HID** inside it
- It can test **Android smartphones**
- It can test **POS(Point-Of-Sale) Systems**
- It can test **your PC**

It is a perfect **weapon** for
penetration testers

- Background and Architecture of IRON-HID
- Hacking a Portable Charger
- Testing a Vulnerability of the Smartphone
- Testing a Vulnerability of the POS System and the PC
- Bonus

Tools you need

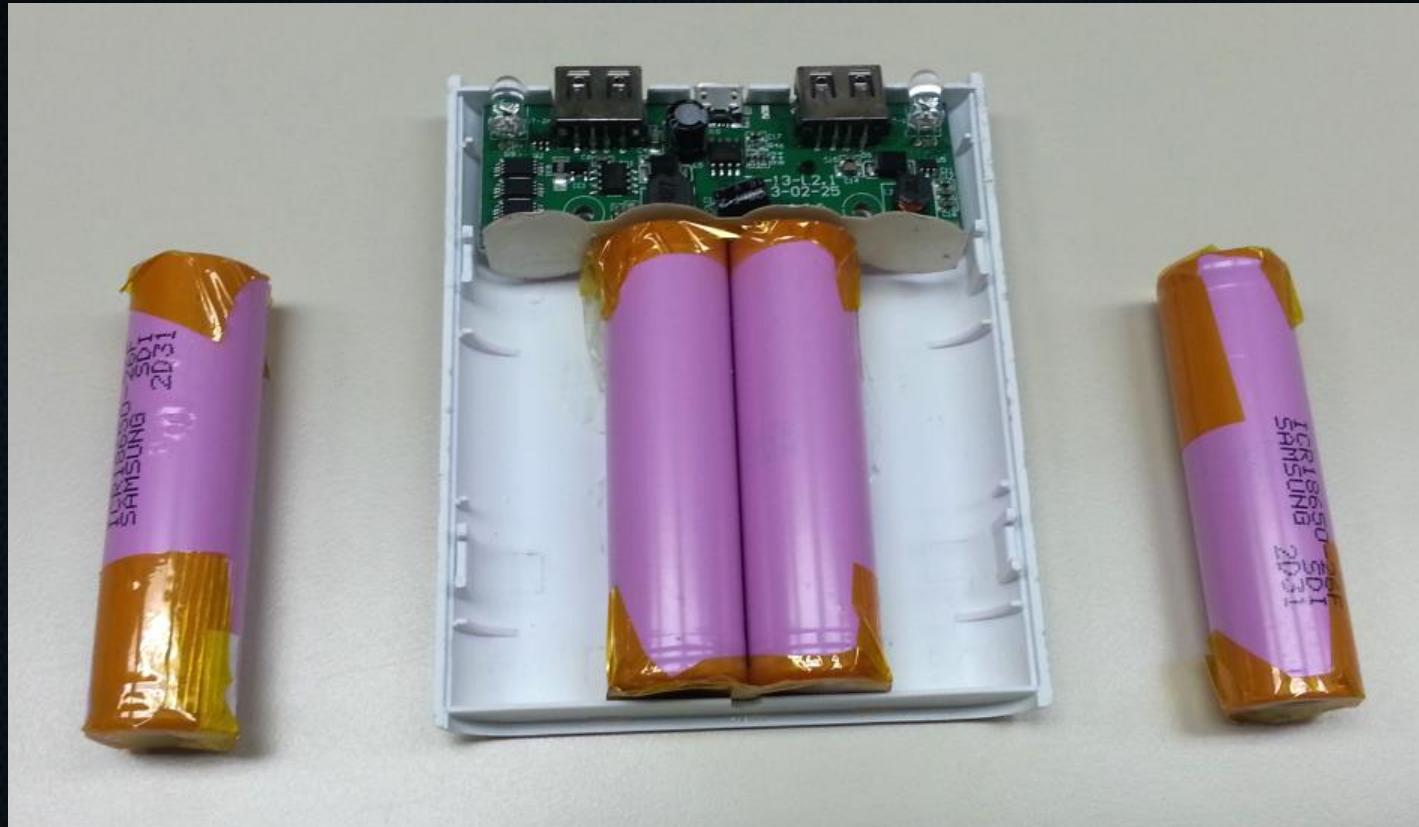


Inside of the portable charger

- It has a very simple architecture
 - A charger module and battery cells
 - High capacity model → More battery cells!



Cutting off battery cells

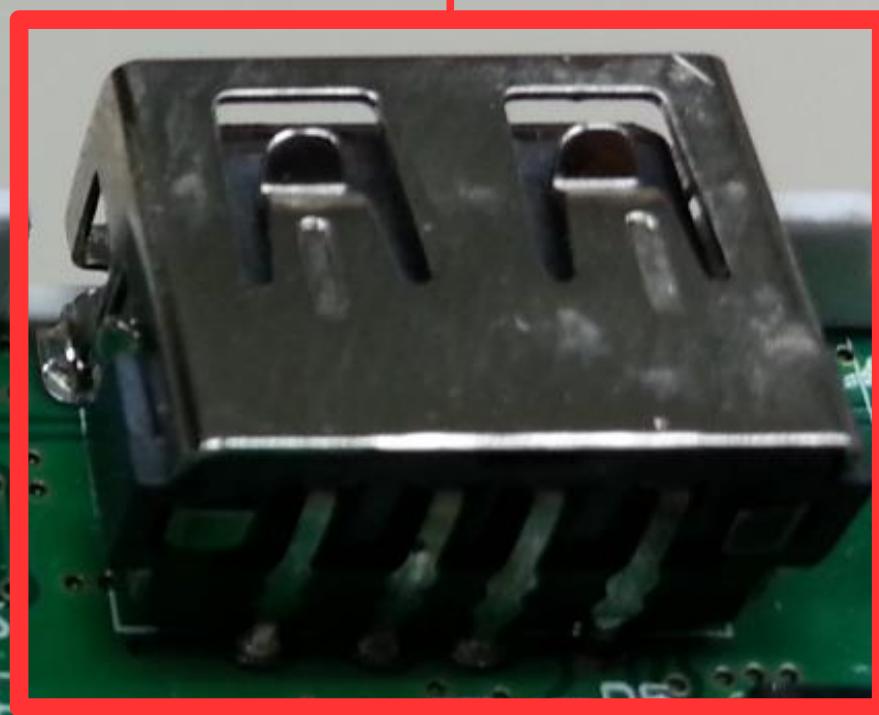
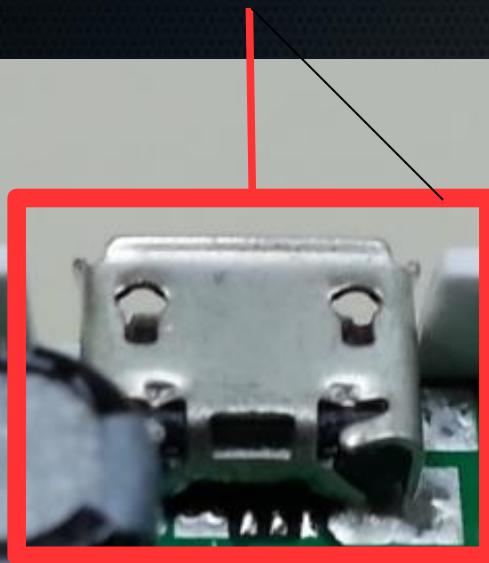


- Make some space for IRON-HIDs
 - Battery cells are connected in parallel
 - Cut off the cell connector carefully

Pin layouts of the charger module

USB Connector
for Input (recharging)

USB Connector
for Output (smartphone)

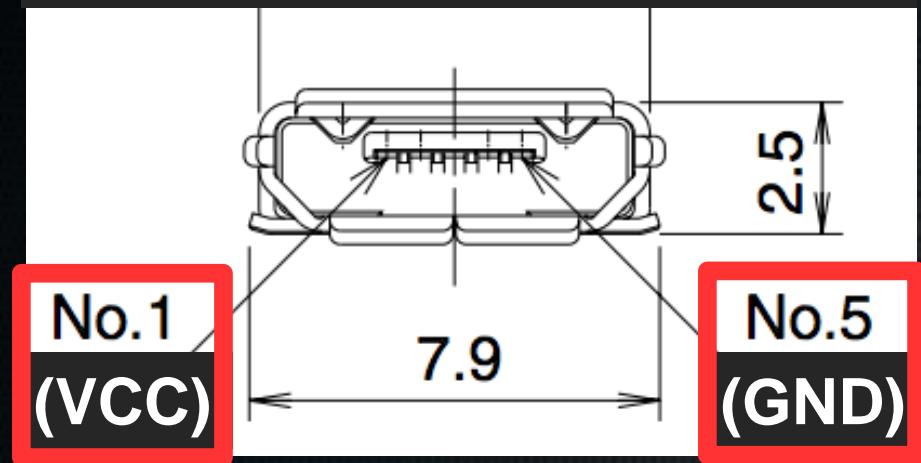


GND	ID	Data-	VCC	(No.5)
		+	(No.1)	

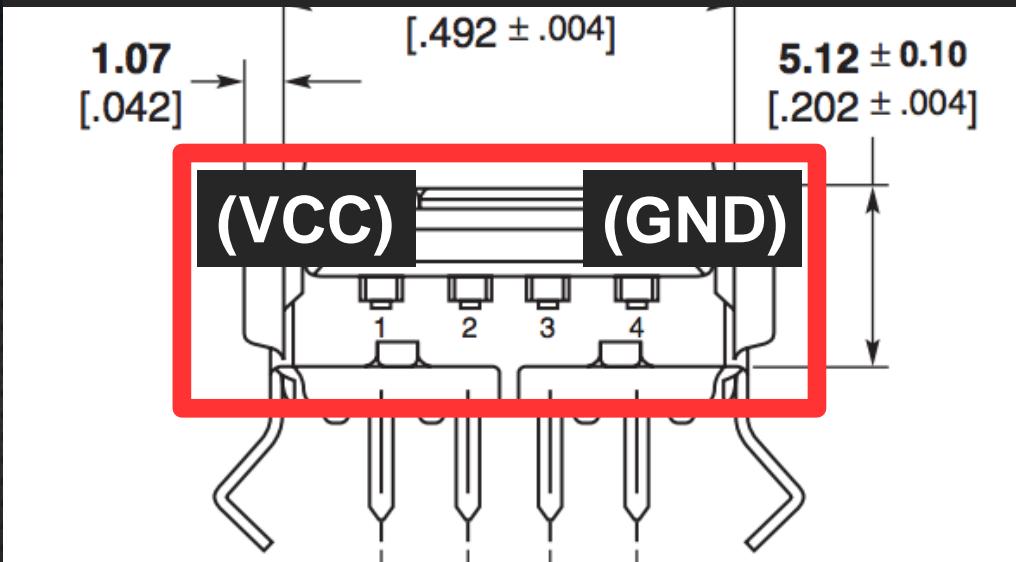
GND	Data-	VCC	(No.4)
	+	(No.1)	

USB Datasheet

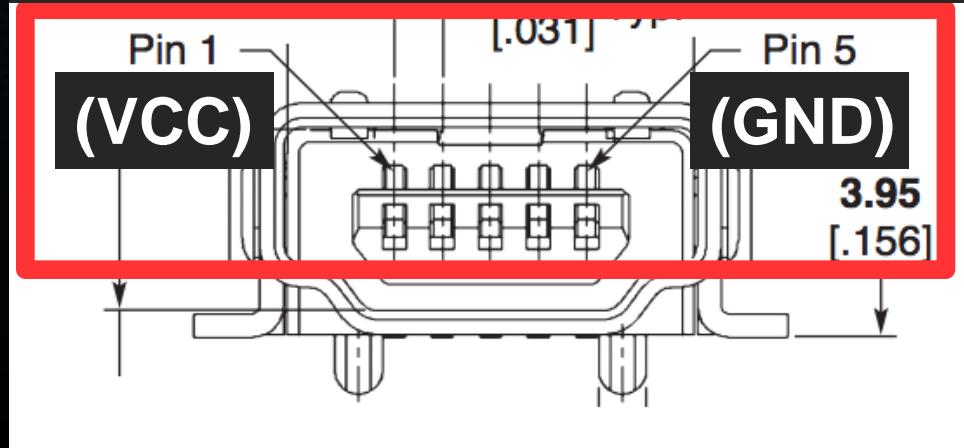
Micro Type



A Type

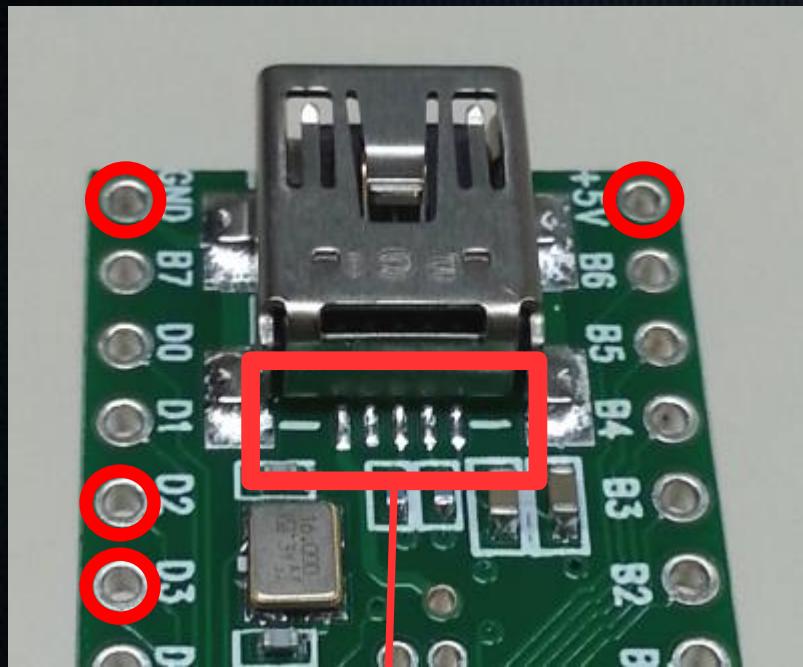


Mini Type



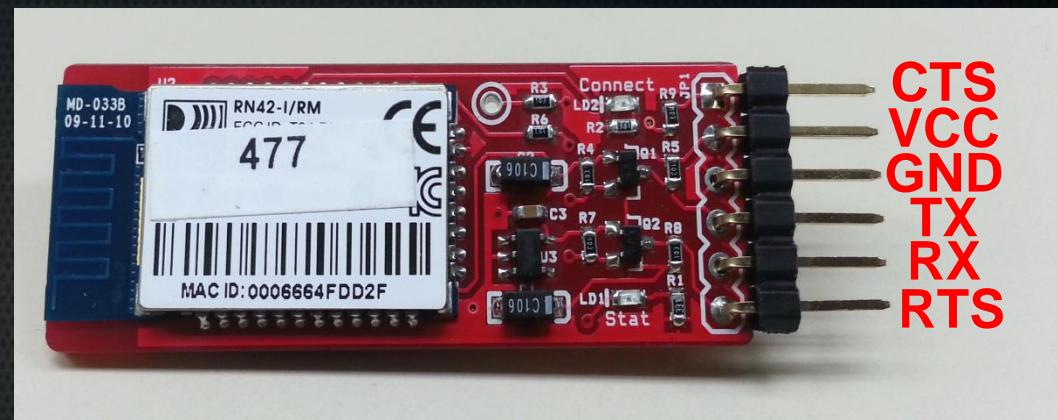
Pin layouts of the IRON-HID

Teensy



GND
ID
Data-
VCC
Data+

Bluetooth Serial Module
(RN-42 Silver)



CTS
VCC
GND
TX
RX
RTS

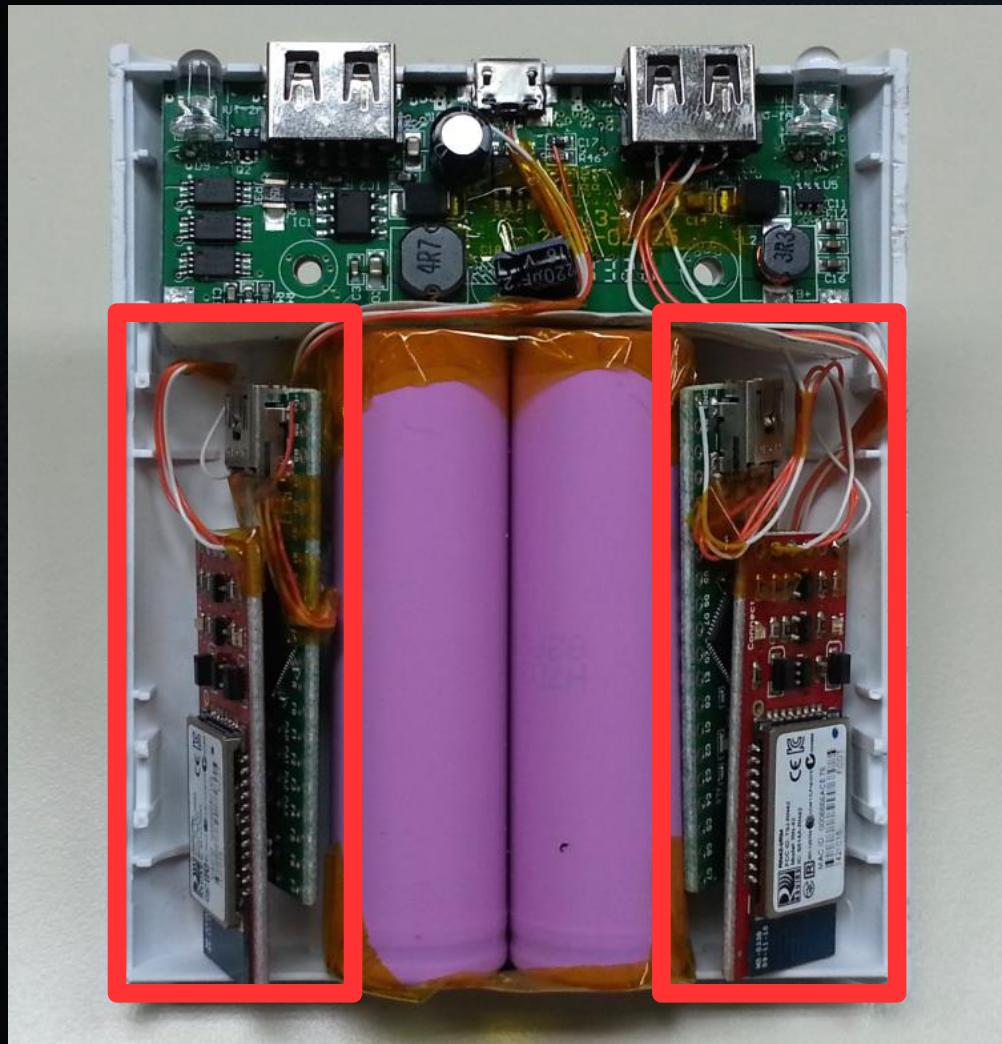
Teensy

5V OUT
D2 (RX)
D3 (TX)
GND

Bluetooth

VCC
TX
RX
GND

You got the power!!



* Rebirth of the Portable Charger *

USB OTG (On-The-Go)



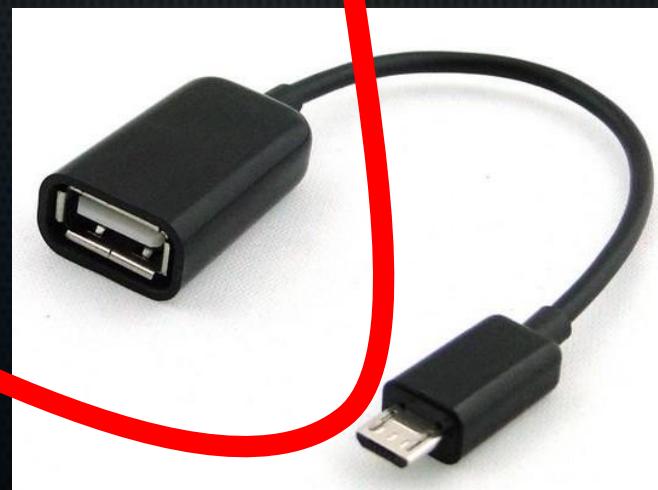
- It activates the **USB host function of smart-phones**
 - You can connect various types of USB peripherals such as a keyboard, a mass-storage (USB drive), a mouse
- * The final piece of the puzzle ***

Smartphone



... ?! ...

Cables



PowerShock

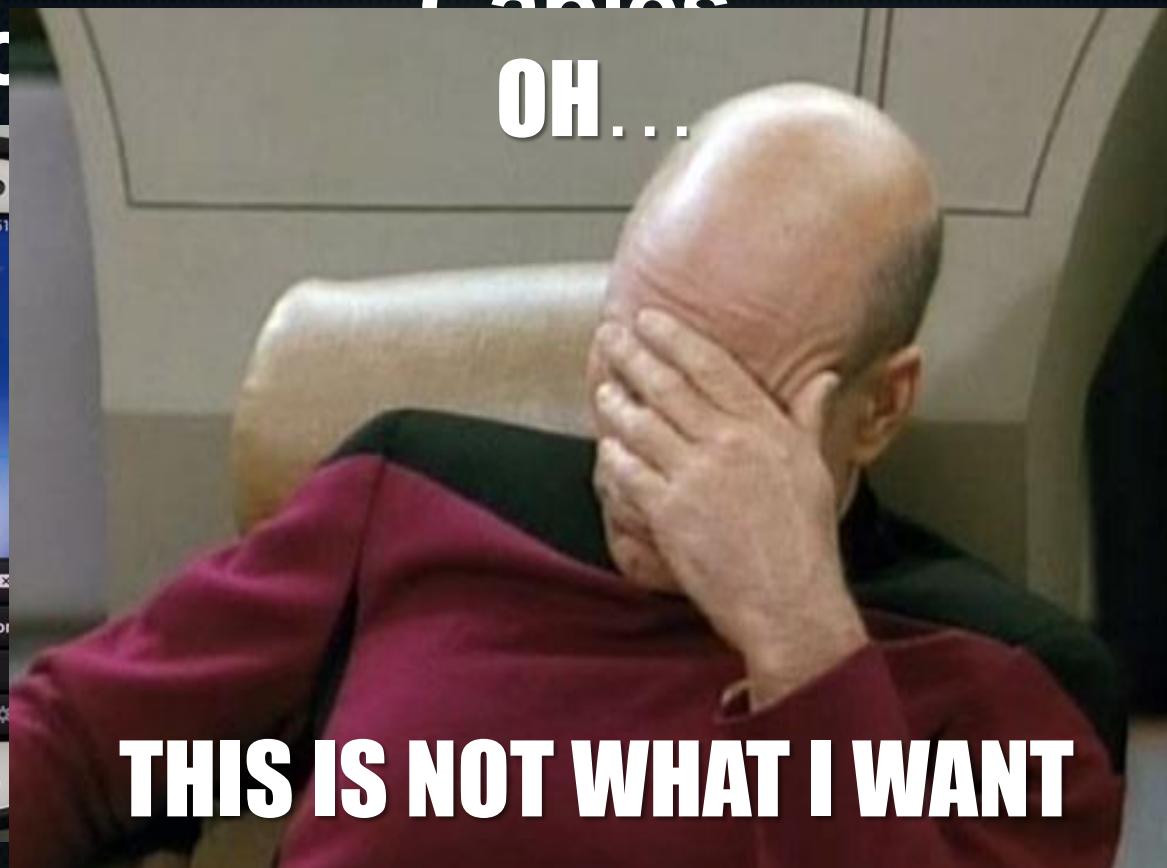


Smartpho



... ?! ...
Cables
OH...

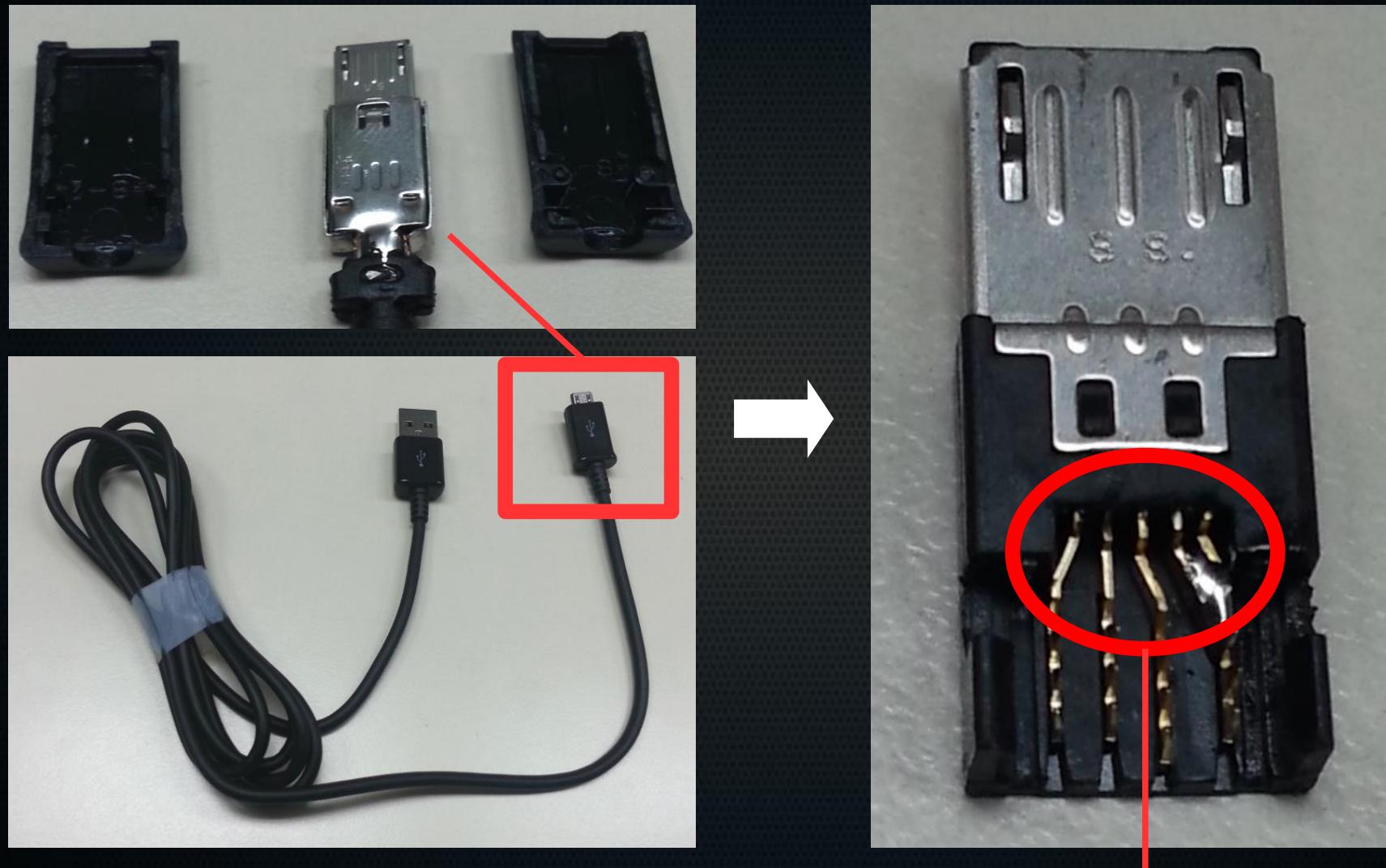
verShock



THIS IS NOT WHAT I WANT



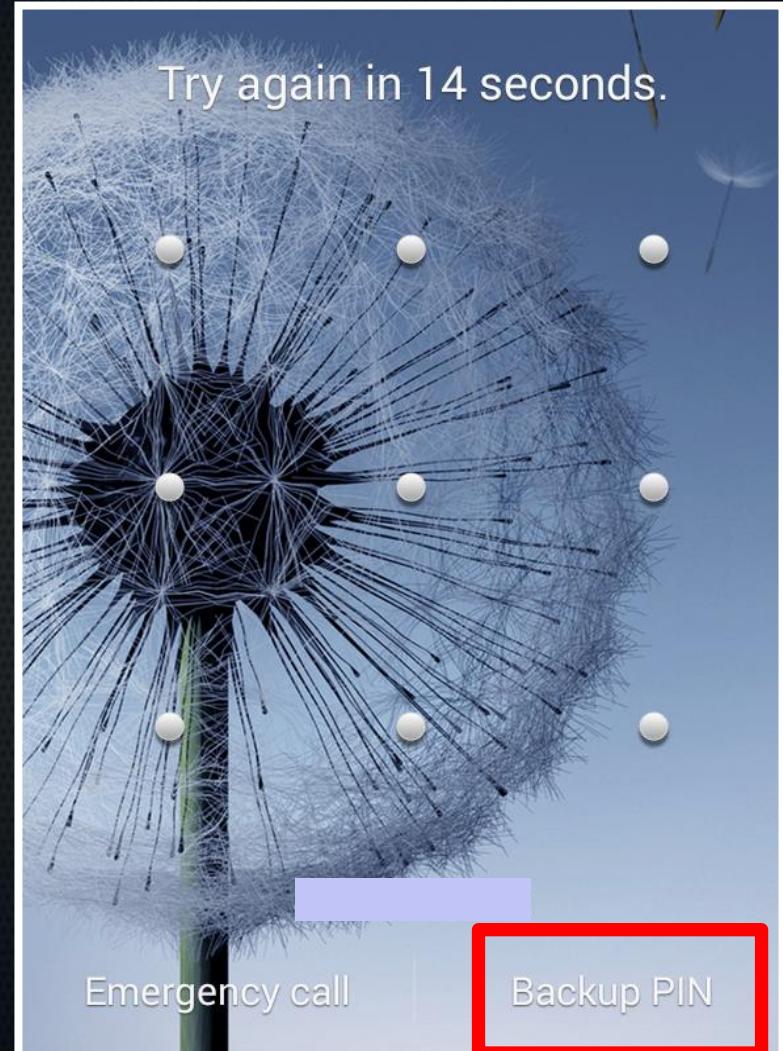
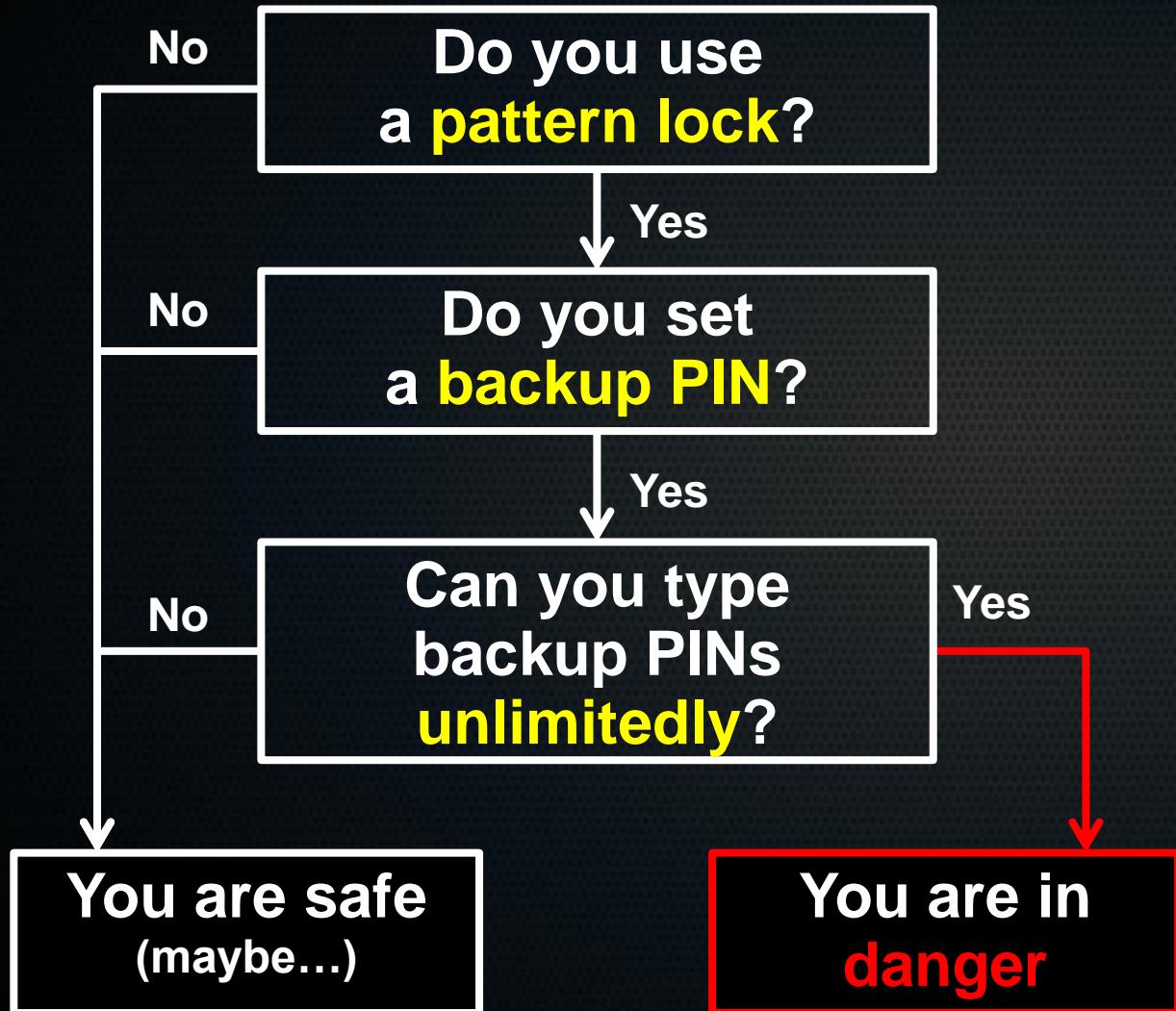
Making a custom OTG cable



Connect the ID pin with the GND pin

- Background and Architecture of IRON-HID
- Hacking a Portable Charger
- Testing a Vulnerability of the Smartphone
- Testing a Vulnerability of the POS System and the PC
- Bonus

Well-known Smartphone Vulnerability



Testing the vulnerability

- Connect **PowerShock** to a smartphone with the custom **OTG cable** and fire!!
 - It is really hard to test the vulnerability with your hands
 - The PowerShock tests it instead of you
 - It sends PINs quickly and automatically!!

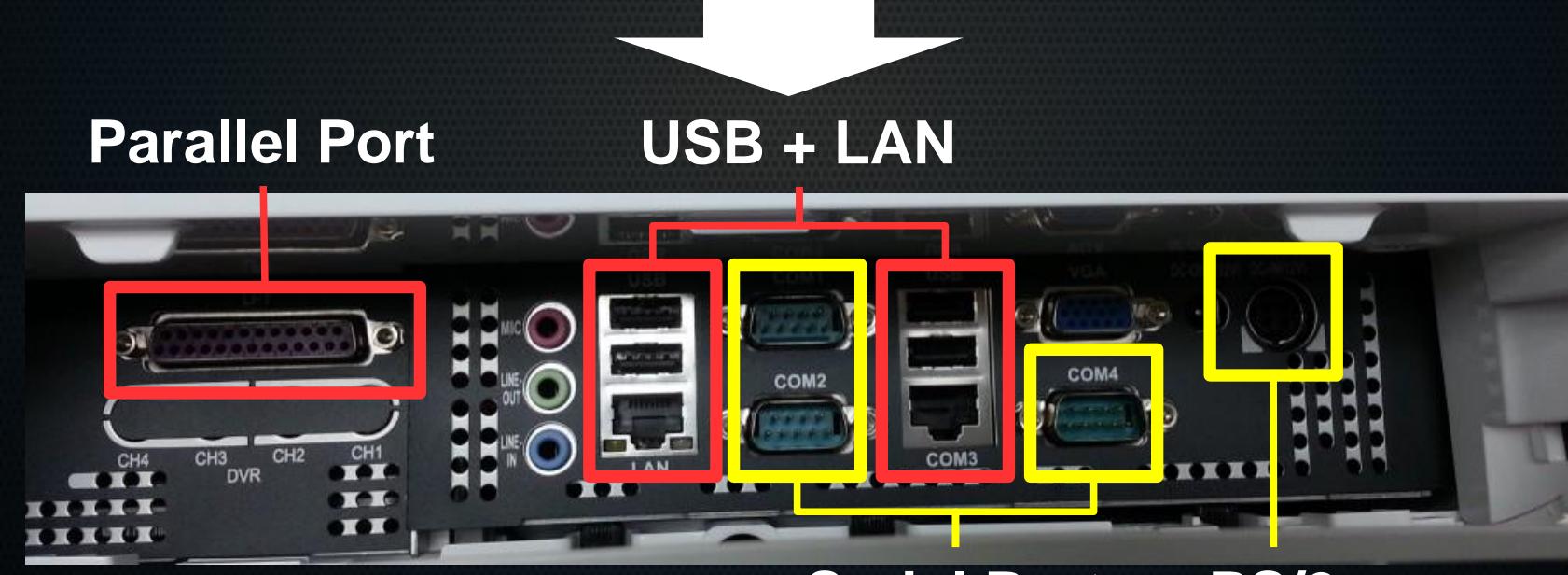
If someone asks you to charge a phone,
charge it with **PowerShock!!**

Demo (Let's test the Android)



- Background and Architecture of IRON-HID
- Hacking a Portable Charger
- Testing a Vulnerability of the Smartphone
- Testing a Vulnerability of the POS System and the PC
- Bonus

Inside of the POS Systems



Many POS systems are PC-based!!

If the PowerShock plugs into the POS?

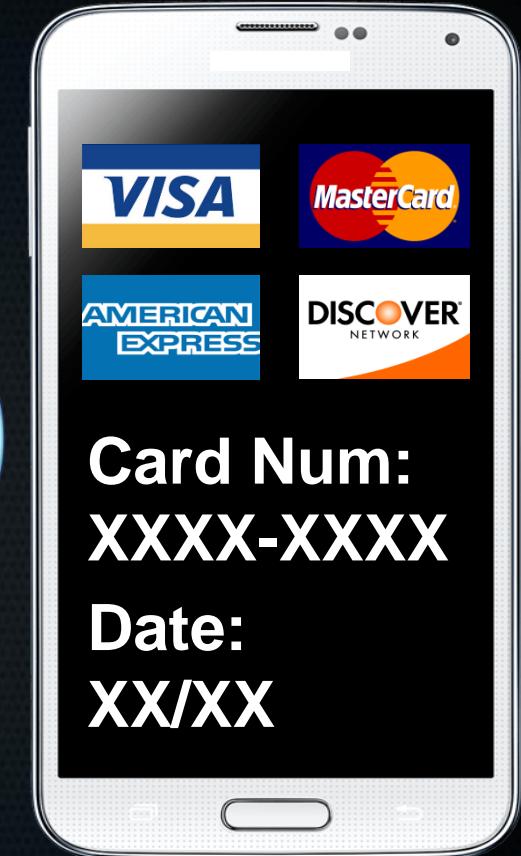


POS System

USB
↔
Recharge



PowerShock



If POS system has a vulnerability,
you can grab **card numbers!!**

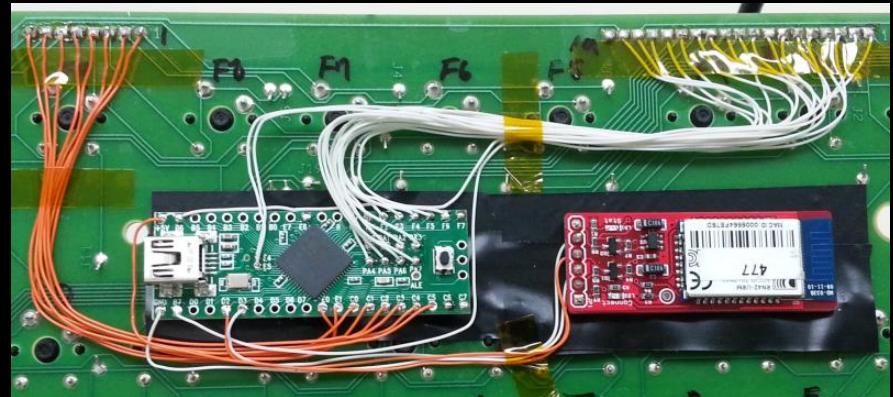
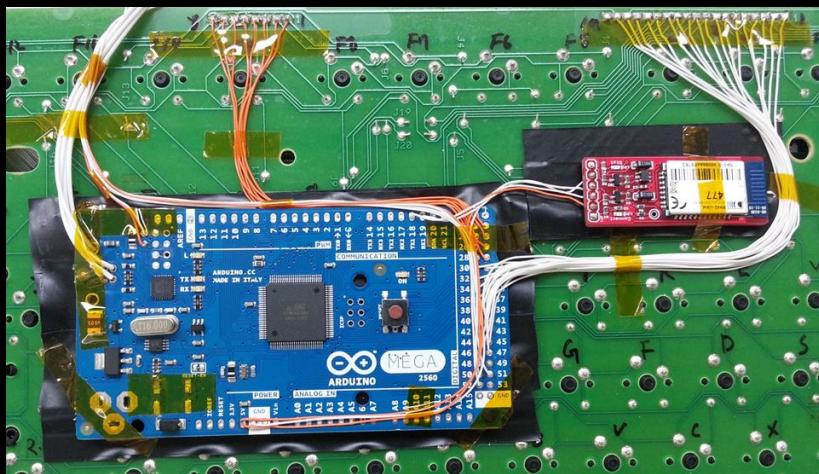
Demo (Let's test the POS system)

CONTROL	COMMAND	KEY
» Start to mount CD-ROM « Microsoft Windows [Version b.3.9b00] (c) 2013 Microsoft Corporation. All rights reserved.		
E:\>c:		
C:\>cd windows		
C:\Windows>dir Volume in drive C has no label. Volume Serial Number is 72E6-1928		
Directory of C:\Windows		
09/14/2014 04:05 PM	<DIR>	
09/14/2014 04:05 PM	<DIR>	
07/23/2013 08:36 AM	<DIR>	Windows
08/22/2013 08:35 AM	<DIR>	ADFS
08/22/2013 08:36 AM	<DIR>	AppCompat
03/18/2014 03:17 AM	<DIR>	apppatch
09/14/2014 04:05 PM	<DIR>	AppReadiness
03/18/2014 03:20 AM	<DIR>	assembly
08/22/2013 04:21 AM		56,832 bfsvc.exe
08/22/2013 08:36 AM	<DIR>	Boot
08/22/2013 08:36 AM	<DIR>	Branding
03/18/2014 03:17 AM	<DIR>	Camera
03/18/2014 03:17 AM	<DIR>	CbsTemp
09/14/2014 04:05 PM	<DIR>	CSC
08/22/2013 08:36 AM	<DIR>	Cursors
09/14/2014 04:04 PM	<DIR>	debug
08/22/2013 08:36 AM	<DIR>	
DesktopTileResources		
Input commands		

CONTROL	COMMAND	KEY
dir Volume in drive C has no label. Volume Serial Number is 72E6-1928		
Directory of C:\		
11/08/2012 12:46 AM	<DIR>	
0c259d27674feb48b7e225de10	<DIR>	Data
05/07/2014 07:09 PM	<DIR>	Desktop
08/17/2013 11:07 PM	<DIR>	Intel
09/14/2014 04:12 PM	<DIR>	17,792 password.txt
09/13/2014 07:42 AM	<DIR>	PerfLogs
08/22/2013 08:22 AM	<DIR>	Program Files
09/14/2014 04:12 PM	<DIR>	Program Files (x86)
07/23/2013 08:36 AM	<DIR>	17,792 password.txt
09/14/2014 04:12 PM	<DIR>	Jscts
08/27/2013 10:52 PM	<DIR>	UTIL
06/10/2014 07:24 PM	<DIR>	VirtualMachine
09/14/2014 04:05 PM	<DIR>	Windows
09/14/2014 04:57 PM	<DIR>	Windows.old
	2 File(s)	17,860 bytes
	12 Dir(s)	25,171,771,392 bytes free
C:\>>> Start to receive password.txt files <<		
b4/17792		
3904/17792		
8128/17792		
121b0/17792		
1b320/17792		
>> Receive file complete <<		
Input commands		

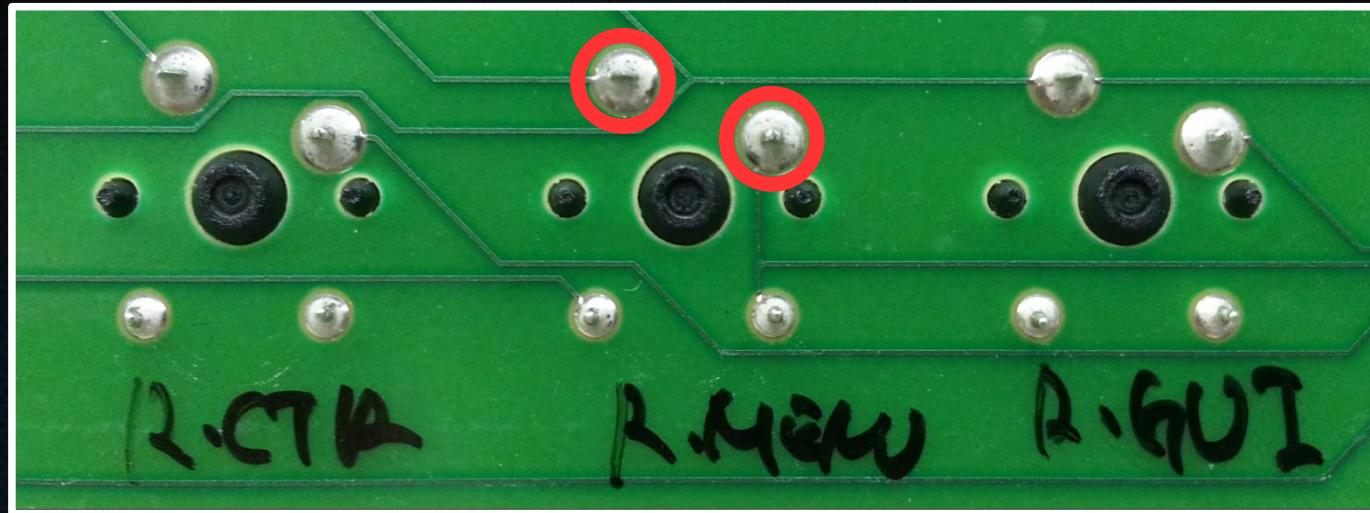
- Background and Architecture of IRON-HID
- Hacking a Portable Charger
- Testing a Vulnerability of the Smartphone
- Testing a Vulnerability of the POS System and the PC
- Bonus

KeyboardShock



Attach IRON-HID onto USB keyboards
and give them to your **colleagues**

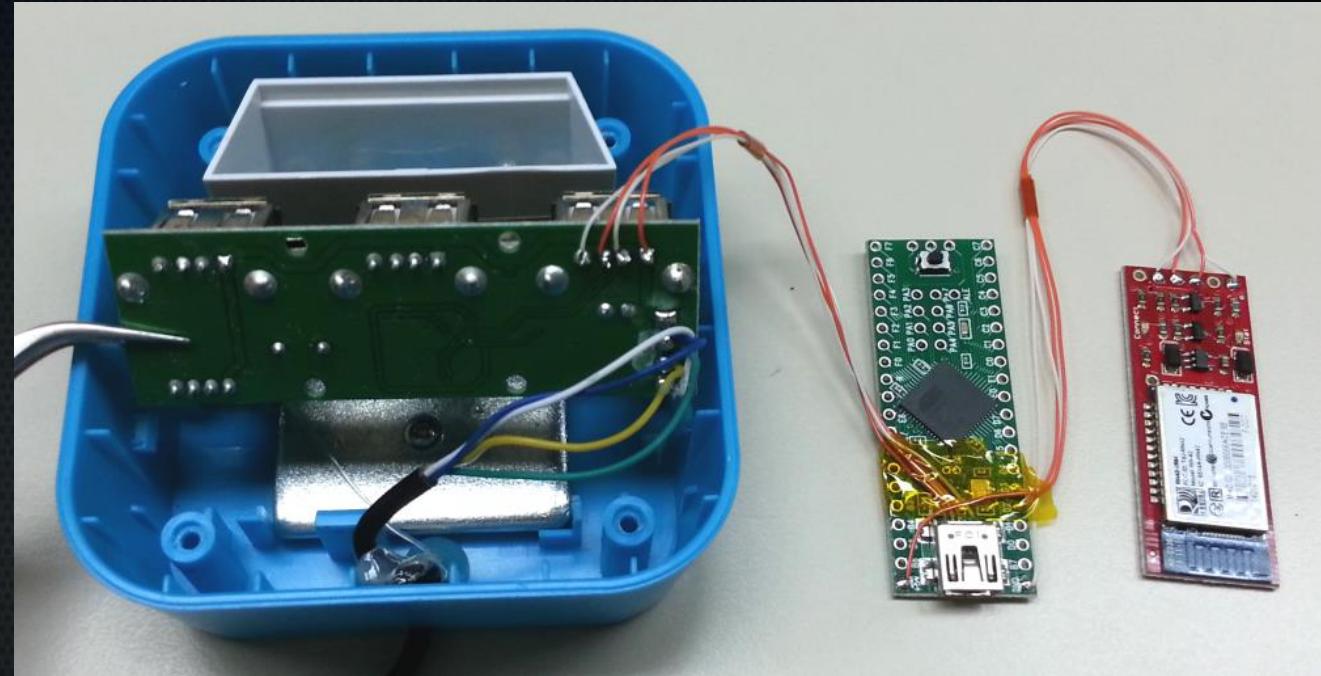
Find the key matrix with multimeter



	Columns						
	0	1	2	3	4	5	
Rows	0		LGUI		ESC		
	1	RCONTROL		RSHIFT	Z	X	
	2				1	2	
	3	LCONTROL		LSHIFT	TILDE	F1	
	4				Q	W	
	5			LSHIFT	TAB	CAPSLOCK	
	6				A	S	
	7	RGUI					
	6	7	8	9	10	11	
Rows	1	F4	G	H	F6	F5	QUOTATION
	2	C	V	M	COMMA	PERIOD	
	3	3	4	7	8	9	0
	4	F2	5	6	EQUAL	F8	MINUS
	5	E	R	U	I	O	P
	6	F3	T	Y	CLOSEBRAKET	F7	OPENBRAKET
	7	D	F	J	K	L	SEMICOLON
	8		B	N			SLASH
	12	13	14	15	16	17	
Rows	1	F5		PAD_0	PAD_PERIOD	UP	LALT
	2	ENTER	NUMLOCK	PAD_SLASH	PAD_ASTERISK	PAUSE	
	3	F10	F11	F12	PAGEDOWN	END	PRINTSCREEN
	4	F9	DELETE	INSERT	PAGEUP	HOME	
	5		PAD_7	PAD_8	PAD_9	PAD_PLUS	SCROLLOCK
	6	BACKSPACE	PAD_4	PAD_5	PAD_6	APPLICATION	
	7	INVERSESLASH	PAD_1	PAD_2	PAD_3	PAD_ENTER	
	8	SPACE	DOWN	RIGHT	PAD_MINUS	LEFT	RALT

The example of the keyboard matrix

ReaderShock



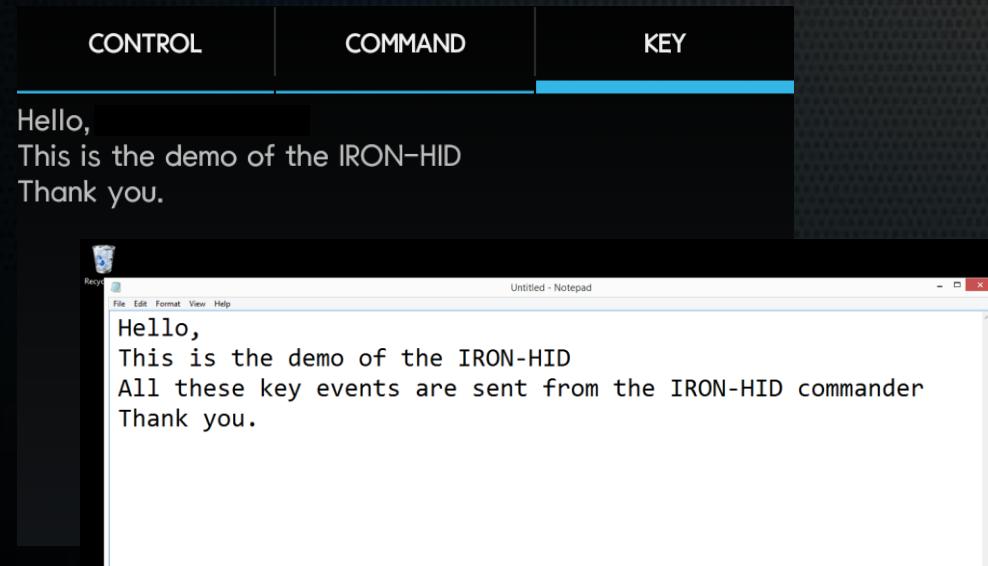
Attach IRON-HID onto card readers
and give them **also** to your **colleagues**

Then...

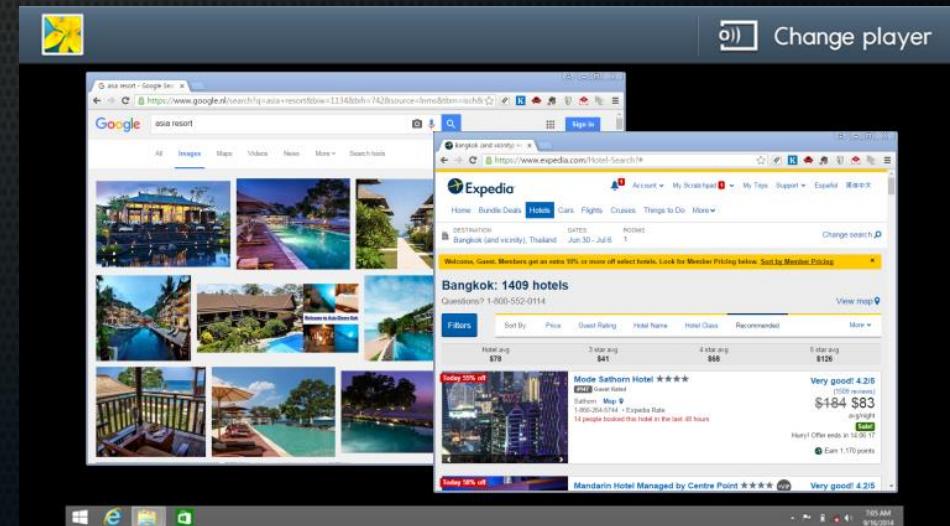
You will be the big brother for fun!!



Executing commands



Logging and sending keys

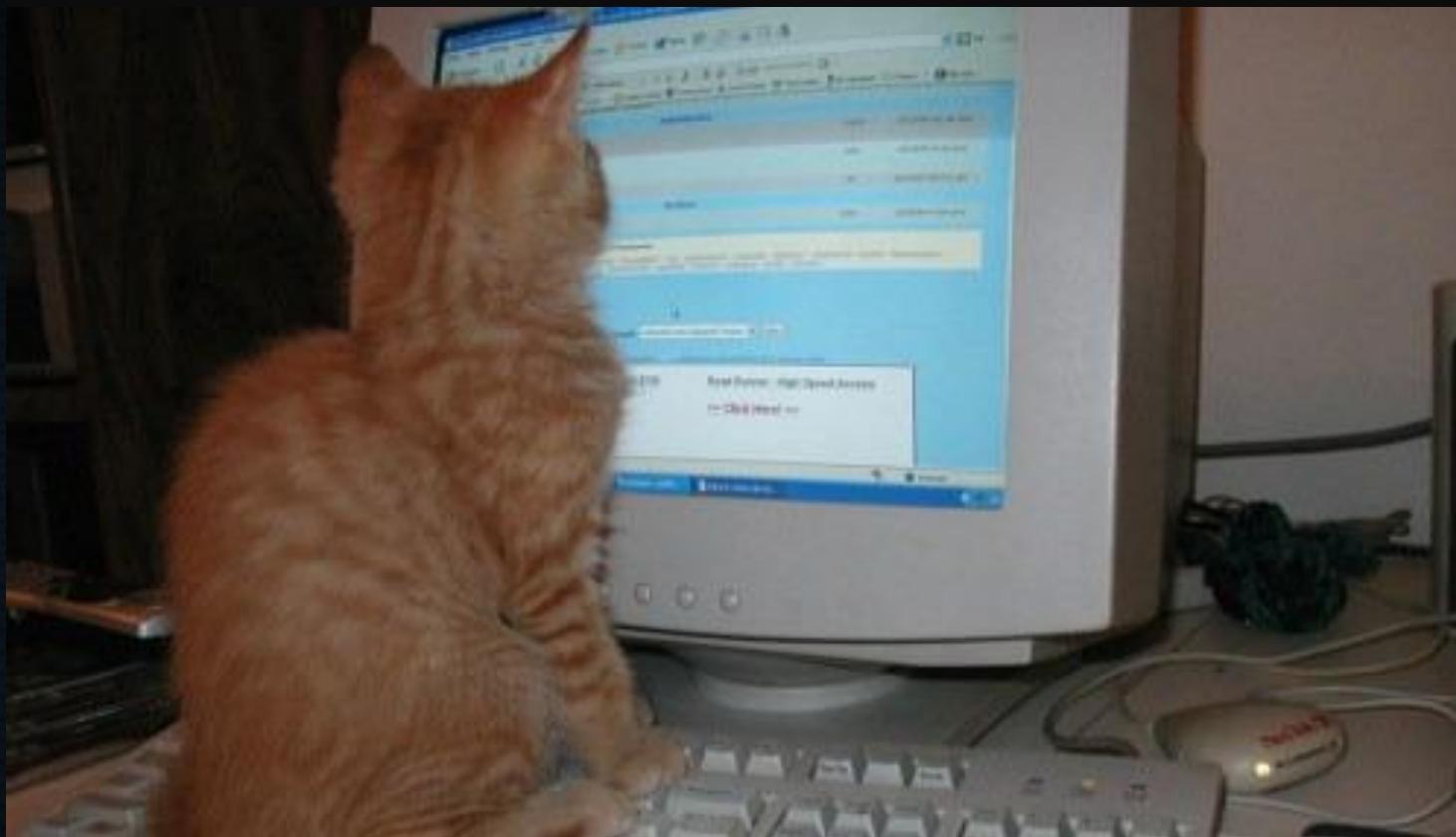


Receiving files and capturing screenshots

Resources

- <http://www.fourwalledcubicle.com>
- <http://cdemu.blogspot.com>
- <http://www.usb.org>
- <https://www.arduino.cc>
- <https://www.pjrc.com/teensy>

Thank you !



**I will be waiting for your email
[@kkamagui1,hanseunghun@nsr.re.kr](mailto:kkamagui1,hanseunghun@nsr.re.kr)**