USB Attack Workshop

Soldering Skills & Basic Keystroke Injection Attacks

[HakCat @ Crash Space]
Alex Lynd & Angelina Tsuboi 03/19/2023

What we're doing today

- 🖥️ Learning about USB attacks: methods & tools
- 🐱 Soldering your own USB Nugget
- ⌨️ Writing keystroke injection scripts!

Alex Lynd

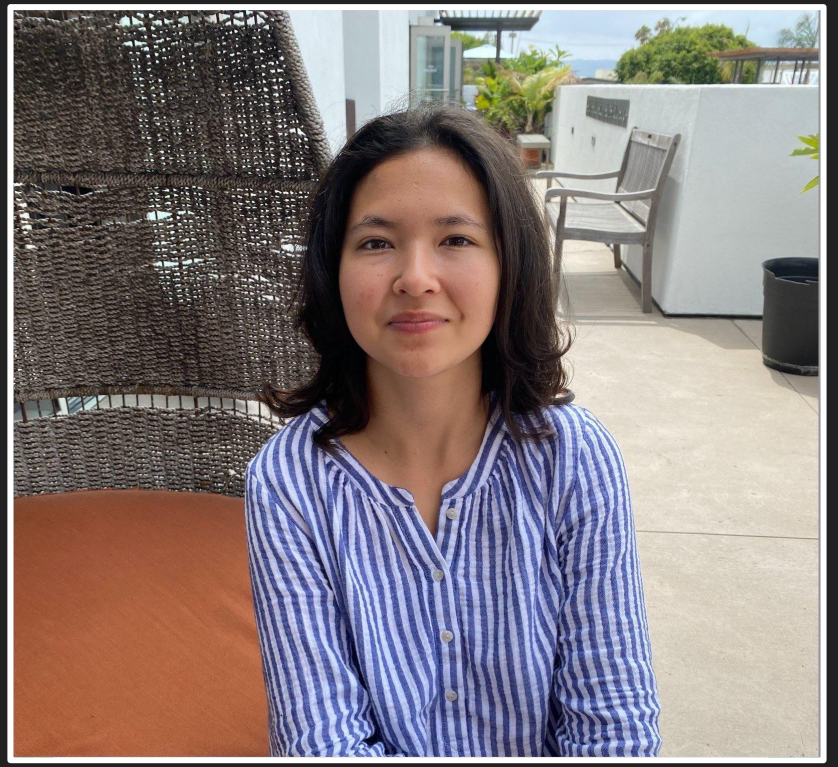
- Hardware Hacker - IOT & Wireless Security
- Content Creator - Hacking Tutorials @ Hak5
- Instructor - I teach & host workshops and stuff

alexlynd.com • lyndlabs.io

Angelina Tsuboi

Hi! I’m a software developer and tinkerer interested in hardware, cybersecurity, and mechatronics.

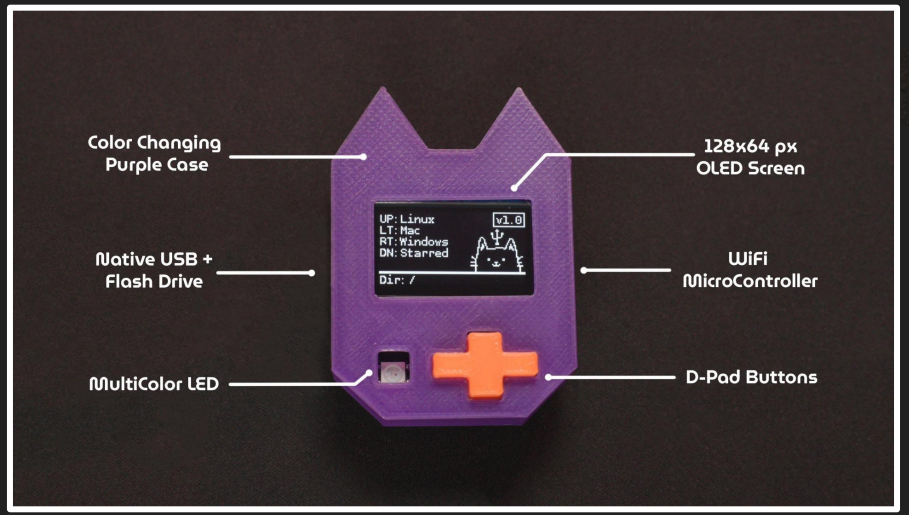
angelinatsuboi.net / @AngelinaTsuboi



What is the Nugget?

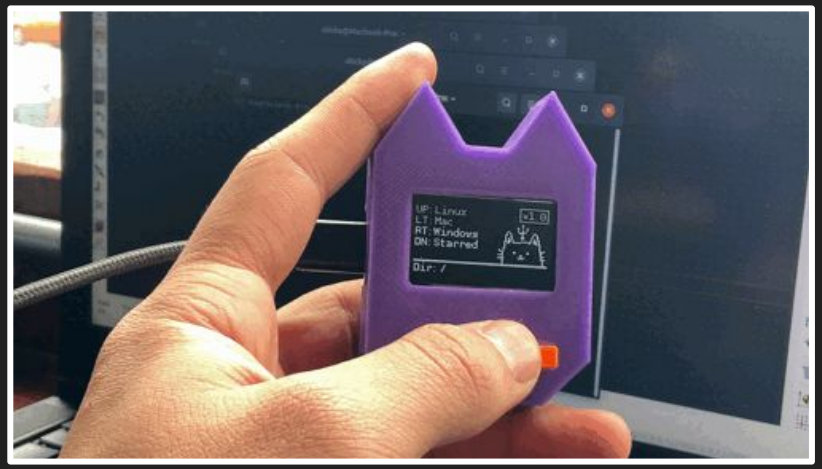
The Nugget is a cat-themed console that makes it fun to learn hacking!

- Hardware Prototypes
- CircuitPython
- WiFi Hacking
- USB Hacking



What is the USB Nugget?

- **Run USB Attacks**
- **Emulate Keyboards & More**



Features:

- DuckyScript
- LED & Screen Feedback
- Flash Drive
- WiFi Interface

What's under the hood?

The USB Nugget is powered by the **ESP32-S2** microcontroller which offers:

- **WiFi** (AP & Client mode)
- **Native USB**
  - Emulate USB Devices
  - Flash Storage
- **Easy Hardware Expansion**

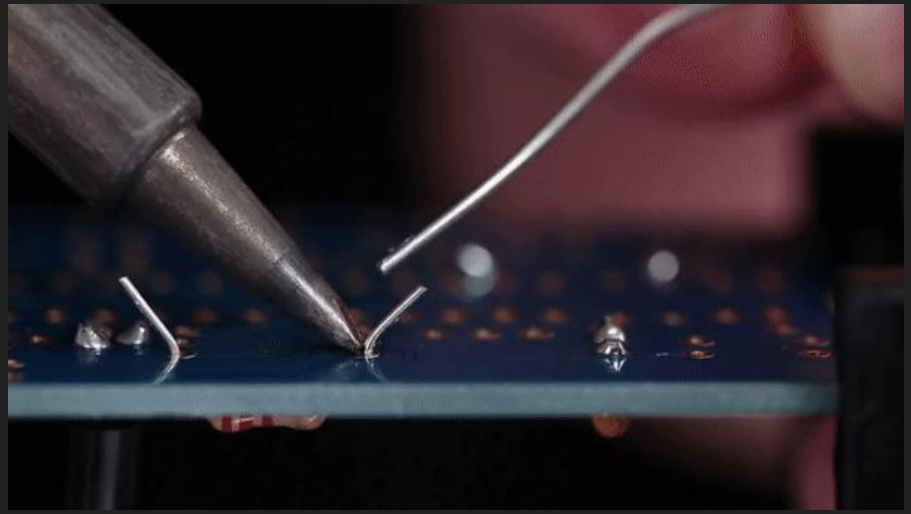
Soldering Skills Class

Build your own USB Nugget!

What is Soldering?

Soldering is an assembly technique that lets us mount components on circuit boards.

- **Solder** is used to attach components to the PCB.
- A **soldering iron** is used to heat up the circuit board *and* the components at the same time.
- Solder hardens and lets us create a stable electrical connection.



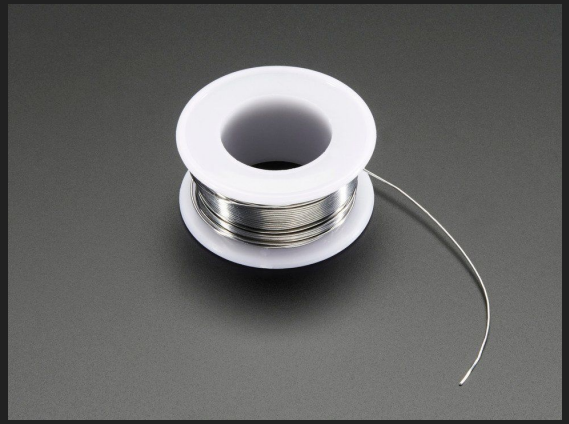
Soldering through hole components

Common Soldering Tools

Soldering Iron

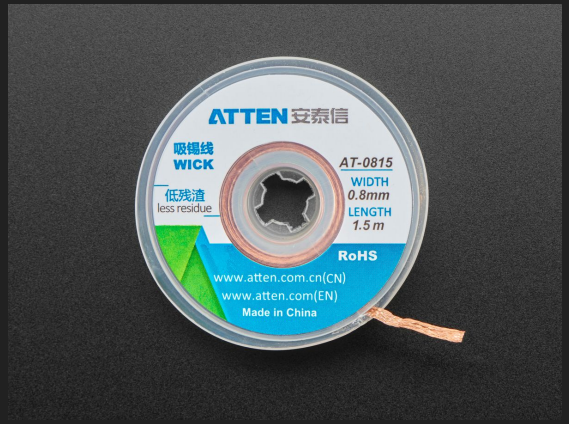
Solder Sucker *(for screw-ups)*

Soldering Materials



Solder

Solder Flux



Solder Wick

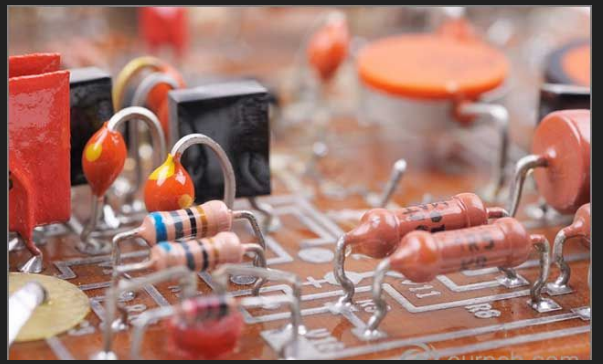
Soldering techniques

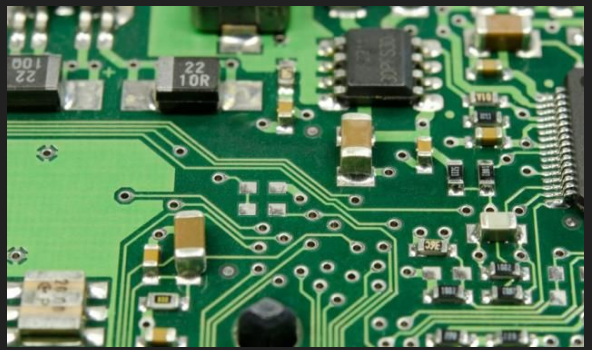
Through-Hole (THT)

- Hand Assembly
- Big Components

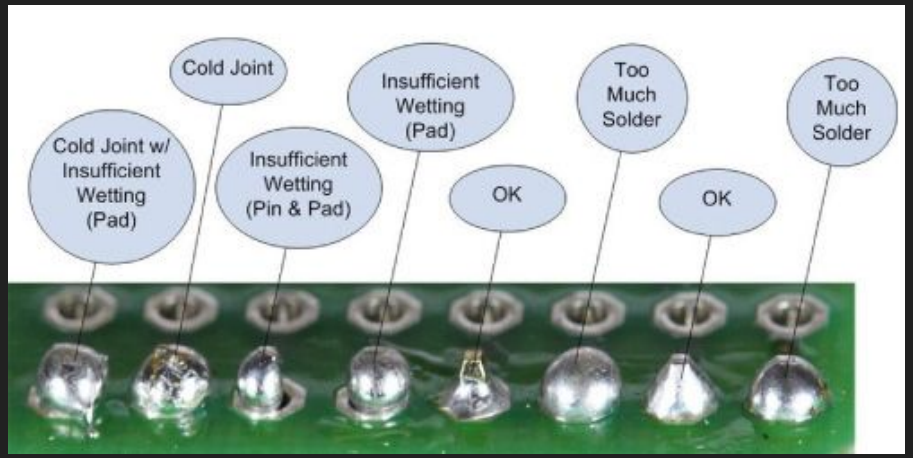
Surface Mount (SMD)

- Cheaper
- Easier for machines

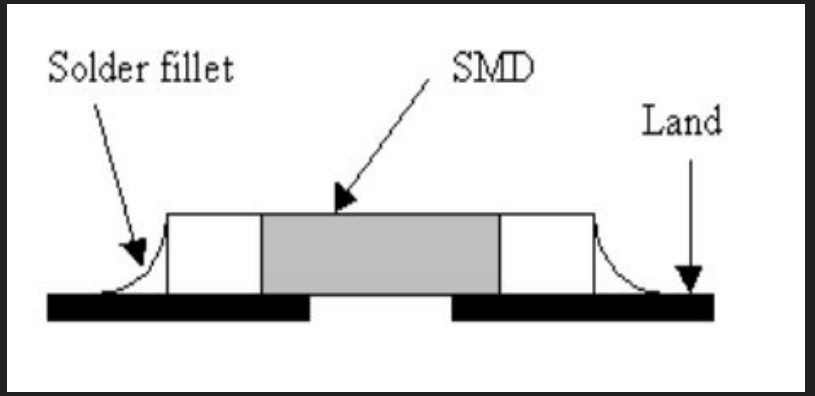




Good solder joints

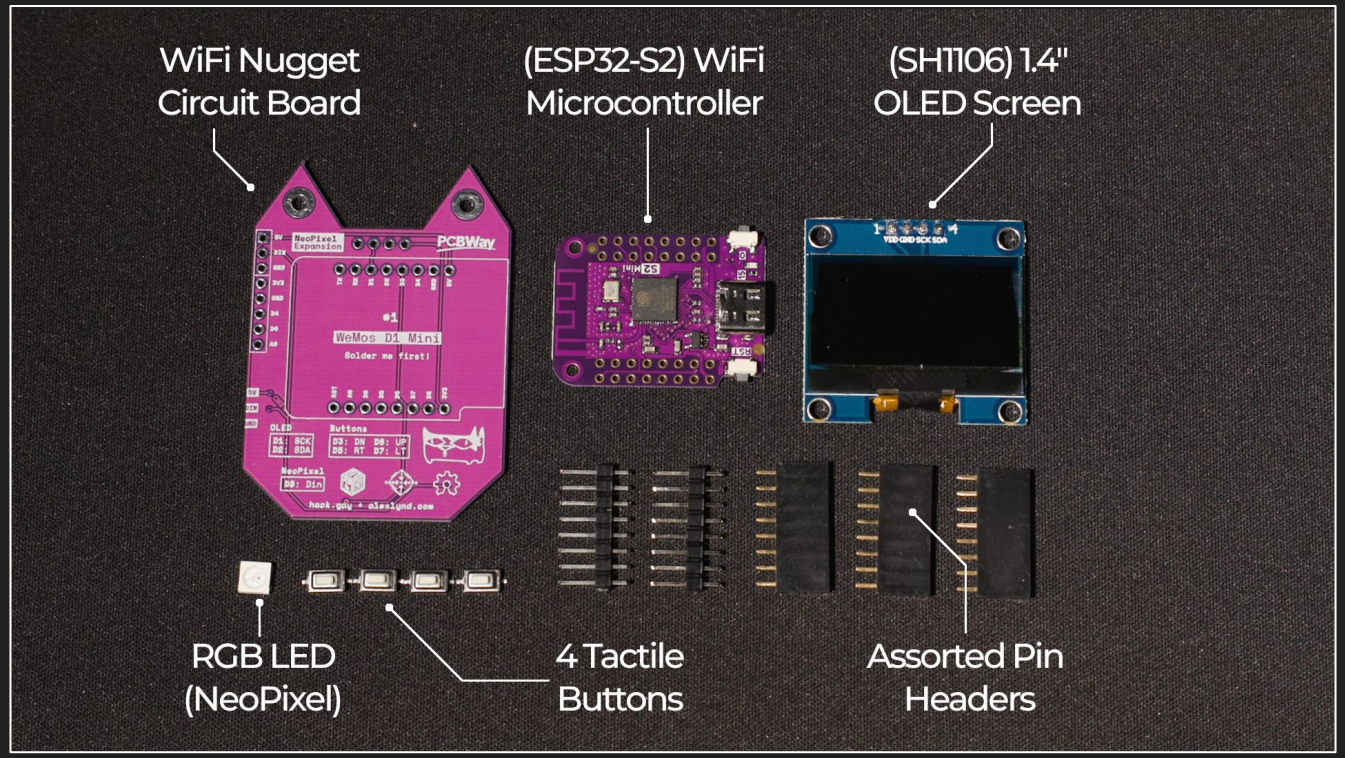


Through-hole joints

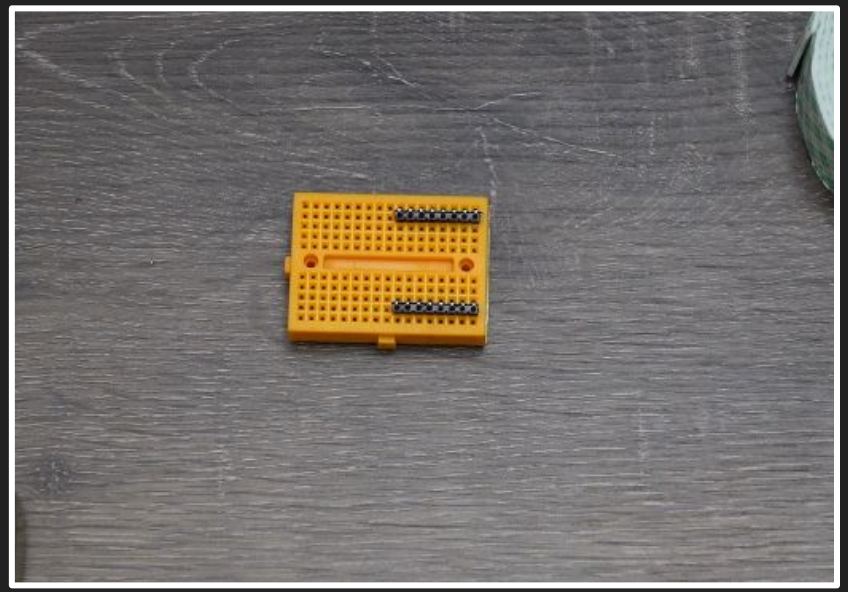


Surface mount pads

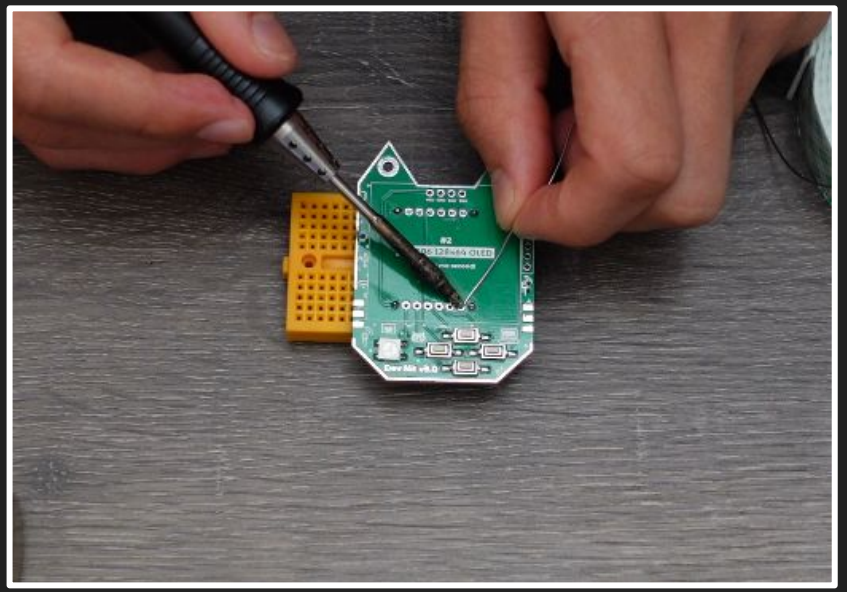
What's in your Nugget Kit



1. Prep the Headers

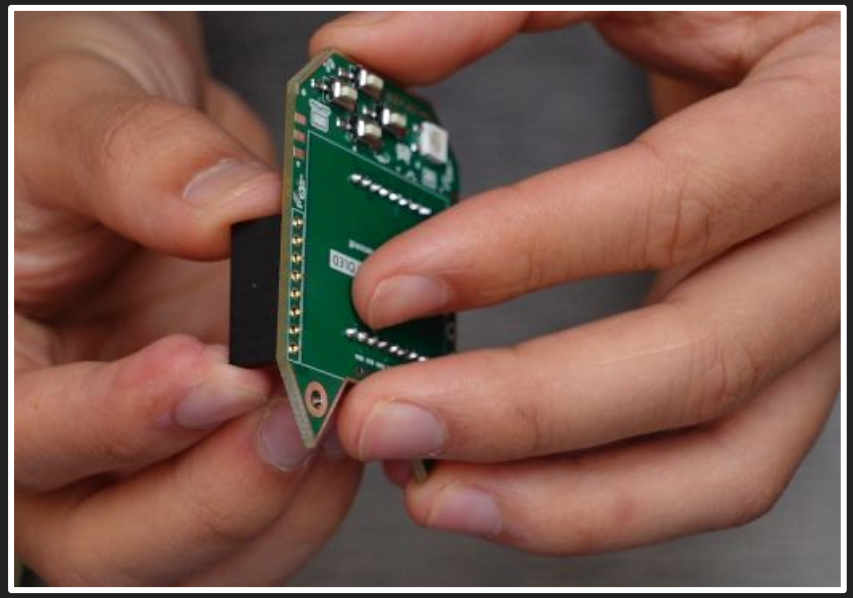


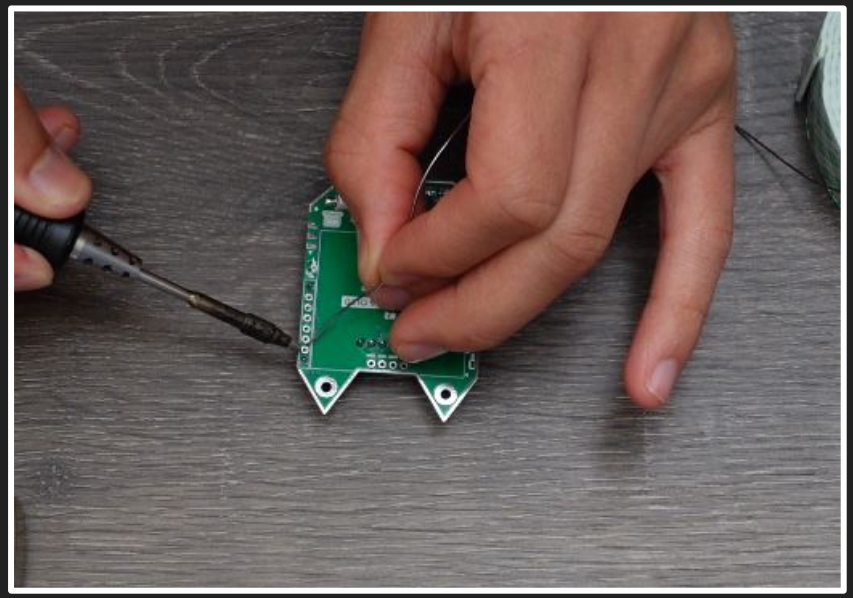
Insert Male Headers Long Side Down



Place Nugget w/ Buttons Facing Up

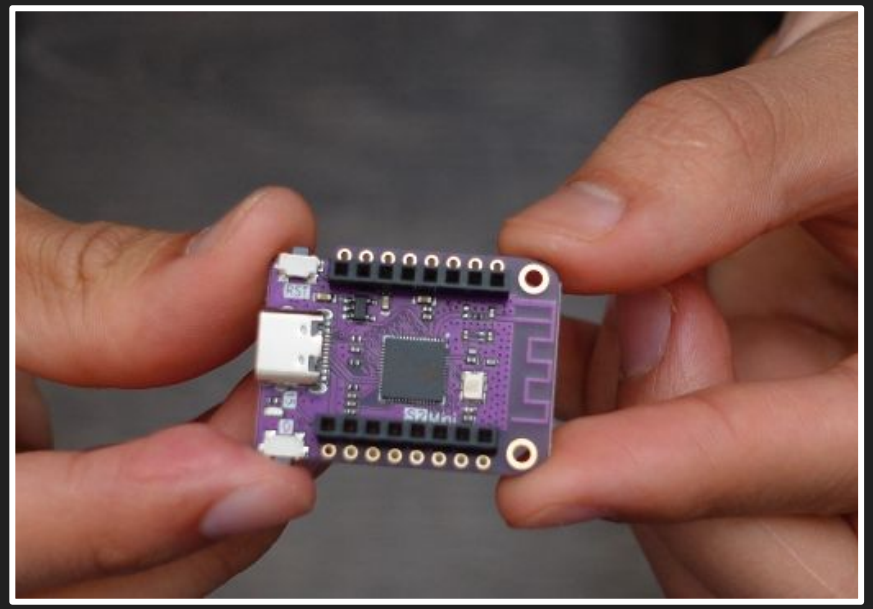
2. Expansion Header



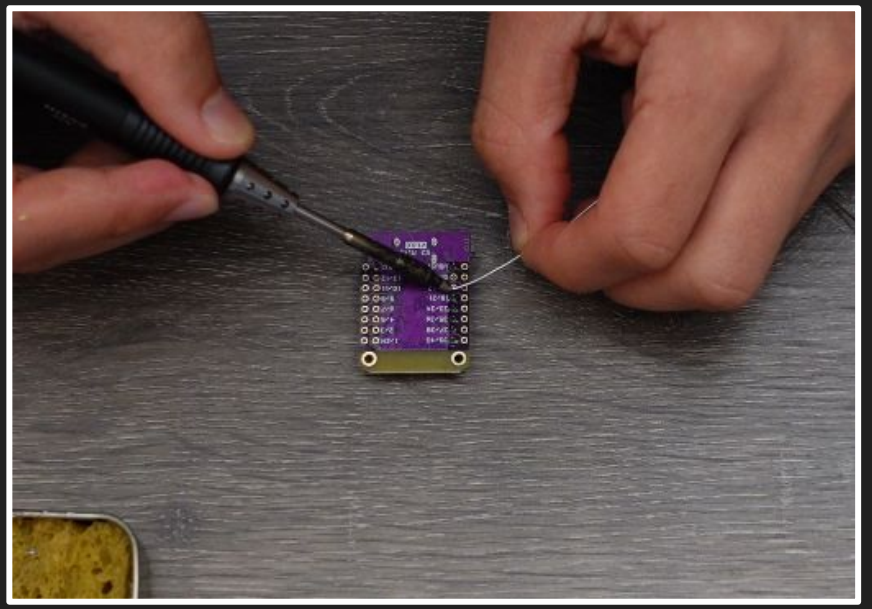


Insert the Long Female Pin Header, and rest the Nugget flush on a flat surface

3. Prep the Microcontroller

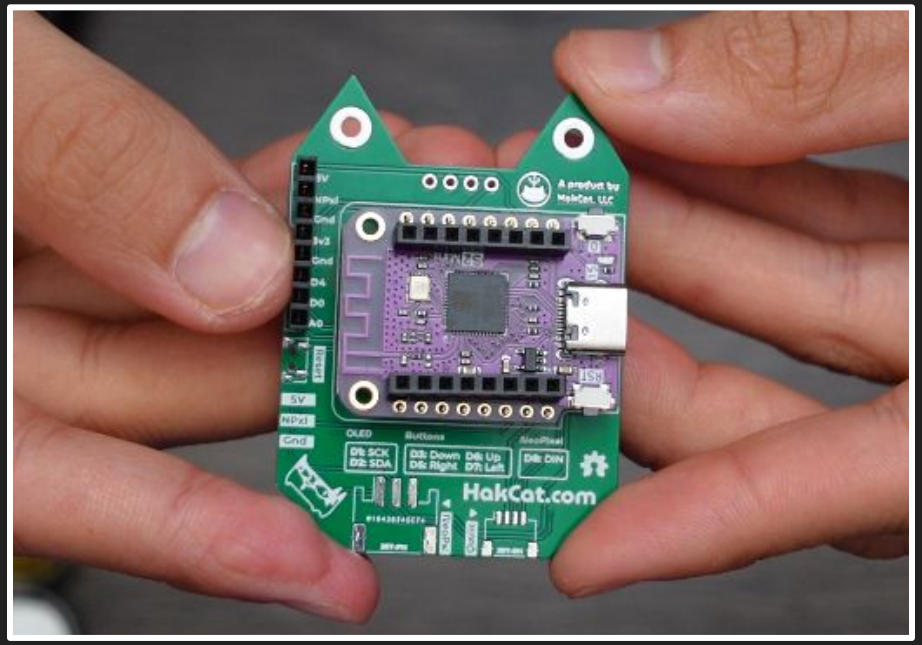


Insert Short Pin Headers on inside rows.

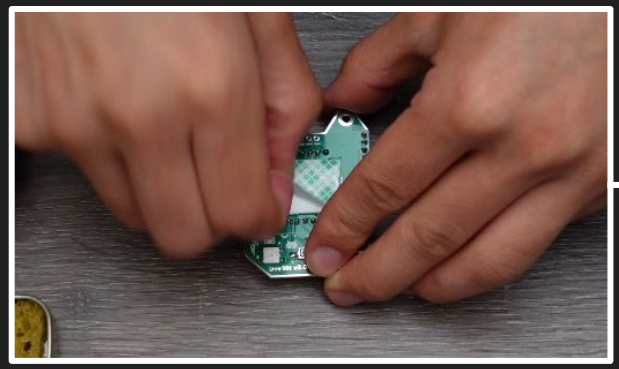


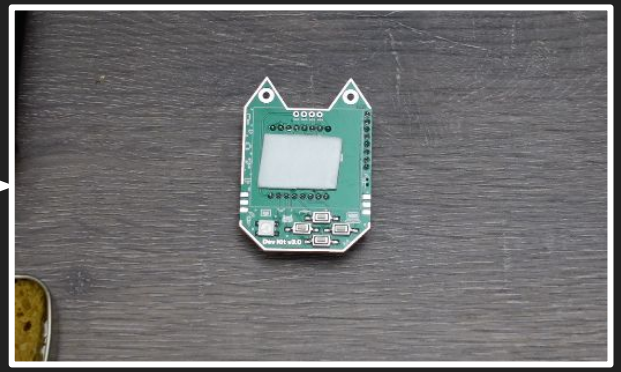
Lie flush on table and solder!

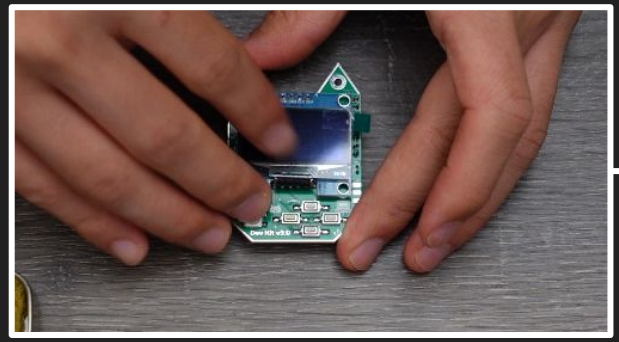
4. Solder the Microcontroller

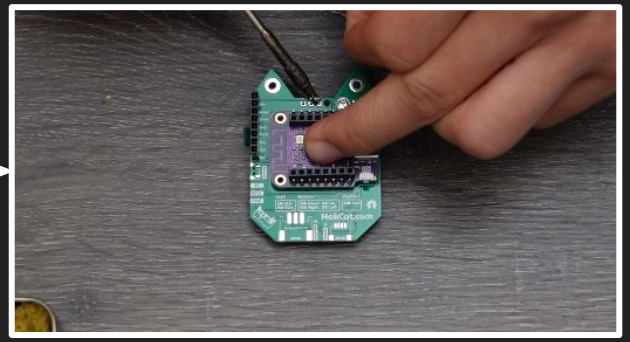


5. Mount & Solder the Screen

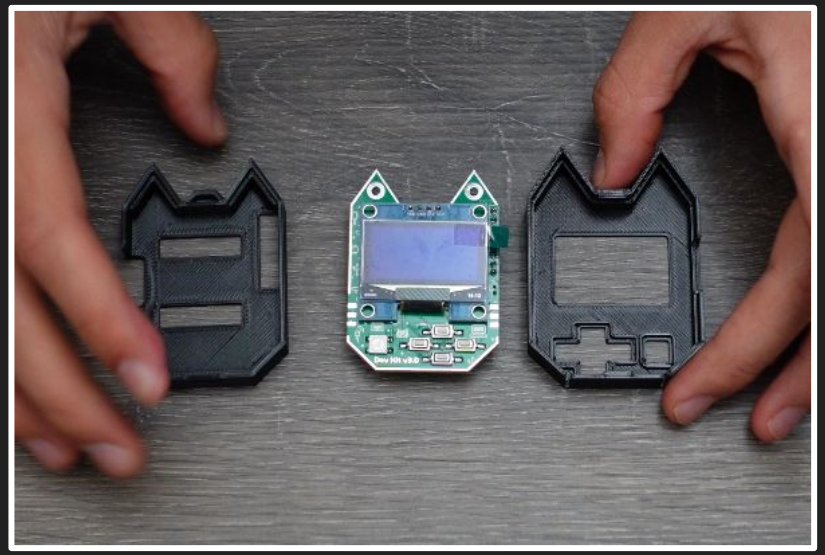








6. Snap on the Case!



Your Nugget is Ready to Hack!

USB Attack Class

1 Hour

🖥️ What are HID Attacks?

Human Interface Device attacks emulate USB devices in order to deliver malicious content to a computer.

HID attacks specifically emulate “trusted” human devices like keyboards.

🖥️ What can be emulated?

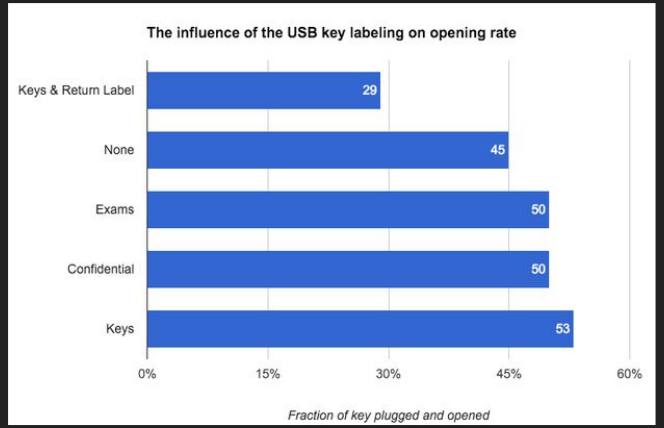
- ⌨️ A **keyboard** can type out pre-programmed malware in seconds.
- 🖱️ A **mouse** can move to keep a victim's screen unlocked.
- A **usb ethernet** adapter can trick computers into re-routing traffic

⌨ What are Keystroke Injection Attacks?

- Emulates a keyboards
- Types out pre-programmed commands
- Computers inherently trust keyboards & humans
- Open & navigate programs, download malware, modify & steal files in seconds

Does this actually work?

- Yes! A study showed that 48% of USB drives left on a university campus were plugged in



Users Really Do Plug in USB Drives They Find

Matthew Tischer[†] Zakir Durumeric[‡†] Sam Foster[†] Sunny Duan[†]
Alec Mori[†] Elie Bursztein[◇] Michael Bailey[†]

[†] University of Illinois, Urbana Champaign [‡] University of Michigan [◇] Google, Inc.
{tischer1, sfoster3, syduan2, ajmori2, mdbailey}@illinois.edu
zakir@umich.edu elieb@google.com

***Abstract*—We investigate the anecdotal belief that end users will pick up and plug in USB flash drives they find by completing a controlled experiment in which we drop 297 flash drives on a large university campus. We find that the attack is effective with an estimated success rate of 45–98% and expeditious with the first drive connected in less than six minutes. We analyze the types of drives users connected and survey those users to understand their motivation and security profile. We find that a drive's appearance does not increase attack success. Instead, users connect the drive with the altruistic intention of finding the owner. These individuals are not technically incompetent, but are rather typical community members who appear to take more recreational risks than their peers. We conclude with lessons learned and discussion on how social engineering attacks—while less technical—continue to be an effective attack vector that our community has yet to successfully address.**

I. Introduction

The security community has long held the belief that users can be socially engineered into picking up and plugging in seemingly lost USB flash drives they find. Unfortunately, median time to connection of 6.9 hours and the first connection occurring within six minutes from when the drive was dropped. Contrary to popular belief, the appearance of a drive does not increase the likelihood that someone will connect it to their computer. Instead, users connect all types of drives unless there are other means of locating the owner—suggesting that participants are altruistically motivated. However, while users initially connect the drive with altruistic intentions, nearly half are overcome with curiosity and open intriguing files—such as vacation photos—before trying to find the drive's owner.

To better understand users' motivations and rationale, we offered participants the opportunity to complete a short survey when they opened any of the files and read about the study. In this survey, we ask users why they connected the drive, the precautions they took, demographic information, as well as standard questions to measure their risk profile and computer expertise. We find that attack was effective against all sub-populations at Illinois. The majority of respondents connected a drive to locate its owner (68%) or out of curiosity (18%).

(a) Unlabeled drive (b) Drive with keys (c) Drive with return label (d) Confidential drive (e) Exam solutions drive

Fig. 1: **Drive Appearances**—We dropped five different types of drives. We chose two appearances (keys and return label) to motivate altruism and two appearances (confidential and exam solutions) to motivate self-interest, as well as an unlabeled control.

Real Life Scenario: Fin7

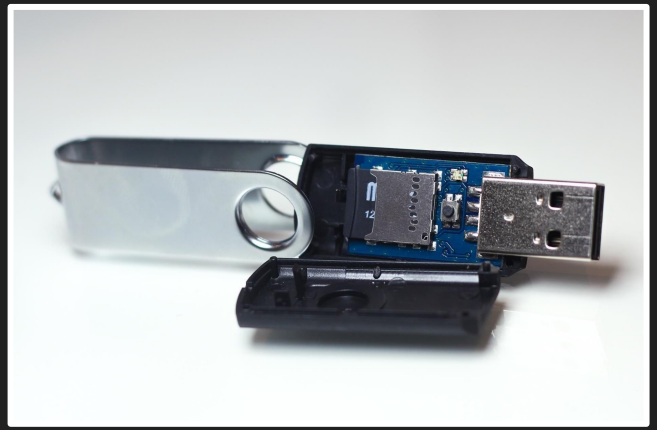
The Fin7 Cybercrime group mailed malicious USB drives that installed ransomware onto targets' computers

- Impersonated Amazon / Health Services / Best Buy etc.
- Social Engineering: enticing packaging
- Fraudulent gift card, thank you letter, USB

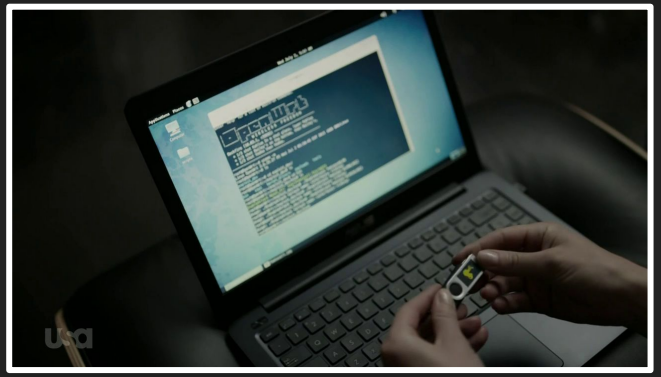
USB Attack Tools

🦆 USB RubberDucky

- First keystroke injection tool, created by Hak5
- Exploded in popularity, featured on shows like Mr. Robot



- ✅ Looks like a flash drive!
- ✅ Simple scripting language
- ❌ Single payload



DuckyScript

A simple language for scripting keyboard-based HID attacks.

- Line-by-line instructions

3 Basic Commands:

- Type Strings!
- Press Key Combos
- Delays or Pauses

Full Screen Windows 10 Update

```
DELAY 3000
GUI r
DELAY 100
STRING https://fakeupdate.net/win10ue/
ENTER
DELAY 3000
F11
```

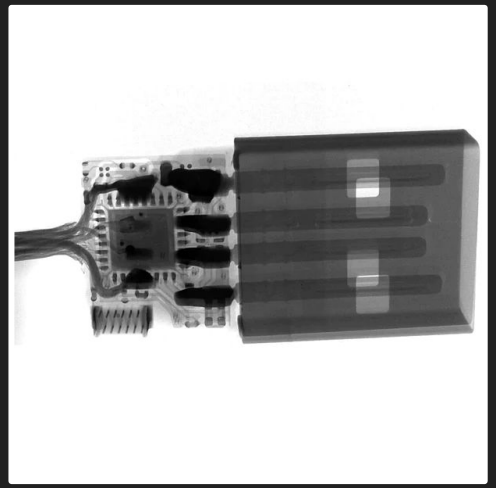
Latest DuckyScript 3.0 allows OS detection & programming logic!

Bash Bunny

- ✅ Flash Storage for Exfiltration
- ✅ Emulate Keyboards, Network Devices, and more!
- ✅ Bluetooth Geofencing
- ✅ Runs Linux
- ❌ Chonky

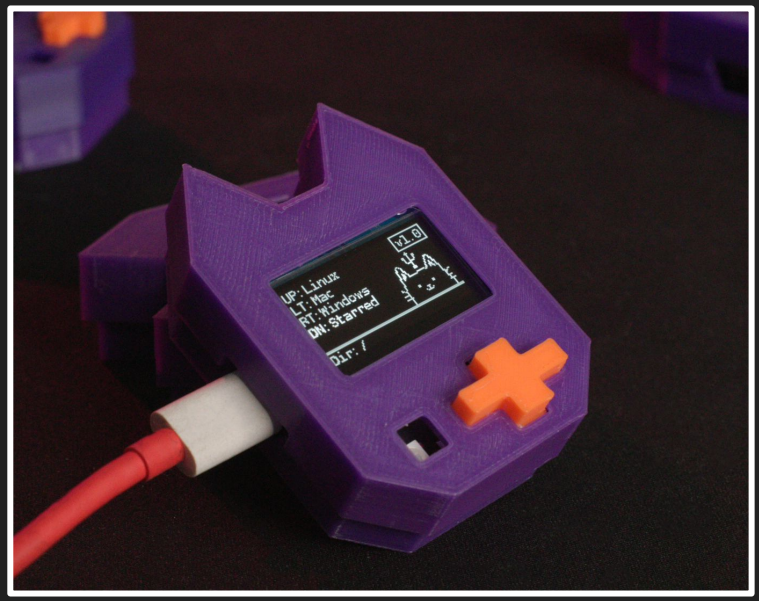
😈 OMG Cable

- ✅ Looks like a charging cable
- ✅ Run attacks over WiFi
  - Geofencing
  - Remote Scripting
- ✅ HID Attacks & Keylogging
- ❌ Inconvenient to program :(



🐱 USB Nugget

- Beginner-focused
- Reactive design
- Easy Debugging



Features:

- Uhh its cute
- Web Interface
- Flash Drive (Payloads & Exfil)

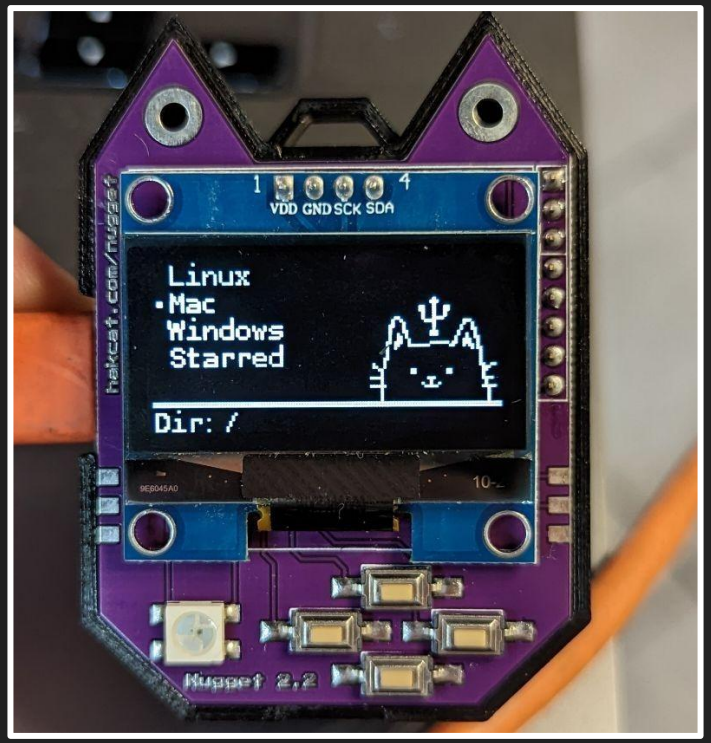
Hacking with the USB Nugget

1 Hour

Navigating the Menu

- **Up / Down**: navigate files & folders
- **Right:** select a folder → payload
- **Left:** go back

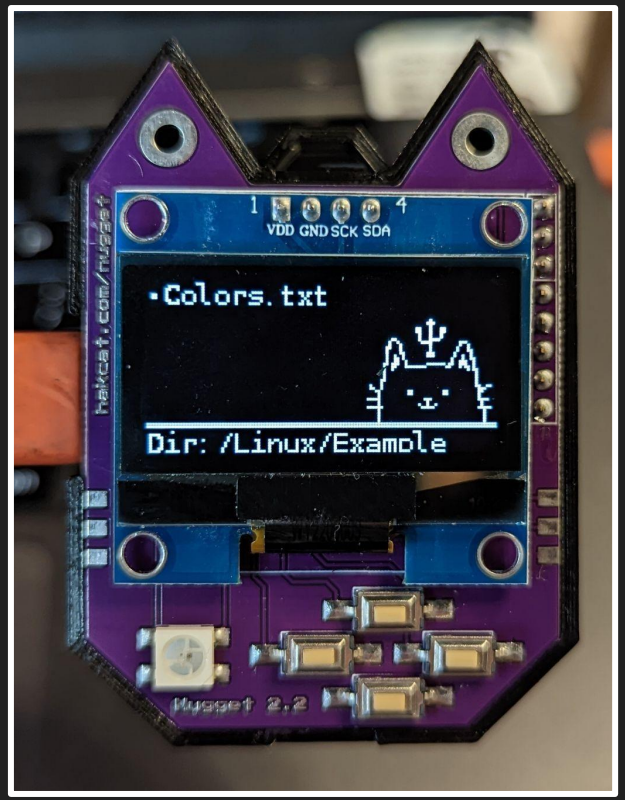
- **The current directory is shown at the bottom of the screen**



Running Payloads

Let’s test your Nugget!

- Select your **Operating System**
- Select the **Example** folder
- Run **colors.txt**.



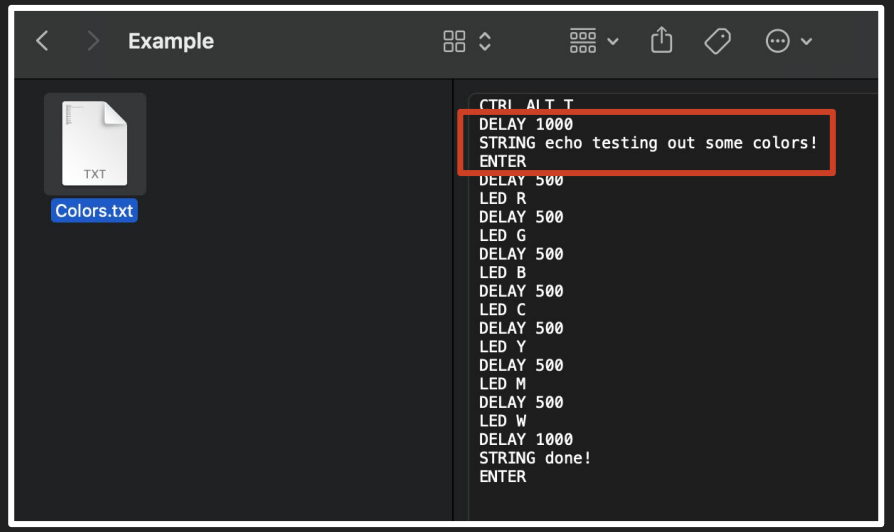
Filesystem & Payload Convention

The USB Nugget has 4 MB of Flash storage!

1. Plug in your Nugget and open the **NUGGET** drive.
2. Use **folders** to organize your payloads
3. **Operating System → Category → Payload.txt**

Edit the Colors Payload

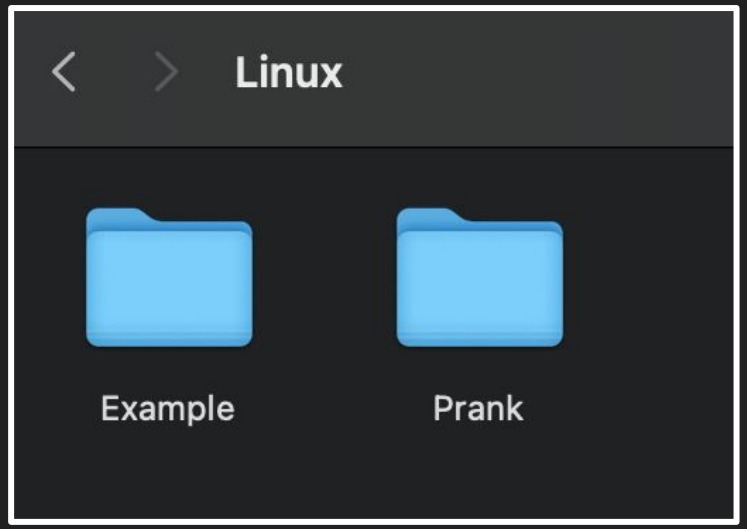
- Navigate to the **colors.txt** payload for your OS.
- Open it with your built-in text editor!
- **Change the output of the colors.txt string!**
- Save the file & run it!



Create a New Payload!

Suggested categories:

- Credentials
- Mobile
- Phishing
- **Prank**
- Exfiltration
- Prank
- Recon
- Remote Access



Create Your First Payload

👉 Tip: Work Backwards

Let's write our first payload! We're going to create a classic RickRoll.

Payload Methodology:

1. **End Goal:** What will it do?
2. **Intermediate Steps:** What programs /commands need to run?
3. **Pseudo-Code:** Outline
4. **DuckyScript**

Intermediate Steps

To execute the rickroll we need to:

1. Open a web browser
2. Open a Youtube video url
3. Turn up the volume!
4. Play video in full-screen

PseudoCode

Let’s take it a step further!

- **Keyboard shortcuts**
- **Terminal commands**
- **Things to type**
- **Delays!**

Delays are **essential** since the Nugget types extremely fast - and programs need time to open!

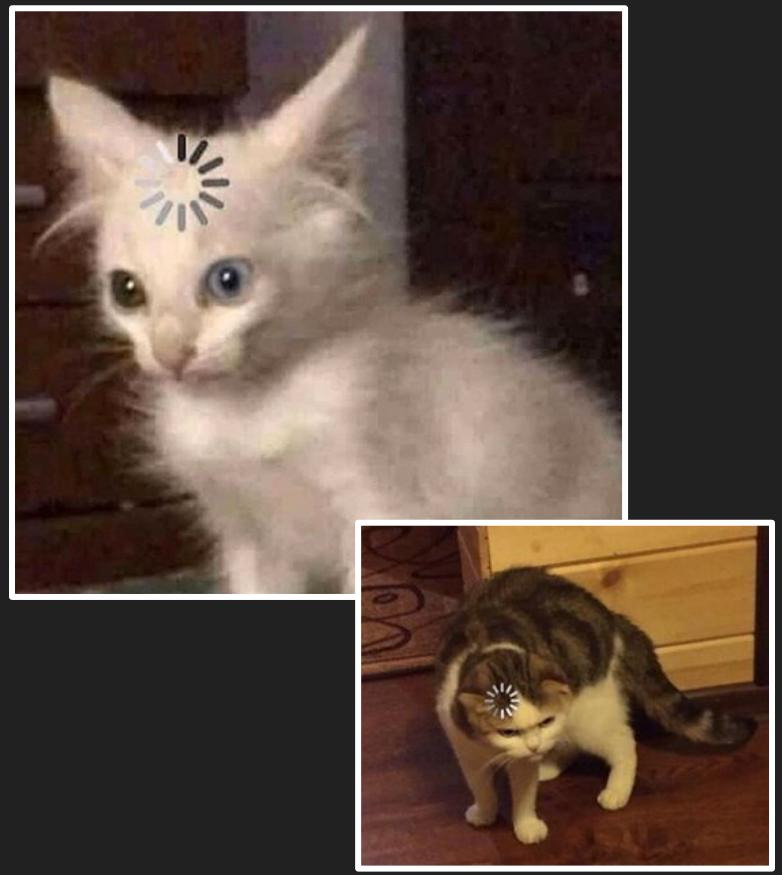
Example PseudoCode

- **Press a key combo** to open a search dialogue
- **Wait** for it to open
- **Type** in chrome / firefox
- **Press Enter**
- **Wait** for browser to open
- **Type** in the url
- **Press enter**
- **Wait** for url to load
- **Press a key** for full screen

Finally, let's turn your pseudocode into actual DuckyScript!

👉 Tip: Delays and Timing

- Delays make one-way scripts possible.
- Because microcontrollers work so quickly, many of the commands would not work without adding time for commands to finish.
- In testing, we should start out with generous delays and gradually optimize them without breaking anything.



Basic DuckyScript Commands

Commands:
REM
STRING
DELAY
DEFAULTDELAY
LED

Modifier Keys:
- CTRL or Control
- SHIFT
- ALT
- **GUI**

Standard Keys:
- a-z
- A-Z
- 0-9
- F1-F12

Key:
- ENTER
- MENU
- DELETE
- HOME
- INSERT
- UPARROW
- DOWNARROW
- LEFTARROW
- RIGHTARROW
- TAB
- END
- ESC
- SPACE
- PAUSE
- PRINTSCREEN
- CAPSLOCK
- NUMLOCK
- SCROLLLOCK
- PAGEUP
- PAGEDOWN

👉 Tip: HotKey Combos & Shortcuts

- Windows 10: https://bit.ly/2nH8IWk
- Linux (Debian): https://bit.ly/3hKs5Nu
- MacOS: https://apple.co/3EfZGGK
- Raspberry Pi OS: https://bit.ly/3TE77x1

Intermediate Payloads

Get Started Creating Attack Payloads!

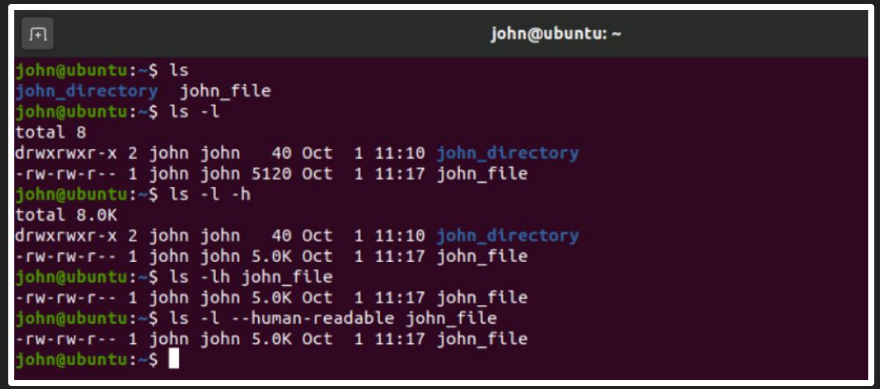
Payload 1: Command Line Exercise

👉 Tip: Using the Command Line

The fastest way to do bad things on a computer is through terminal / powershell / command prompt.

You can:

- Create & modify files
- Open applications
- Run networking commands
- And more!



👉 Tip: Terminal Shortcuts

Quickest way to open a terminal on different operating systems.

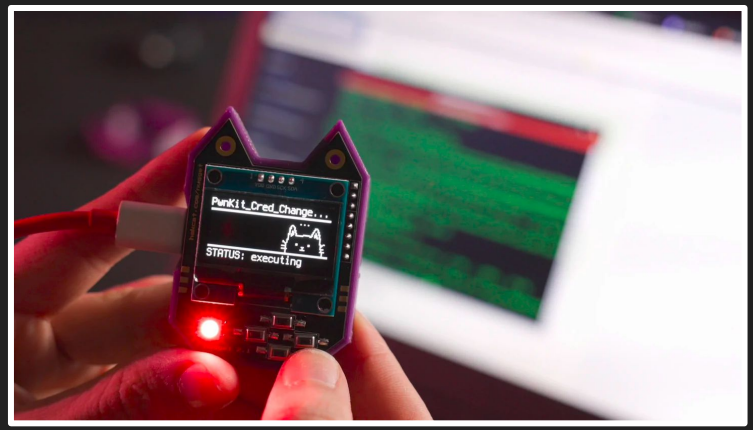
Linux: CTRL ALT T

Mac:

- CTRL SPACE
- terminal
- ENTER

Windows:

- GUI R
- cmd
- ENTER



😺 Challenge: Dogecoin Ransom Message

Open a fake ransomware site in full screen using a terminal, and read a ransom message demanding crypto!

Hint:

- Use “say” or “espeak” commands
- Function keys can enable fullscreen
- https://www.cryptoprank.com/#/crypto

Bonus: Turn up the volume & lock the computer

Payload 2: Stagers & Remote Execution

👉 Tip: Stagers

Using the DuckyScript payload as a stager lets us download external malware or executables!

Manual	Type out the whole damn script
Storage	Deploy locally from a flash drive - less can go wrong
Remote	Single command, dynamic payload

🐱 Challenge: **Bee Movie Attack**

Download the entire bee movie script onto the victim's desktop as a text file!

Hints:

- https://bit.ly/3ZZElL1
- CLI tools like **curl** or **wget** can download urls

Bonus: Narrate the bee movie script and download 3 cursed pictures of Barry Benson to the victim's computer

👉 Tip: Web Interface

Let's set up the **web interface** to try a remote attack!

- Open the **.usbnugget.conf** file in a text editor
- Edit the network & password parameters!
- **Do not add a space!** :(
- Save, and restart your Nugget

Access the Web Interface

The web interface allows you to run stored payloads or write new ones!

- Join the Wi-Fi Access point you set up on your Nugget!
- In a browser, navigate to: http://192.168.4.1
- Try running your payload from the web browser!

Payload 3: Data Exfiltration

👉 Tip: Data Exfiltration

How can we exfiltrate data from a victim device?

- **Locally**
  - Physical access,
  - Quicker & less conspicuous
- **Remote**
  - Better for long term access
  - Creates web traffic

Let's try it **locally** first!

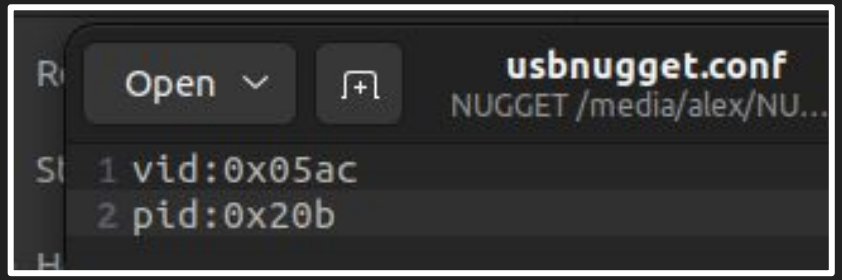
Advanced Data Exfiltration: Side-Channel

- Keyboards & HID devices have bi-lateral communication
- Computers can toggle CAPSLOCK or indicator keys
- We can use this to exfiltrate data in a protected environment by bitbang data via binary

👉 Tip: HID Emulation

We can emulate common USB / HID vendors!

- Open the **.usbnugget.conf** file
- By default, we emulate an Apple Keyboard to prevent MacOS systems from flagging the Nugget
- USB vendor list: http://www.linux-usb.org/usb.ids
- Try changing the VID/PID, and reset your Nugget for the change to take effect!



VID: Vendor ID
PID: Product ID

Real Life Scenario: Razer Admin Exploit

A Razer Synapse bug lets you get Windows admin privileges by plugging in a Razer mouse or keyboard.

https://www.bleepingcomputer.com/news/security/razer-bug-lets-you-become-a-windows-10-admin-by-plugging-in-a-mouse/

🐱 Challenge: **Data Exfiltration**

Steal a file containing secret credentials from the Raspberry Pi and emulate a Logitech device!

Hint:

- VID / PID list: http://www.linux-usb.org/usb.ids
- .txt file located at ~/Pi/Documents/creds.txt
- Flash drive mounts at ~/media
- Linux commands: cd, cp

Bonus:

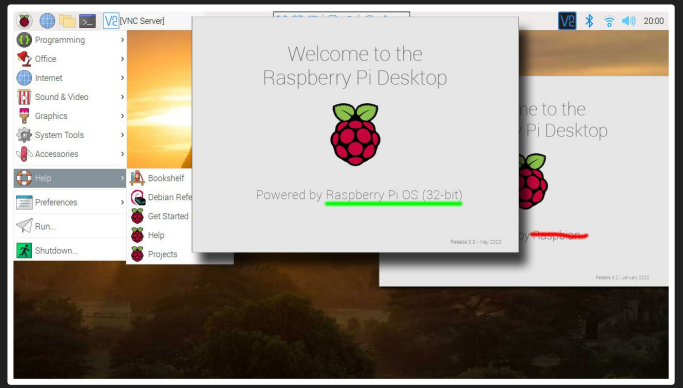
- Steal other **.txt** files and **images** from the home directory!
- Save network info or filesystem info as a text file

Payload Challenge

CTF: Design the Highest Scoring Payload

In our last section, we'll be working together to write payloads to win a prize!

- Our target is a Raspberry Pi computer running Linux (Raspbian).
- Your goal is to make a payload that causes the most amount of mischief!



Example Actions

- Steal a file
- Delete a file
- Write a file with a message in it
- Steal a hash
- Corrupt a hash
- Kill the computer
- Plant a keylogger
- Rickroll
- Join rogue Wi-Fi network
- Team ASCII banner
- Grabify link tracker
- Cron task
- Netcat backdoor
- Change background
- Auto-restart computer
- Auto-quit programs

Attack Criteria

For our final challenge, we'll be dividing into teams and working on HID attack scripts to achieve a number of specific goals.

Each team will get time to write their script, and then 90 seconds to plug in and run their script.

The team to earn the most number of points wins a prize! Points are awarded when a team achieves the actions below:

Points	File Operations	Flags	Destruction	Advanced (x 2 points)
10	Create a text file with a message	Display a message demanding bitcoins	Reboot or shut down the computer	Create a Cron Task
20	Delete a file	Change the Wallpaper	Kill the network connection	Download & execute a bash or Python file
30	Download a file to the desktop	Get a Grabify link hit from the target computer	Kill the computer (No boot)	Steal data via Grabify
40	Create a fork bomb	RickRoll in a browser window	Create startup task that shuts down computer	Join an (evil) Wi-Fi network
50	Steal a file off the computer	Change RPI's SSH MOTD Banner to your team name	Encrypt files or the file system (ransomware)	Netcat backdoor (remote access)

Links to USB Rubber Ducky Payloads

- Payload - Non-Malicious Auto Defacer
- Payload - Lock Your Computer Message
- Payload - Ducky Downloader
- Payload - Ducky Phisher
- Payload - FTP Download / Upload
- Payload - Restart Prank
- Payload - Silly Mouse, Windows is for Kids
- Payload - Windows Screen rotation hack
- Payload - Powershell Wget + Execute
- Payload - mimikatz payload
- Payload - MobileTabs
- Payload - Ugly Rolled Prank
- Payload - XMAS
- Payload - Pineapple Association (VERY FAST)
- Payload - Remotely Possible
- Payload - Batch Wiper/Drive Eraser
- Payload - Generic Batch
- Payload - Paint Hack
- Payload - Local DNS Poisoning
- Payload - Deny Net Access
- Payload - RunEXE from SD
- Payload - Run Java from SD
- Payload - Download mimikatz, grab passwords and email them via gmail
- Payload - Hotdog Wallpaper
- Payload - Android 5.x Lockscreen
- Payload - Chrome Password Stealer
- Payload - Website Lock
- Payload - Windows 10 : Download & Change Wallpaper
- Payload - Windows 10 : Download & Change Wallpaper another version
- Payload - Windows 10 : Download and execute file with Powershell
- Payload - Windows 10 : Disable windows defender
- Payload - Windows 10 : Disable Windows Defender through powershell
- Payload - Windows 10 : Wifi, Chrome Dump & email results
- Payload - Windows 7 : Logoff Prank
- Payload - Netcat Reverse Shell
- Payload - Fake Update screen
- Payload - Rickroll
- Payload - Fast Meterpreter
- Payload - Data-Exfiltration / Backdoor
- Payload - Fake Update screen
- Payload - OSX Sudo Passwords Grabber
- Payload - OSX Root Backdoor
- Payload - OSX User Backdoor
- Payload - OSX Local DNS Poisoning
- Payload - OSX Youtube Blaster
- Payload - OSX Photo Booth Prank
- Payload - OSX Internet Protocol Slurp
- Payload - OSX Ascii Prank
- Payload - OSX iMessage Capture
- Payload - OS X Wget and Execute
- Payload - OSX Passwordless SSH access (ssh keys)
- Payload - OSX Bella RAT Installation
- Payload - OSX Sudo for all users without password
- Payload - MrGray's Rubber Hacks
- Payload - Copy File to Desktop
- Payload - Youtube Roll
- Payload - Disable AVG 2012
- Payload - Disable AVG 2013
- Payload - EICAR AV test

Payload Repository

For more payloads, check out these payload repositories:

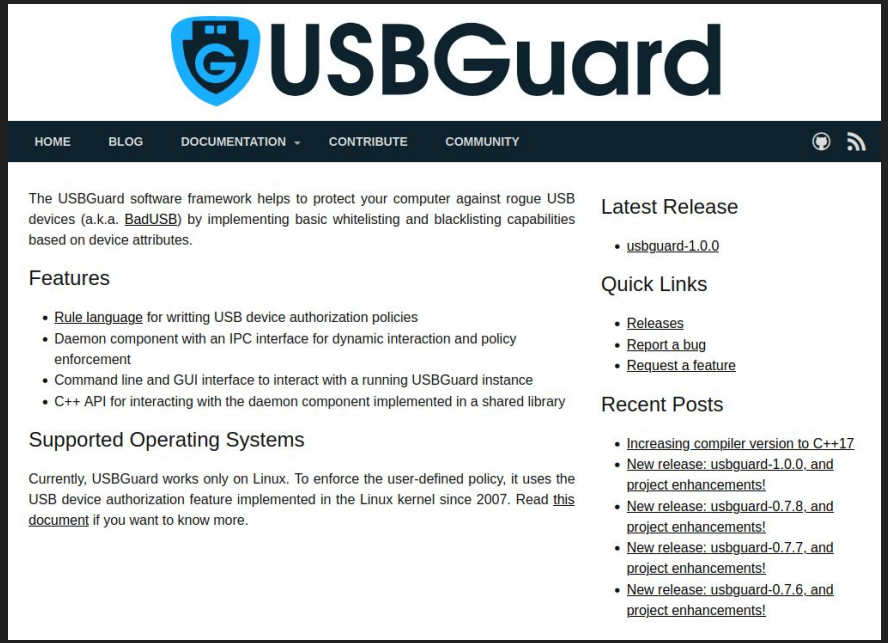
https://hak5.org/blogs/payloads/

https://github.com/HakCat-Tech/USB-Nugget-Payloads

Taking it Further

Mitigation

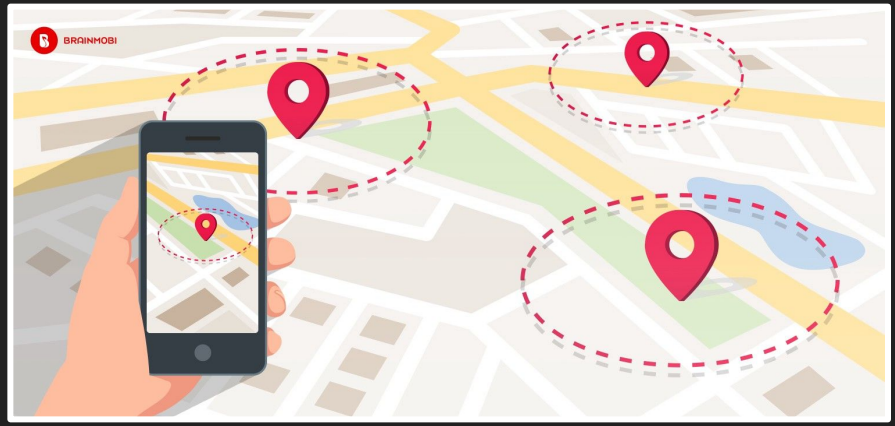
- Don’t plug in random devices into your computer.
- Whitelisting / Blacklisting USB Devices
- USBGuard or other keystroke injection detection tools can look for fast keystrokes



GeoFence Attacks

GeoFence attacks can determine if specific people are nearby, by looking for the presence of their laptop / cell phone.

This can be done by looking for known WiFi or BlueTooth devices.



Mobile Attacks

Mobile phones (iOS and Android) also support HID keyboards!

Check out mobile payloads here:

https://github.com/hak5/usbrubberducky-payloads/tree/master/payloads/library/mobile

Other USB Attacks: Ethernet

- This Bash Bunny payload emulates a USB-ethernet adapter, and pretends to be the network gateway.
- This allows it to intercept network traffic.
- Works on locked computers

https://shop.hak5.org/blogs/bash-bunny/network-hijack-attacks-with-the-bash-bunny

Thanks for coming!

Follow **@alexlynd** for upcoming events
& check out **lyndlabs.io** for more info.

Learn more about the Nugget at: **usbnugget.com**