

Hardware - Hunny

Captions & Subtitles

Position

☐ Bottom (Overlaid)

☐ Top (Overlaid)

☒ Below Slide

☐ Above Slide

Language

Spoken Language:

Subtitle Language:

Microphone

For best results, use a headset microphone.

Microphone: Microphone (High Definition Audio Device)

Appearance

Change other subtitle display preferences including font size, style, color, background color, and transparency:

[More Settings \(Windows\)...](#)

OK Cancel

Malagasy
Malay
Malayalam [Preview]
Maltese
Māori
Norwegian (Bokmål)
Persian
Polish
Portuguese
Portuguese (Portugal) [Preview]
Punjabi [Preview]
Querétaro Otomi
Romanian
Russian
Samoan
Serbian (Cyrillic)
Serbian (Latin)
Slovak
Slovenian
Spanish
Swedish
Tahitian
Tamil
Telugu
Thai
Tongan
Turkish
French

101

Hardware Hacking 101

- Hunny



Hello!

I'm Hunny

- Volunteer/Member of Hack Miami & Defcons Hardware Hacking Village
- You can find me at @Hunny1506 in the %27discord

Disclosures and Liability Statement

Harmful Substances

In the process of Hardware Hacking it is **PROBABLE** you will encounter substances known to cause cancer in California...

- Lead/Heavy Metals
- Noxious/Harmful/Toxic Fumes
- High temperatures

Legal/Liability Statement

You are responsible for your own safety, and compliance with local, state, federal, and/or national laws.

Also... you **WILL** void the warrantee and violate the terms of use/service







Recommended Safety Equipment and Conditions

- Well ventilated space to assemble and disassemble
- Respirator/Mask
- Eye Protection
- Heat resistant gloves/tools/clothes/surface
 - Natural (non-meltie) fibers
- Heat tolerant work surface

Recommended Safety Equipment and Conditions

- Well ventilated space to assemble and disassemble
- Respirator/Mask
- Eye Protection
- Heat resistant gloves/tools/clothes/surface
 - Natural (non-meltie) fibers
- Heat tolerant work surface



**Alteration of an
electronic device or
machine that makes it
do something outside its
original function.**

But also...

Fixing

Repurposing

**Making
your own
use**

Tools Recommended

iFixIt Kit

Is considered the go to disassembly kit

Chip/board/component/sensor interface

The tool that lets you interact with chips and/or components

Logic

Analyzer/Occilloscope

Records signals that can be translated

Soldering set up

Solder, Iron, mat, rosin, desolder, helping hands, clamps, tweezers

Computer with HH tools

HHV Plug- Kali with the cool tools available here

Google.... Github....

Redit... some raspberry pi and arduino can't hurt either

Common protocols

**Inter-Integrated
Circuit (I2C)**

**Universal
Asynchronous
Receiver/Transmitter
(UART)**

**Serial Peripheral
Interface (SPI)**

**Jtag-
Not a protocol.**

Multi protocol, variable voltage tools

Tigard



Bus Pirate

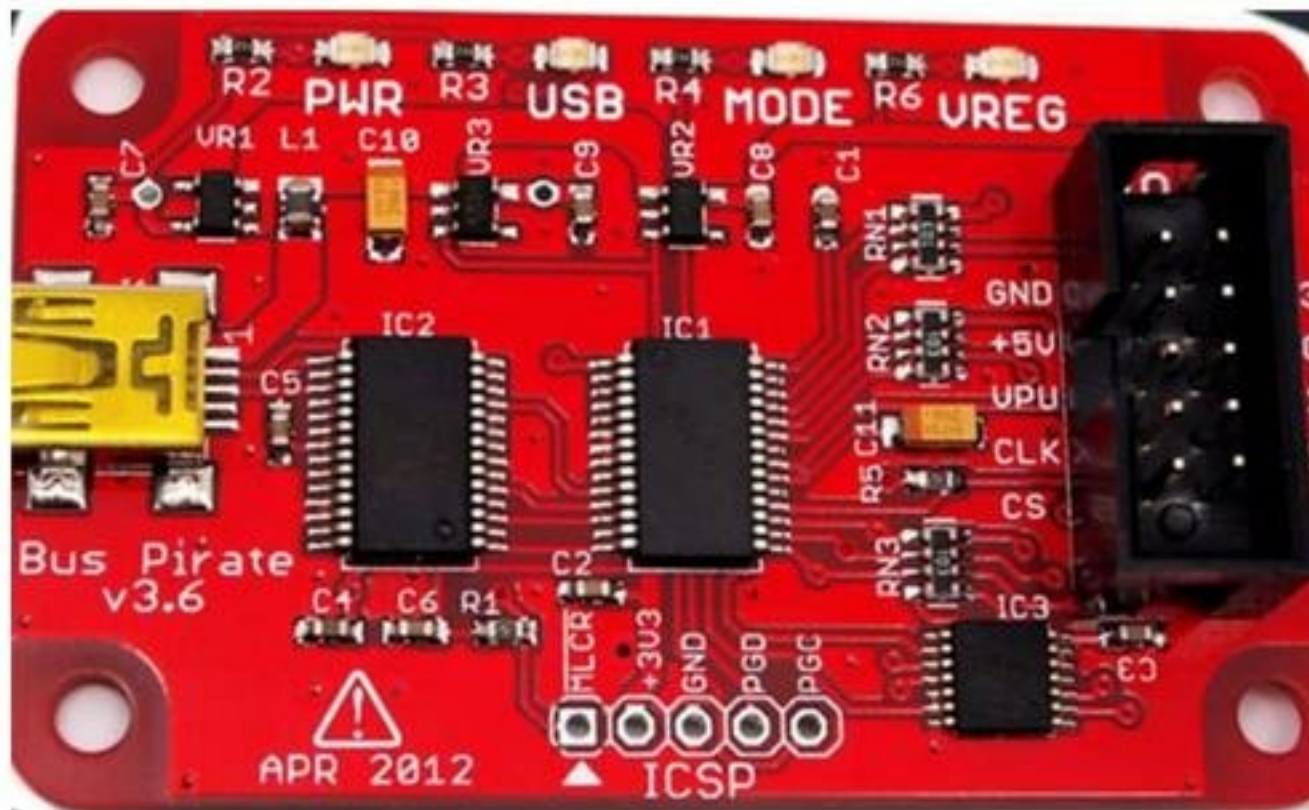


Adafruit FT232H



, variable voltage tools

Bus Pirate



Adafruit FT232



Multi protocol, variable voltage tools

Tigard



Bus Pirate



Adafruit FT232RL



Software

Flashrom

OpenOCD

RBaseFind

Other Flash
programmers

Circuit simulators

Hardware Hacking
Village Defcon has
two images.. A
heavy and a light.
Comes with
everything

3. Some examples of hardware hacks



3. Some examples of hardware hacks

Wi-Fi Pineapple



Rubber Ducky



Gas pump skimmers



Favorite old school
router...
WRT54G



Favorite old school
router...
WRT54G



```
GitTerm - /dev/ttyACM0 9600-8-N-1
File Edit Log Configuration Controlsignals View Help
Welcome to DEF CON 29!
Note: This badge is running very limited firmware. The full firmware
will be available when DEF CON starts.

Choose an option:
[1]: Change LED Colors
[2]: Change Keymap
[3]: Reset EEPROM
Enter Number:2
Which Key would you like to change?

  1  2
  3  4

Enter Number:2
Enter new keystroke for key 2
You may enter a single character or string of characters.
Modifiers go before the character they affect
Available modifiers: [ctrl][alt][shift][gui]
Media keys: [play][next][back][stop][eject][mute][vol+][vol-]
New keystroke:
```



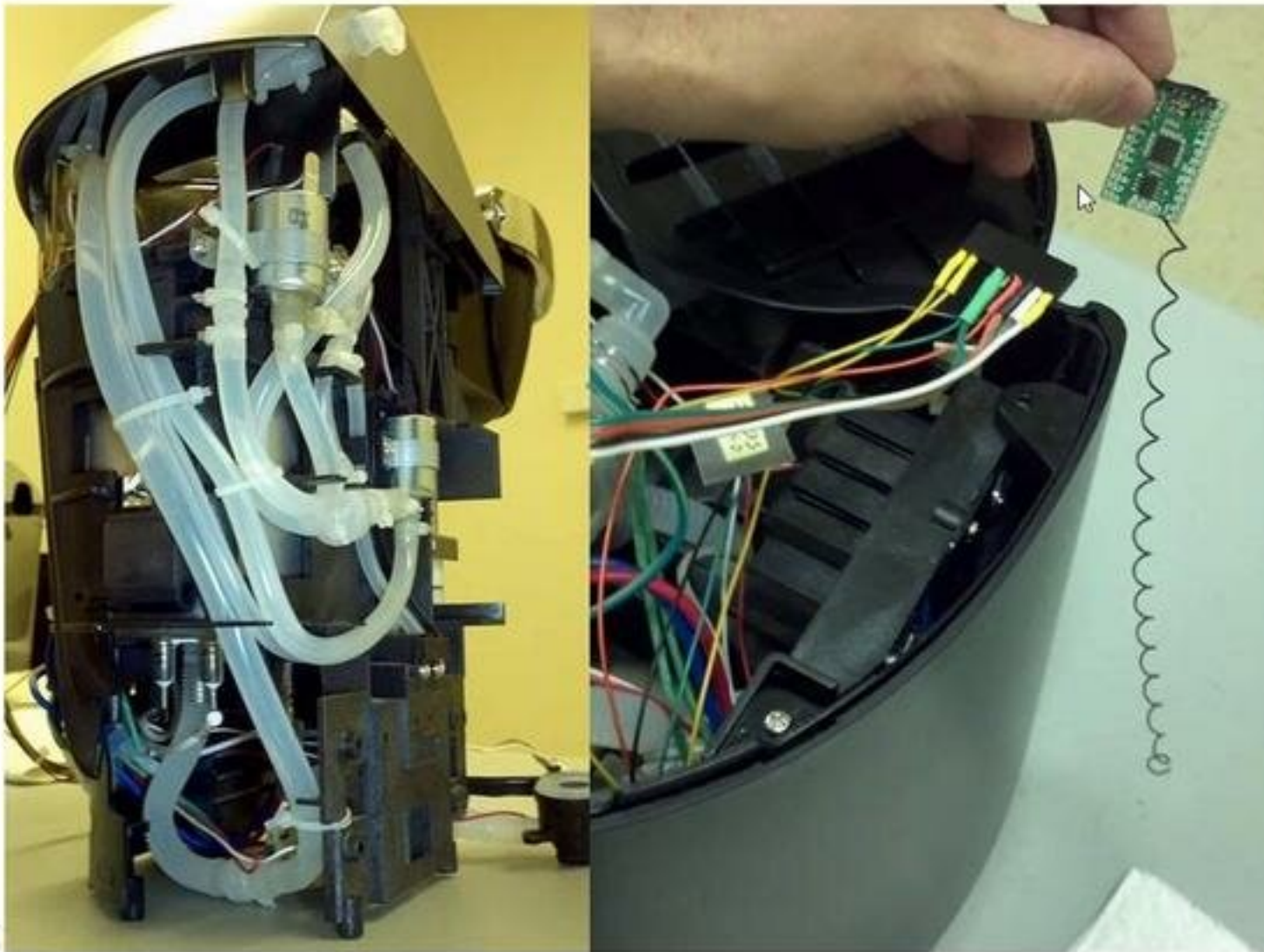
Badges and blinkies

characters.
[mute] [vol+] [vol-]

DTR RTS CTS CD DSR RI



Making your Keurig wireless



Make your own messages...





Credits

Special thanks to all the people who made and released these awesome resources for free:

- Bunny from DCHHV
- Presentation template by [SlidesCarnival](#)

Articles that helped me

- <https://www.riverloopsecurity.com/blog/2020/02/hw-101-spi/>
- <https://www.circuitbasics.com/basics-of-the-spi-communication-protocol>
- https://site.ieee.org/ocs-cssig/?page_id=770

End of slide show, click to exit.



Bajando por esa extraña madriguera de conejo de hackeo de hardware conmigo.
Gracias por su presentación. Cualquier pregunta esta vez.