INJECTYLL-HIDE

Pushing the Future of Hardware Implants to the Next Level

Jonathan Fischer, Jeremy Miller

@c4m0ufl4g3

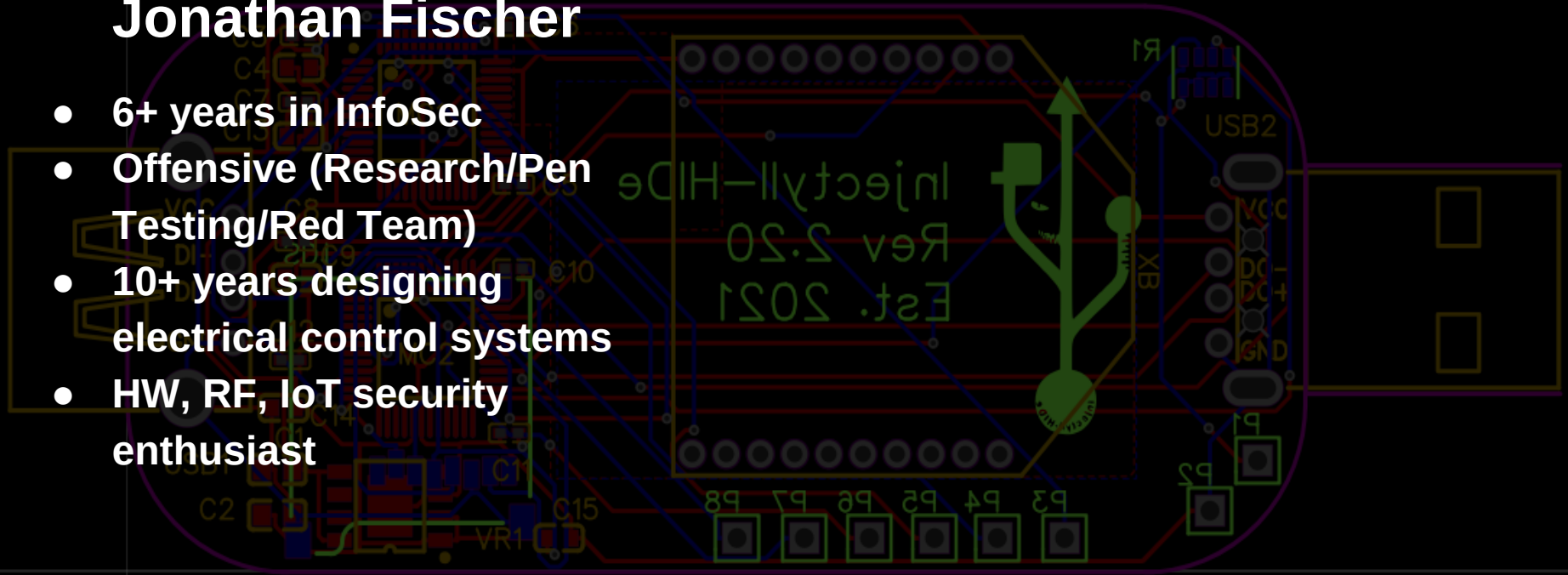
@Injectyll_HIDe

@allTheJurm

Who are we?

Jonathan Fischer

- 6+ years in InfoSec
- Offensive (Research/Pen Testing/Red Team)
- 10+ years designing electrical control systems
- HW, RF, IoT security enthusiast



Who are we?

Jonathan Fischer

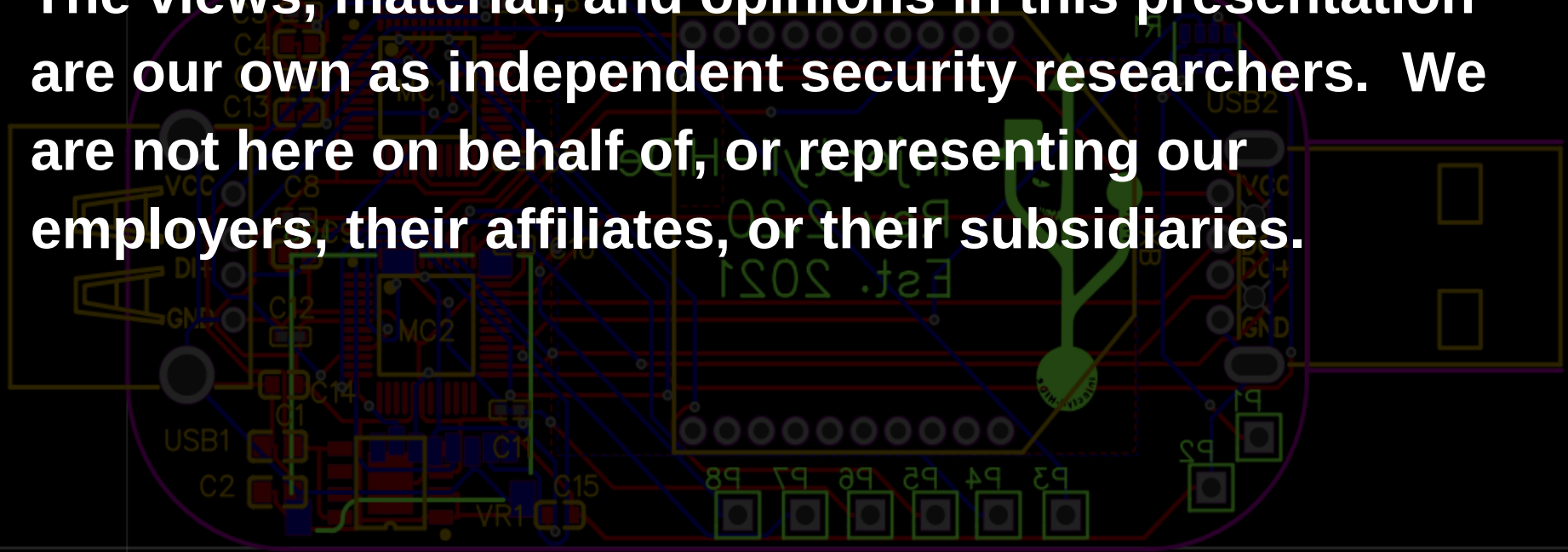
- 6+ years in InfoSec
- Offensive (Research/Pen Testing/Red Team)
- 10+ years designing electrical control systems
- HW, RF, IoT security enthusiast

Jeremy Miller

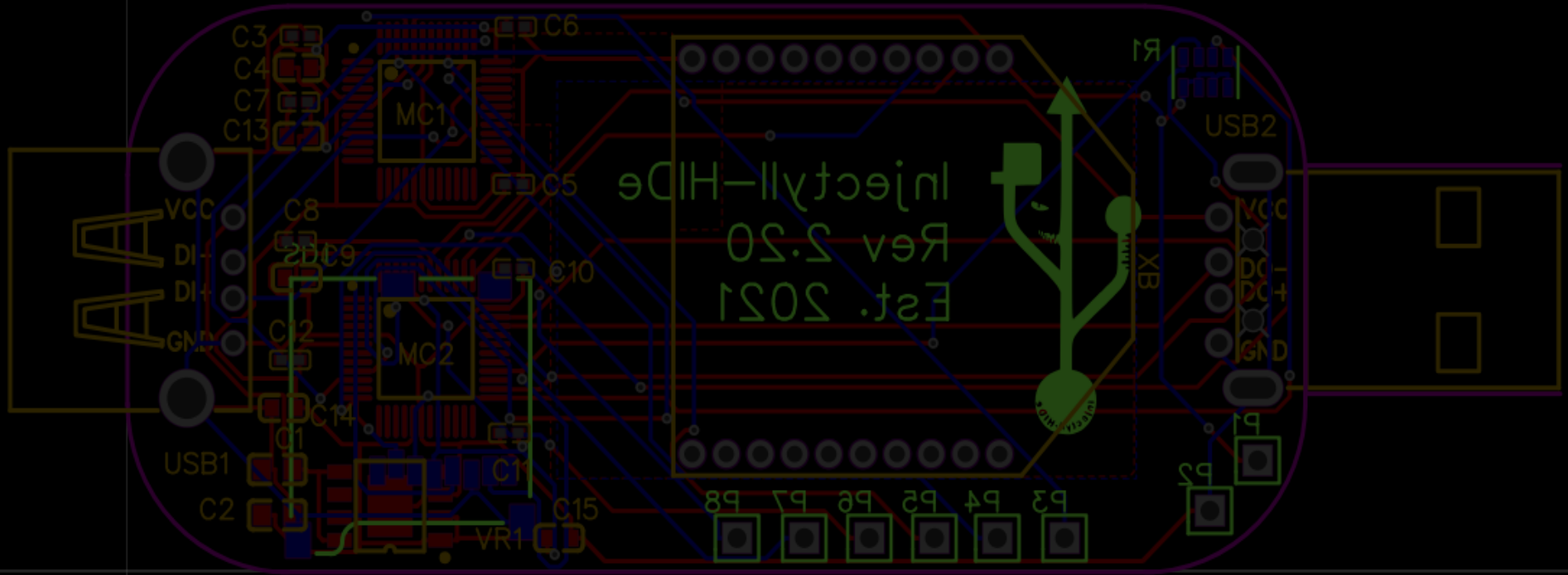
- 12+ years in InfoSec
- Red Team
- Blue Team
- Security Research
- Security Engineering
- Retail, Financial, Hosting, Life Sciences.

Work Disclaimer

The views, material, and opinions in this presentation are our own as independent security researchers. We are not here on behalf of, or representing our employers, their affiliates, or their subsidiaries.

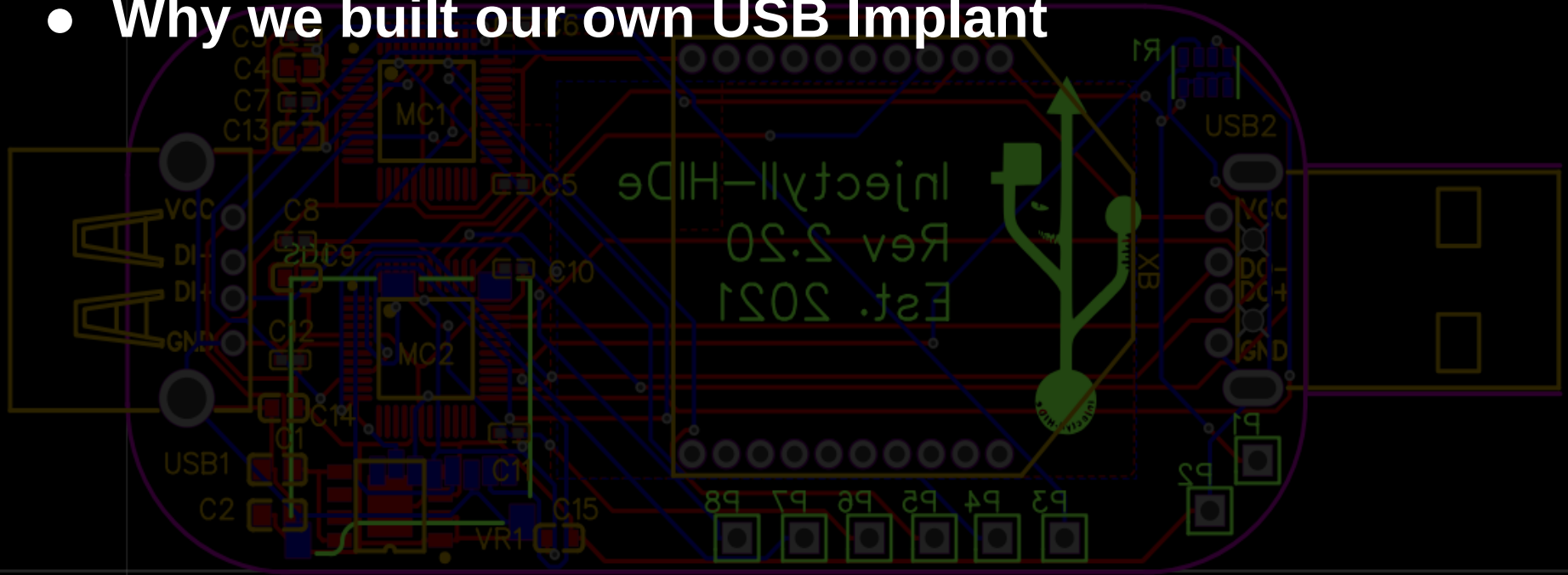


What's this talk about?



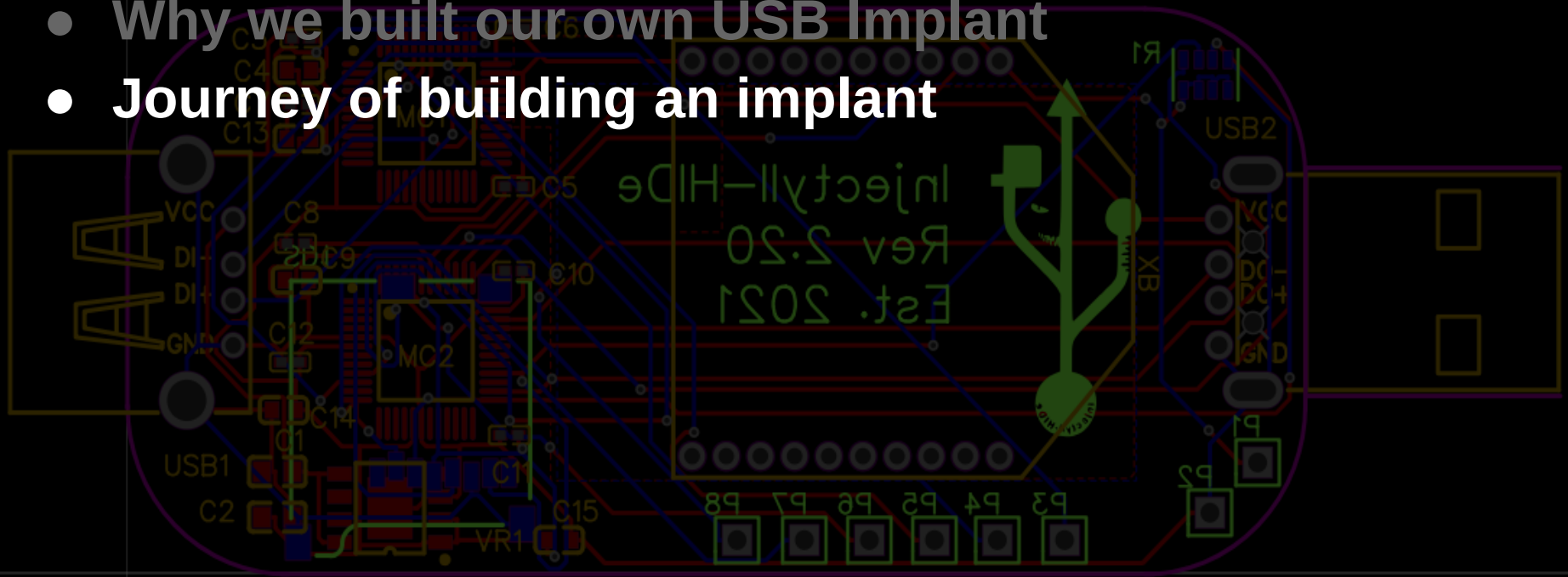
What's this talk about?

- **Why we built our own USB Implant**



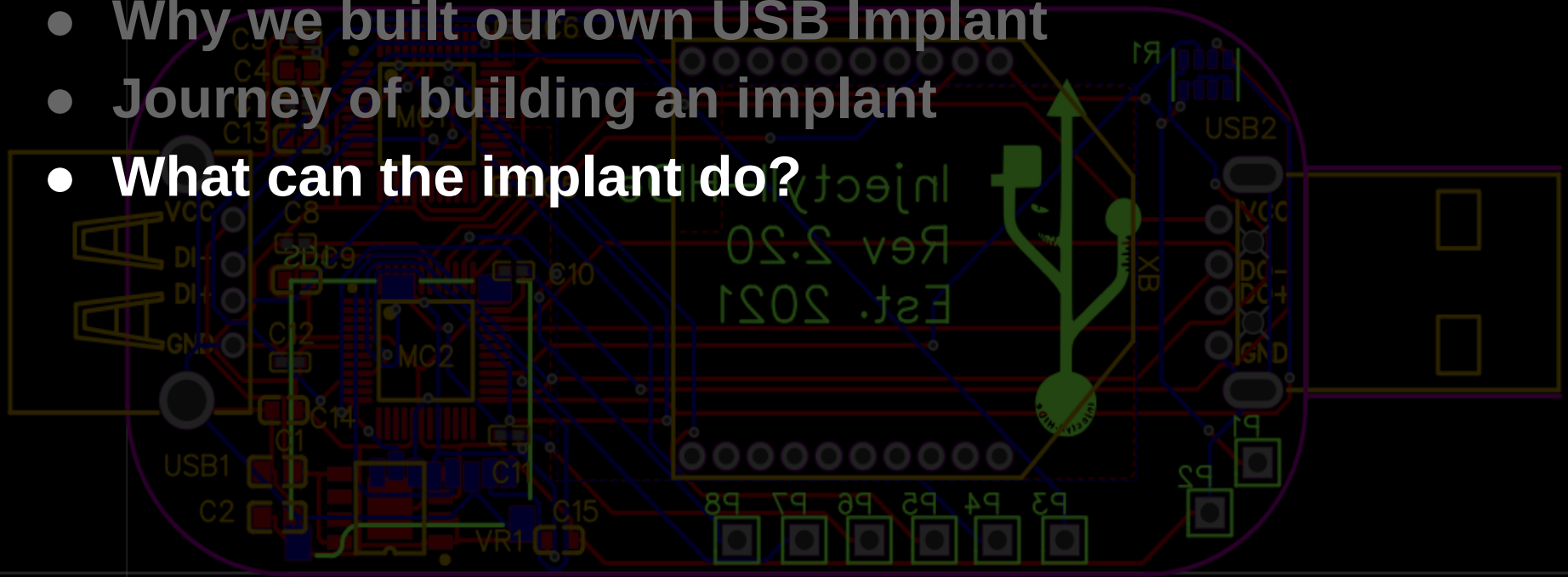
What's this talk about?

- Why we built our own USB Implant
- **Journey of building an implant**

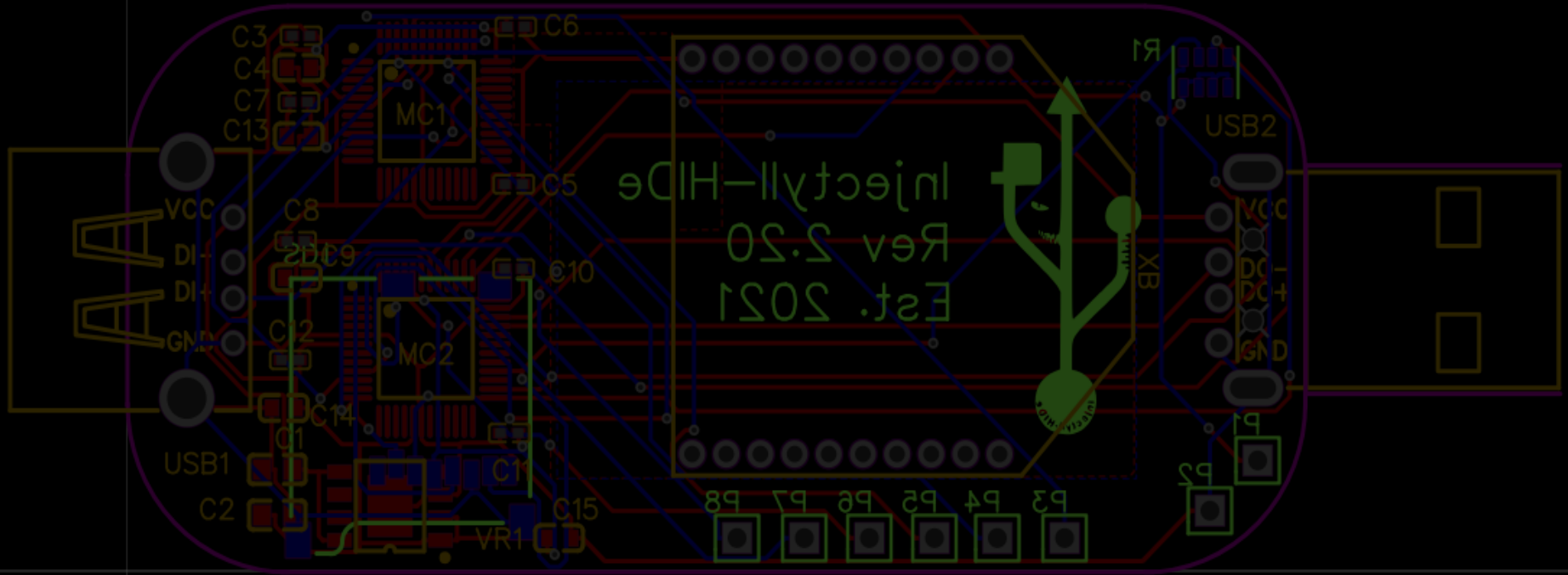


What's this talk about?

- Why we built our own USB Implant
- Journey of building an implant
- **What can the implant do?**



Hardware Attacks. Why?



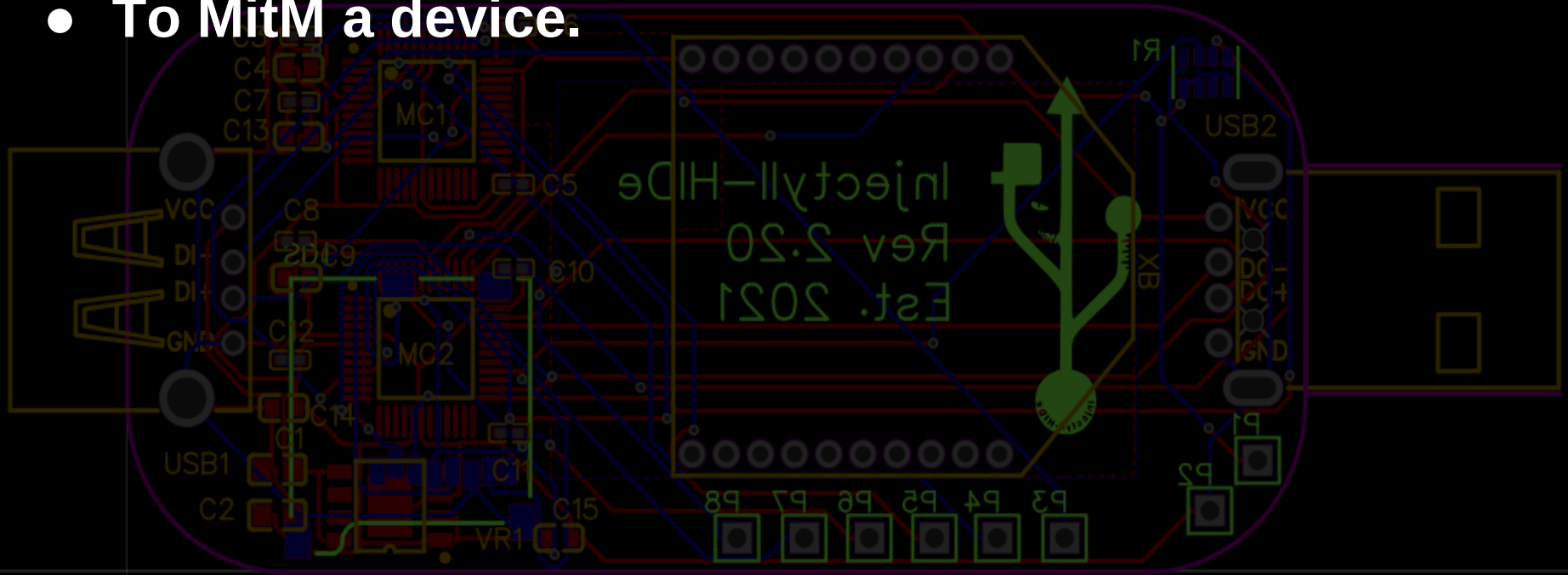
@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

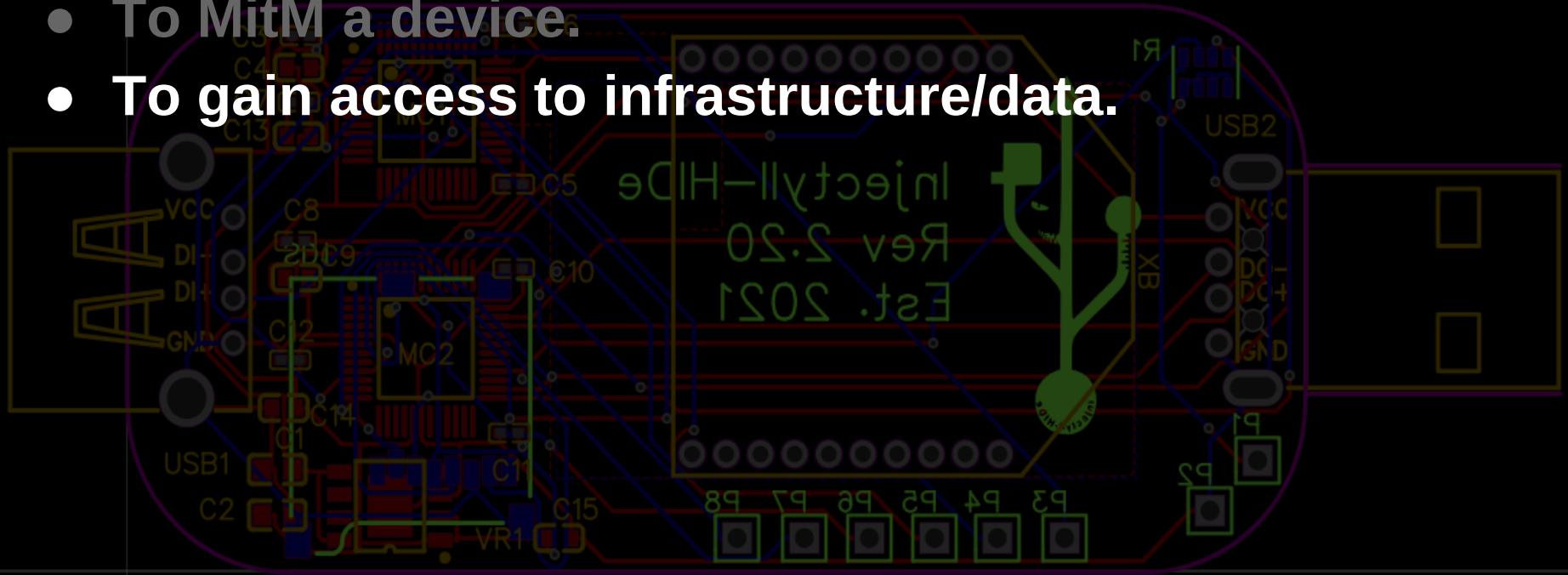
Hardware Attacks. Why?

- **To MitM a device.**



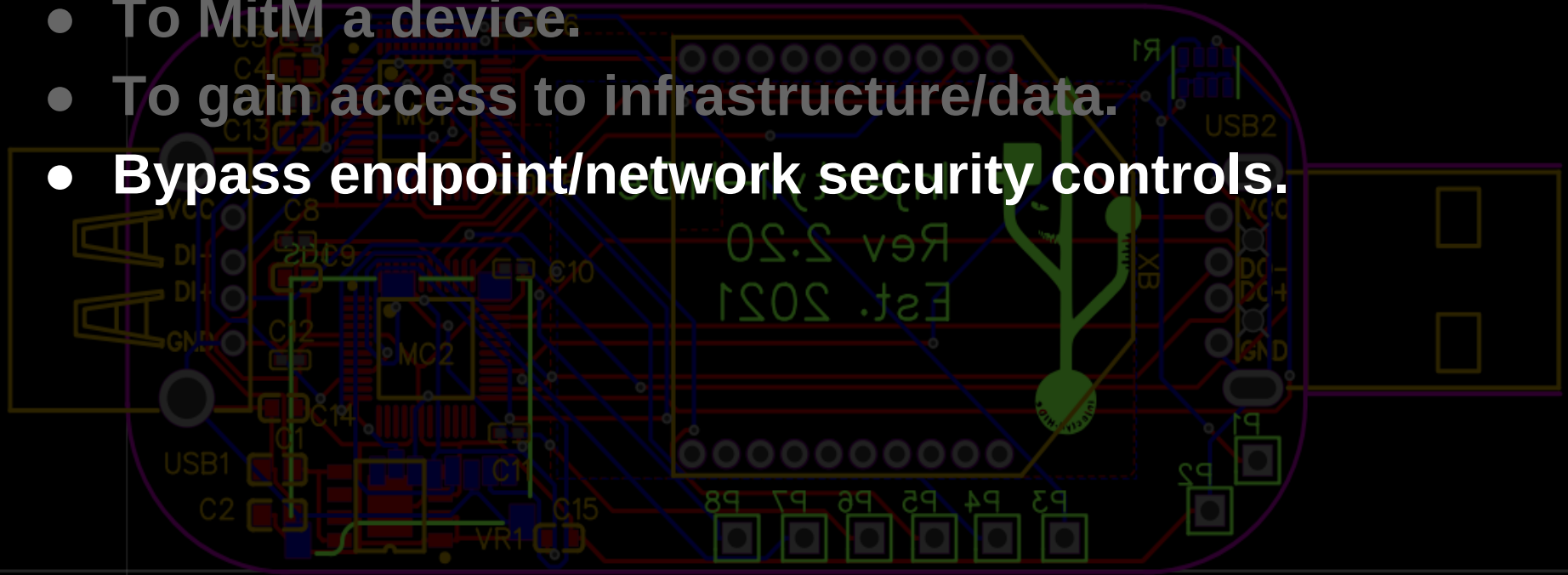
Hardware Attacks. Why?

- To MitM a device.
- **To gain access to infrastructure/data.**



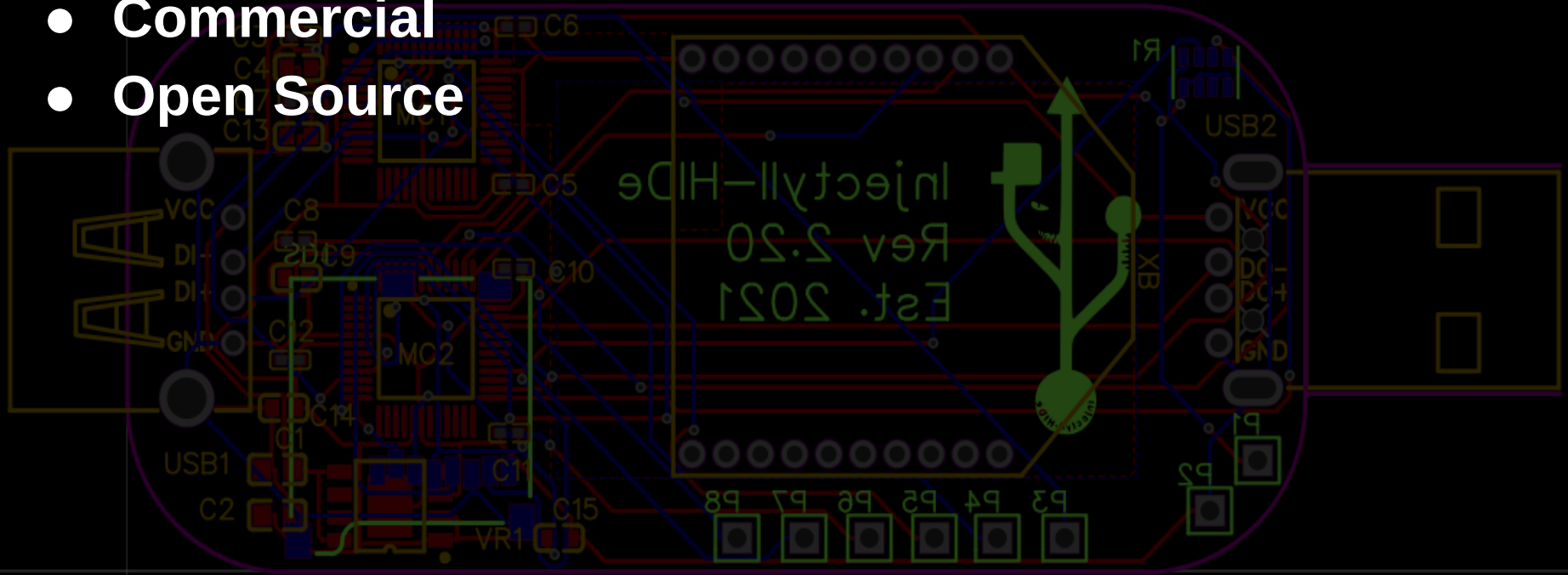
Hardware Attacks. Why?

- To MitM a device.
- To gain access to infrastructure/data.
- **Bypass endpoint/network security controls.**



What's out there now?

- Commercial
- Open Source



Commercial


Keycroc

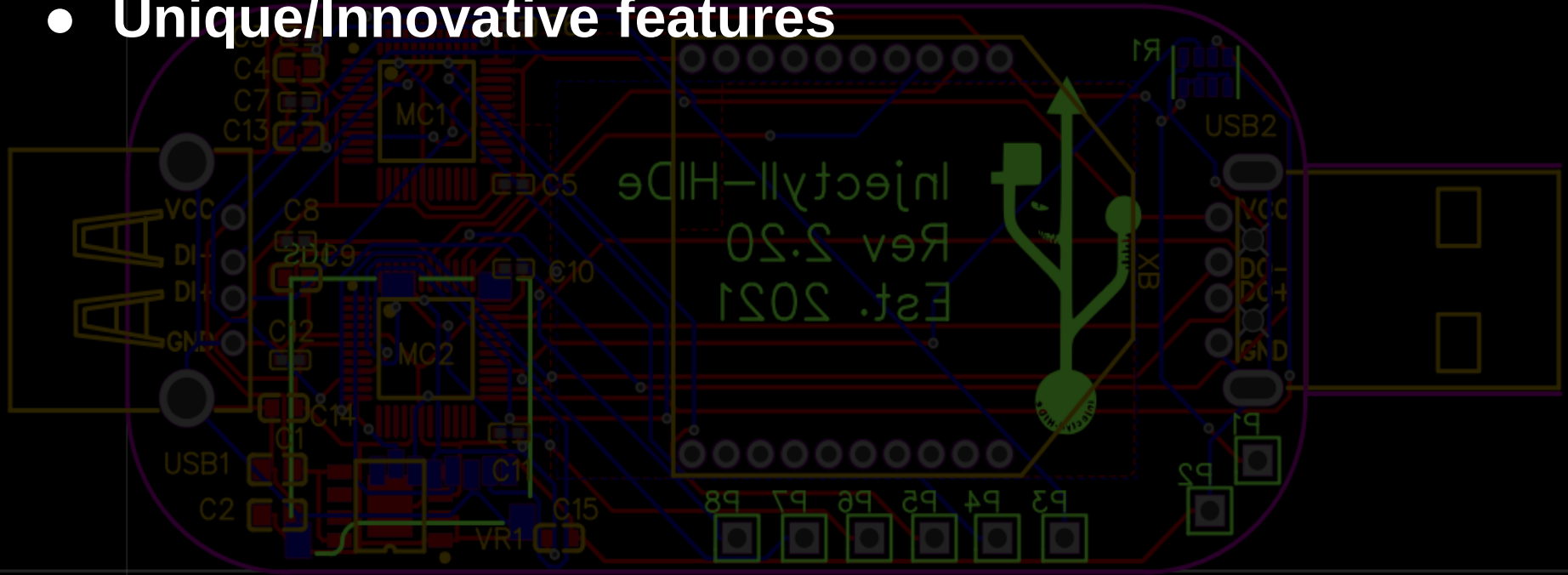

O.MG


Keelog
KeyGrabber
Module
USB


USBNinja
Ninja Pro
Module
V1.1
USB Ninja Pro ADAPTER

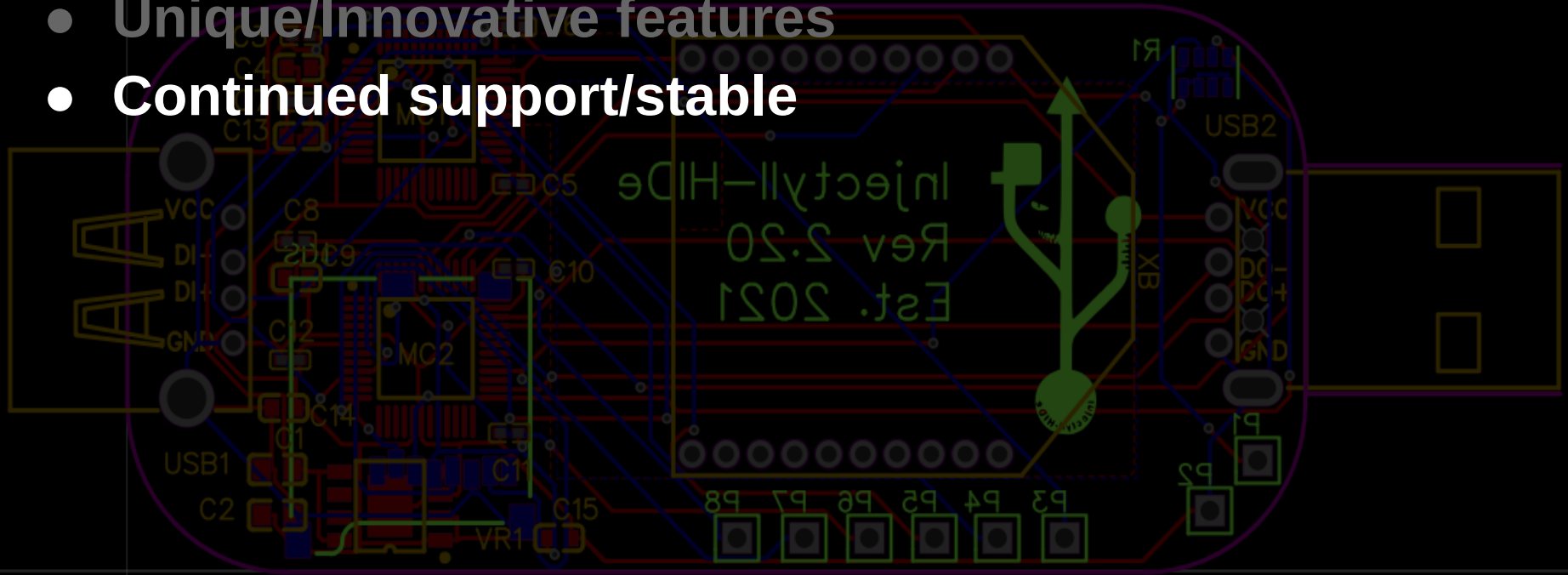
Commercial

- **Unique/Innovative features**



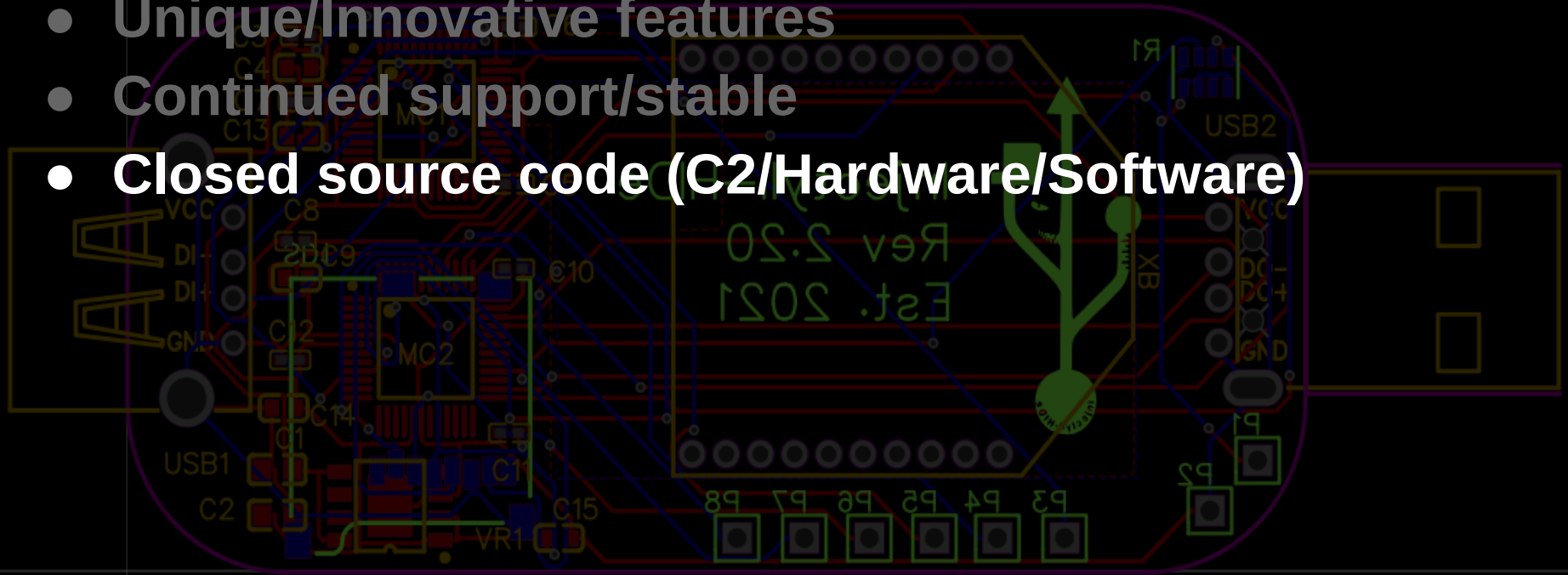
Commercial

- Unique/Innovative features
- **Continued support/stable**

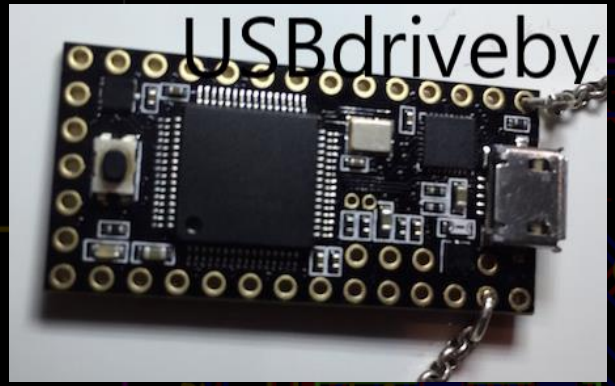


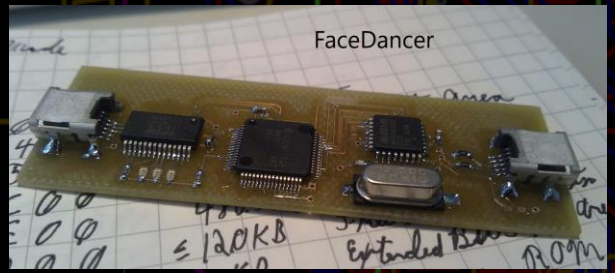
Commercial

- Unique/Innovative features
- Continued support/stable
- **Closed source code (C2/Hardware/Software)**



Open Source





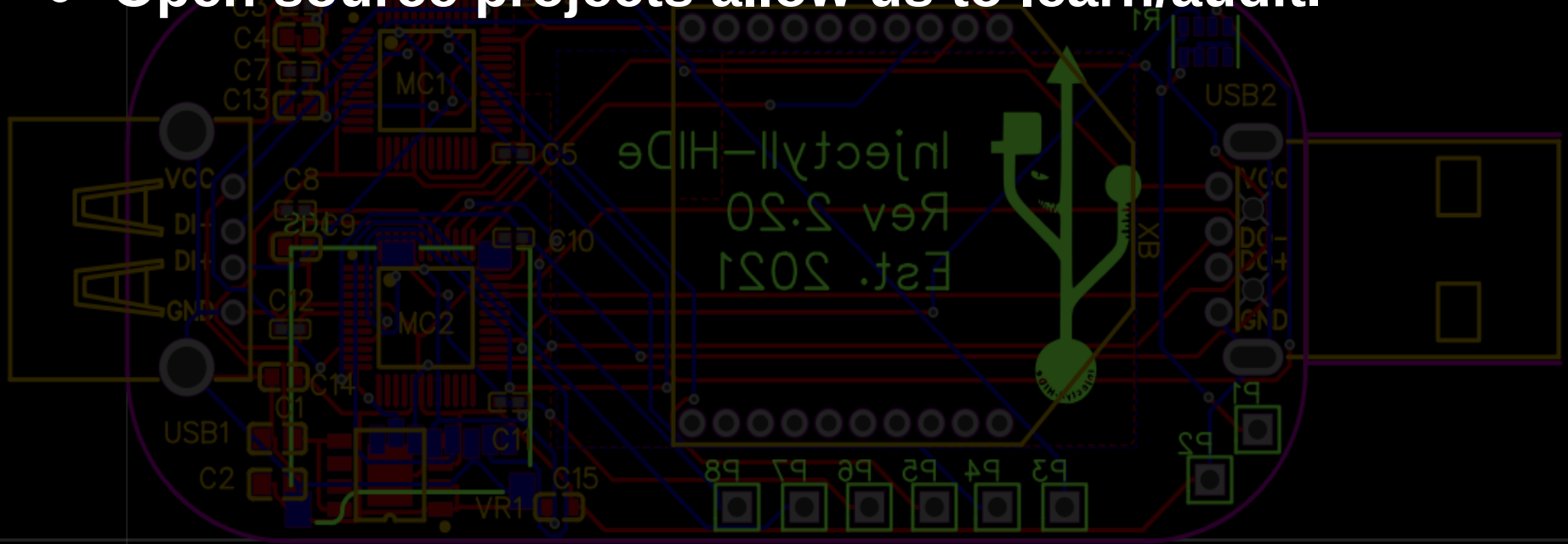
@c4m0ufl4g3

@allTheJurm

@Injectyll_HIDe

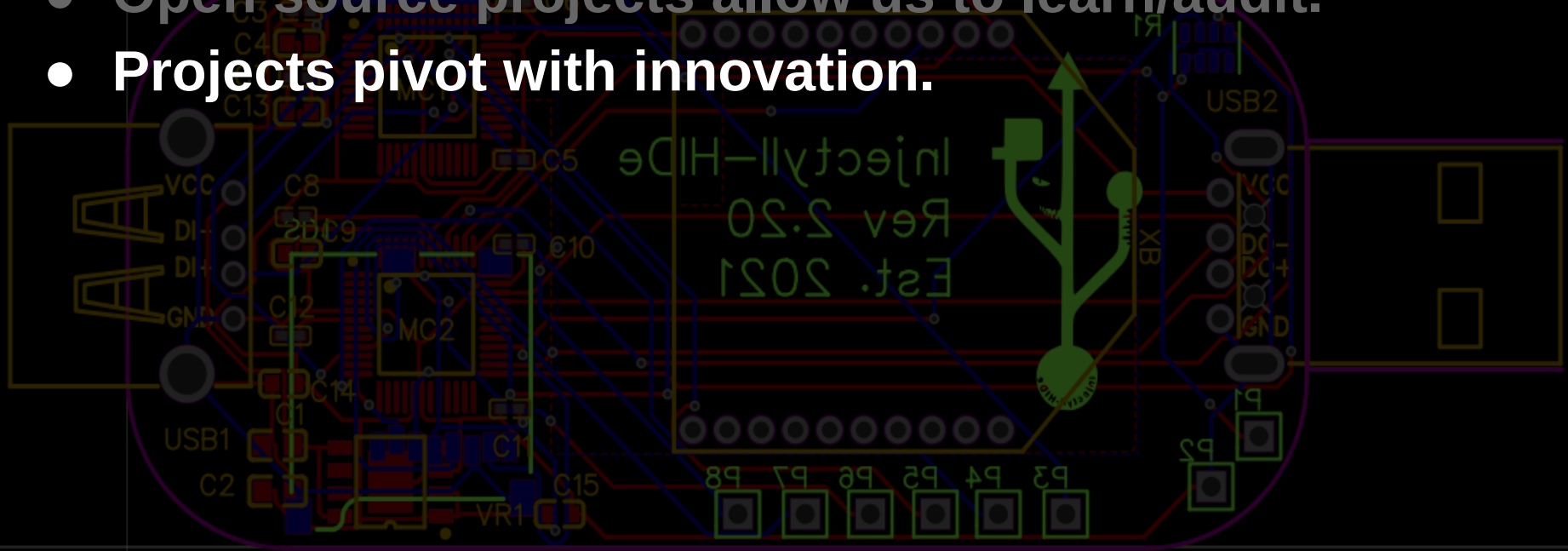
Open Source

- **Open source projects allow us to learn/audit.**



Open Source

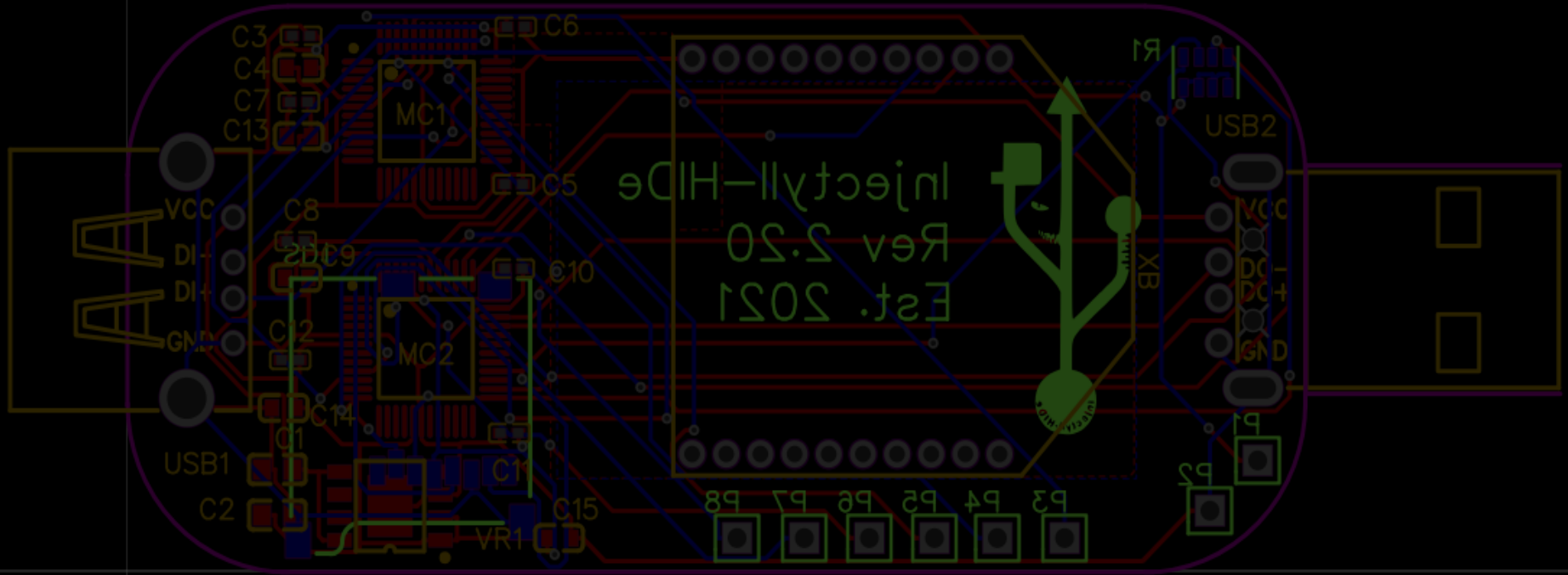
- Open source projects allow us to learn/audit.
- **Projects pivot with innovation.**



Open Source

- Open source projects allow us to learn/audit.
- Projects pivot with innovation.
- **Support is based on the community.**

Why create our own?



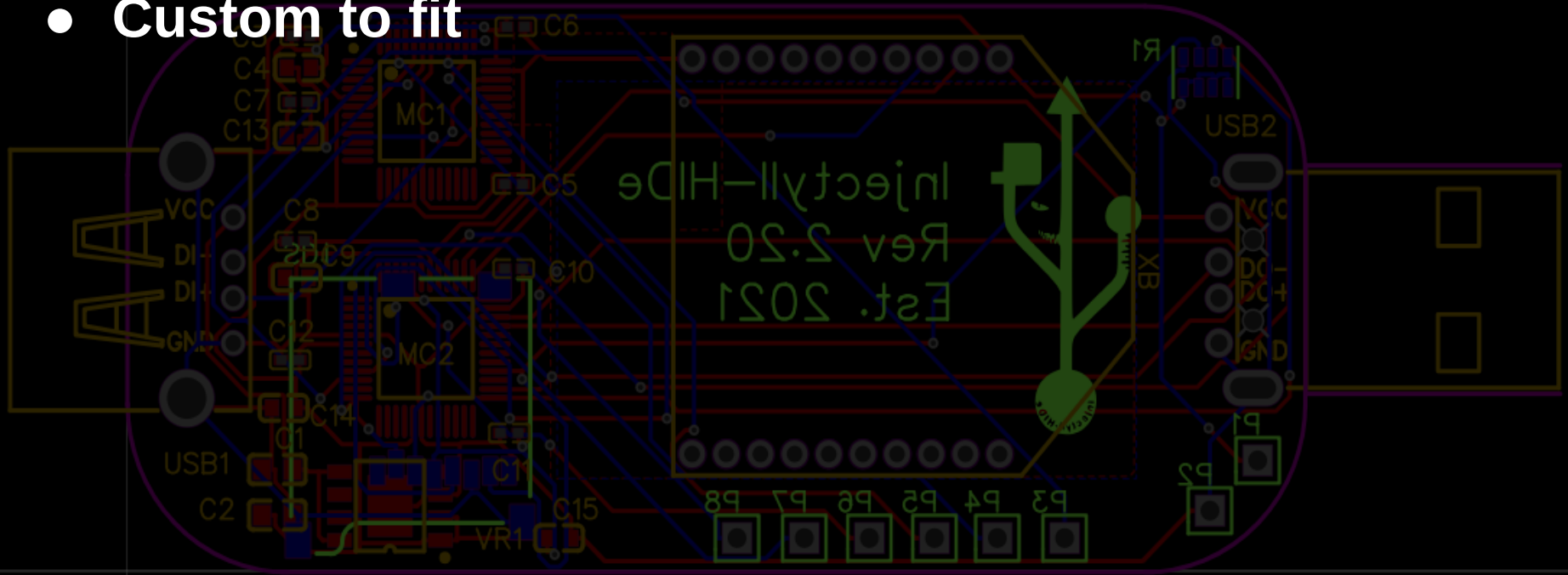
@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

Why create our own?

- **Custom to fit**

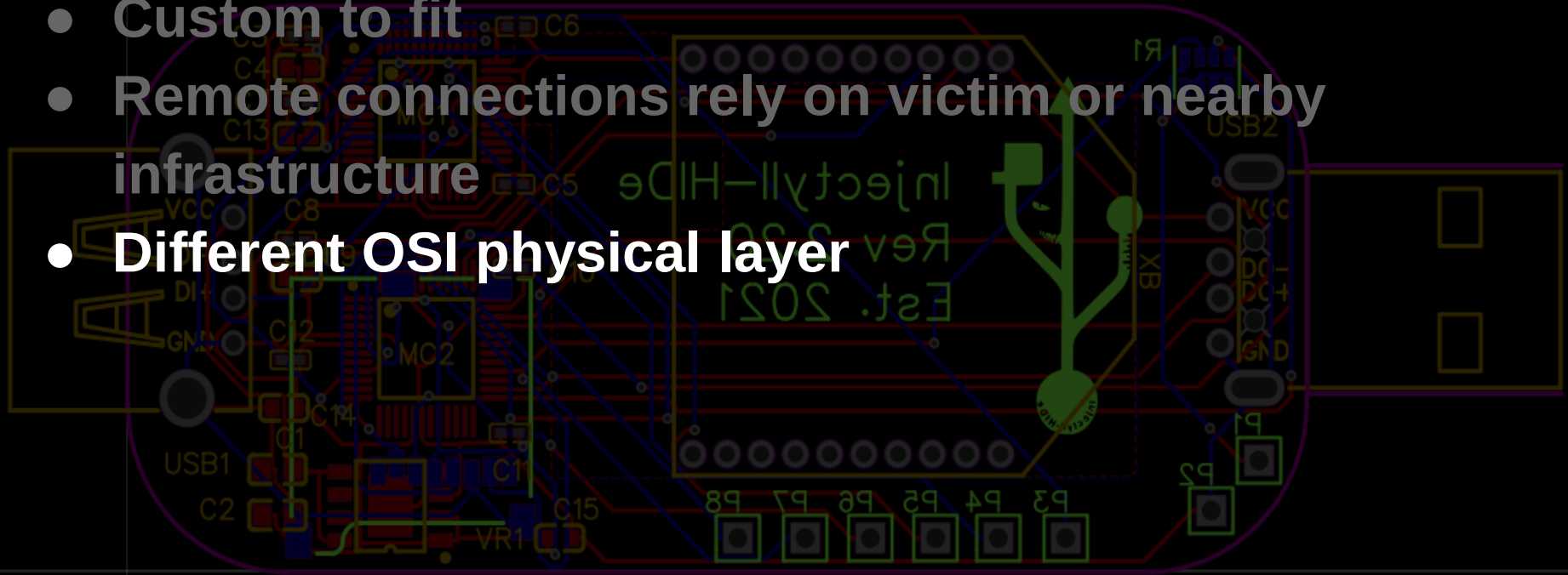


Why create our own?

- Custom to fit
- **Remote connections rely on victim or nearby infrastructure**

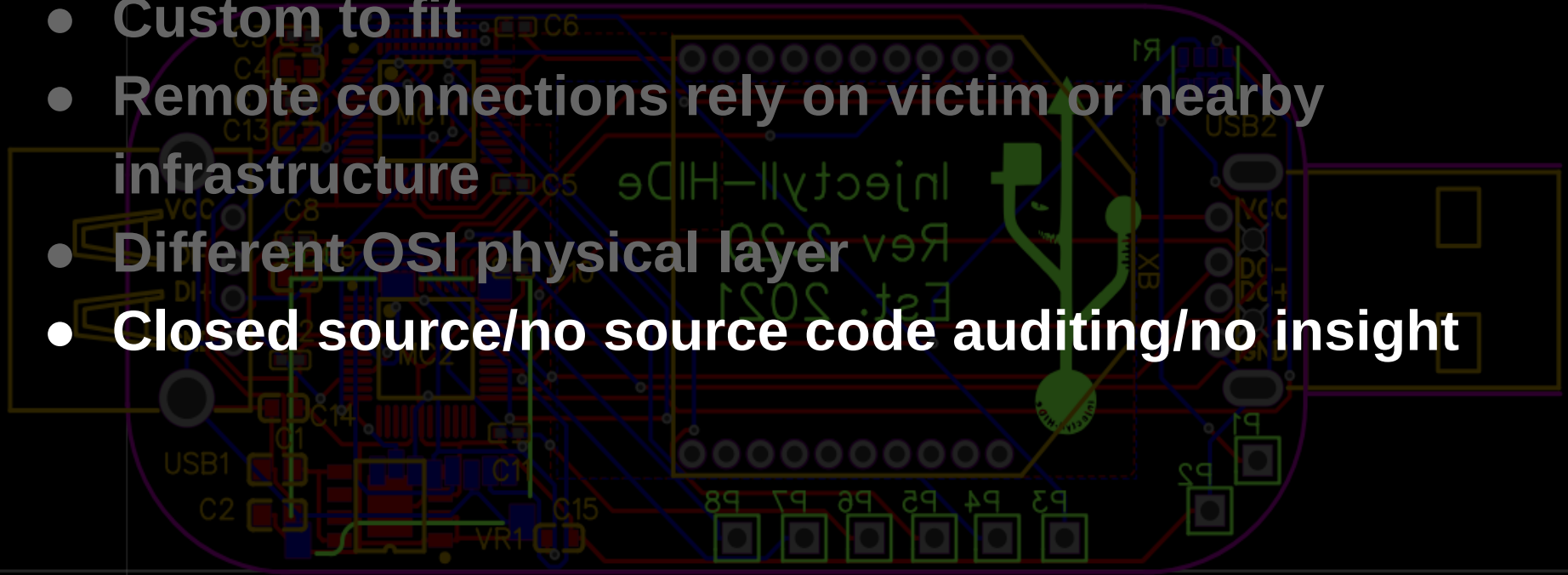
Why create our own?

- Custom to fit
- Remote connections rely on victim or nearby infrastructure
- **Different OSI physical layer**



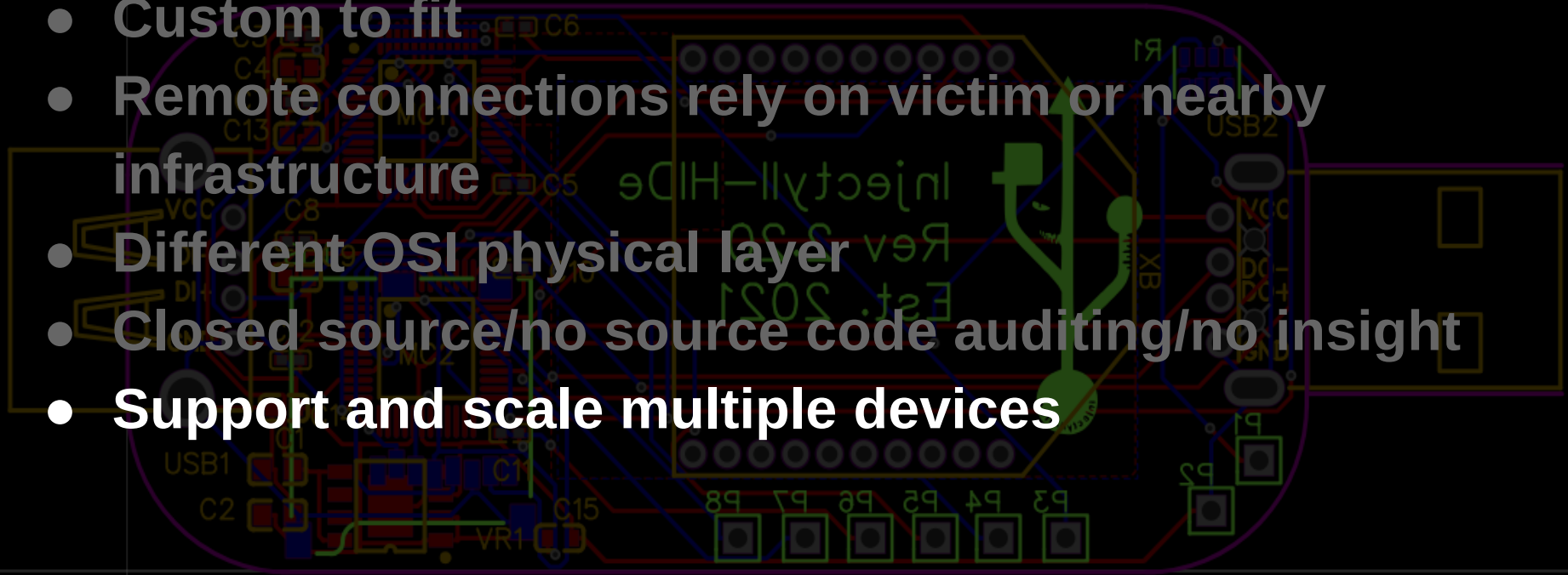
Why create our own?

- Custom to fit
- Remote connections rely on victim or nearby infrastructure
- Different OSI physical layer
- **Closed source/no source code auditing/no insight**

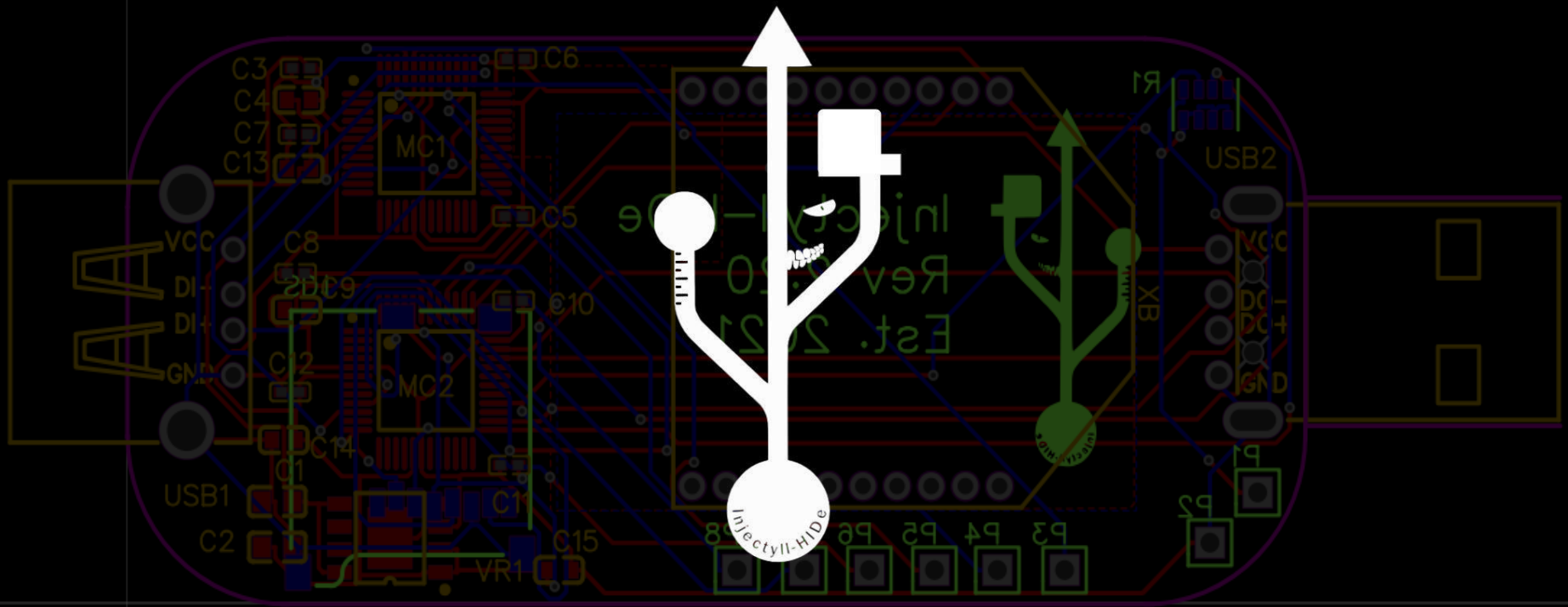


Why create our own?

- Custom to fit
- Remote connections rely on victim or nearby infrastructure
- Different OSI physical layer
- Closed source/no source code auditing/no insight
- **Support and scale multiple devices**

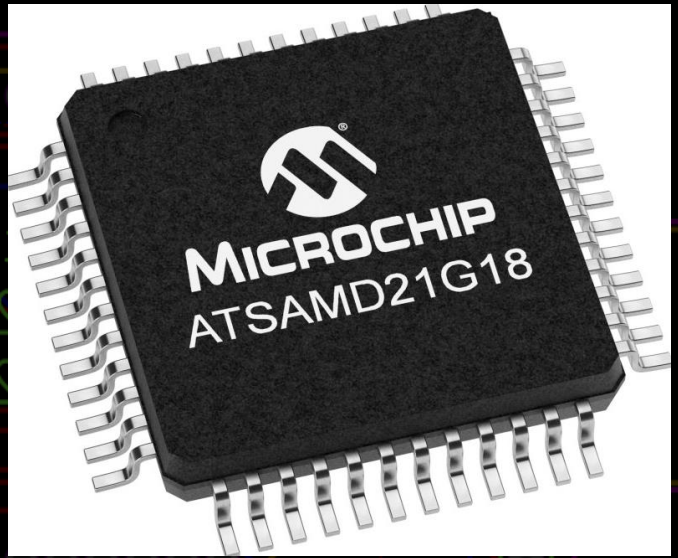


Enter Injectyll-HIDe



The Hardware

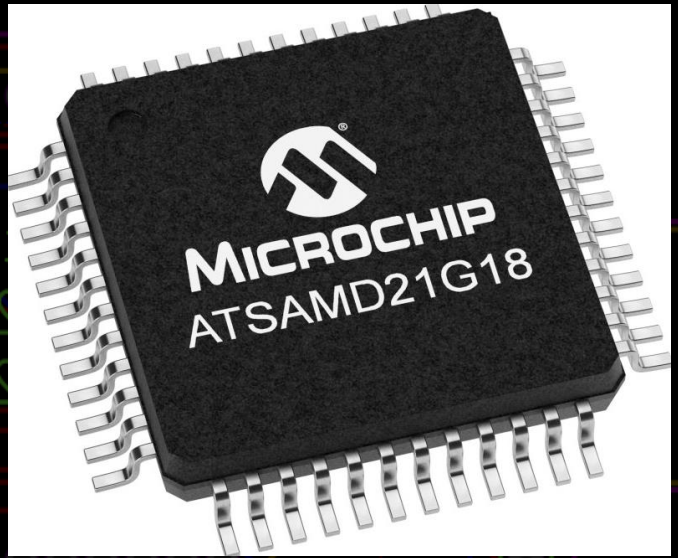
SAMD21G18
MicroController



The Hardware

SAMD21G18 MicroController

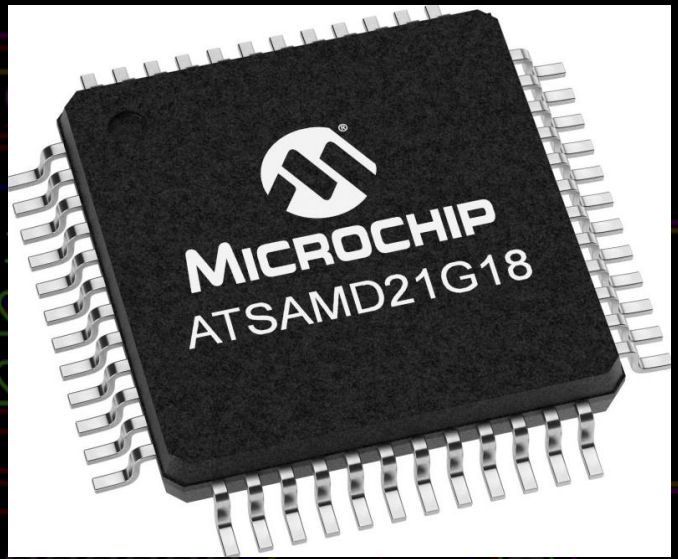
- 2 on the implant to act as the Client and Host.



The Hardware

SAMD21G18 MicroController

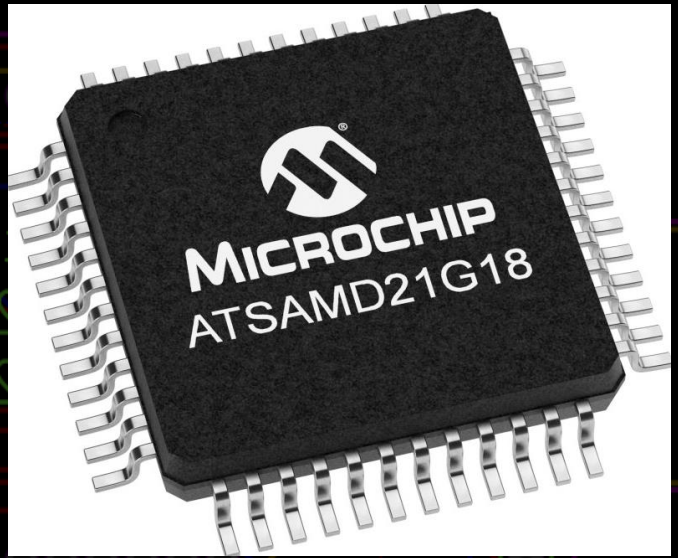
- 2 on the implant to act as the Client and Host.
- Easy to develop on. (Lots of documentation)



The Hardware

SAMD21G18 MicroController

- 2 on the implant to act as the Client and Host.
- Easy to develop on. (Lots of documentation)
- Extra SERCOM space (communicate with radio/storage)



The Hardware

XBee3 Radio

The Hardware

XBee3 Radio

- Allows for mesh RF communication

The Hardware

XBee3 Radio

- Allows for mesh RF communication
- Range increased as more devices join network.

The Hardware

XBee3 Radio

- Allows for mesh RF communication
- Range increased as more devices join network.
- Control and receive data from many devices.

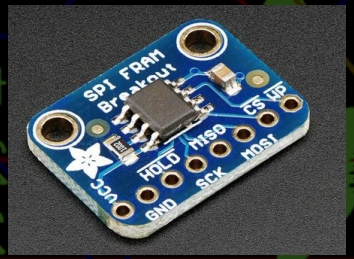
The Hardware

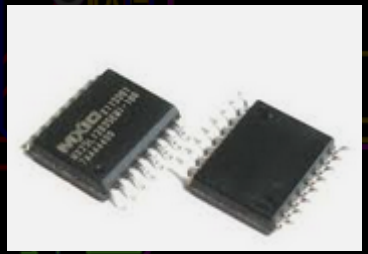
XBee3 Radio

- Allows for mesh RF communication
- Range increased as more devices join network.
- Control and receive data from many devices.
- Authentication and Encryption

The Hardware

Storage

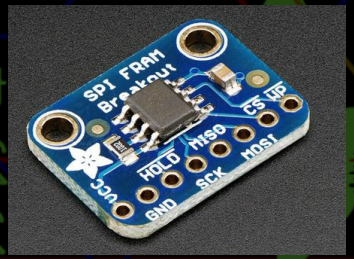


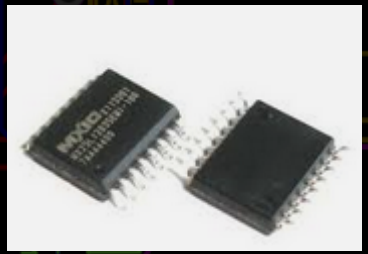


The Hardware

Storage

- Currently using a micro SD card on board.

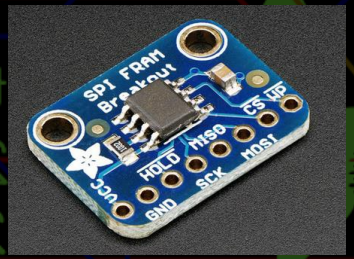


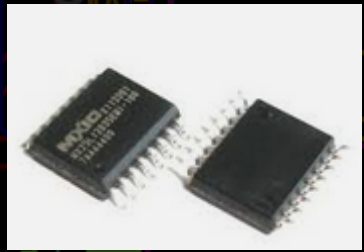


The Hardware

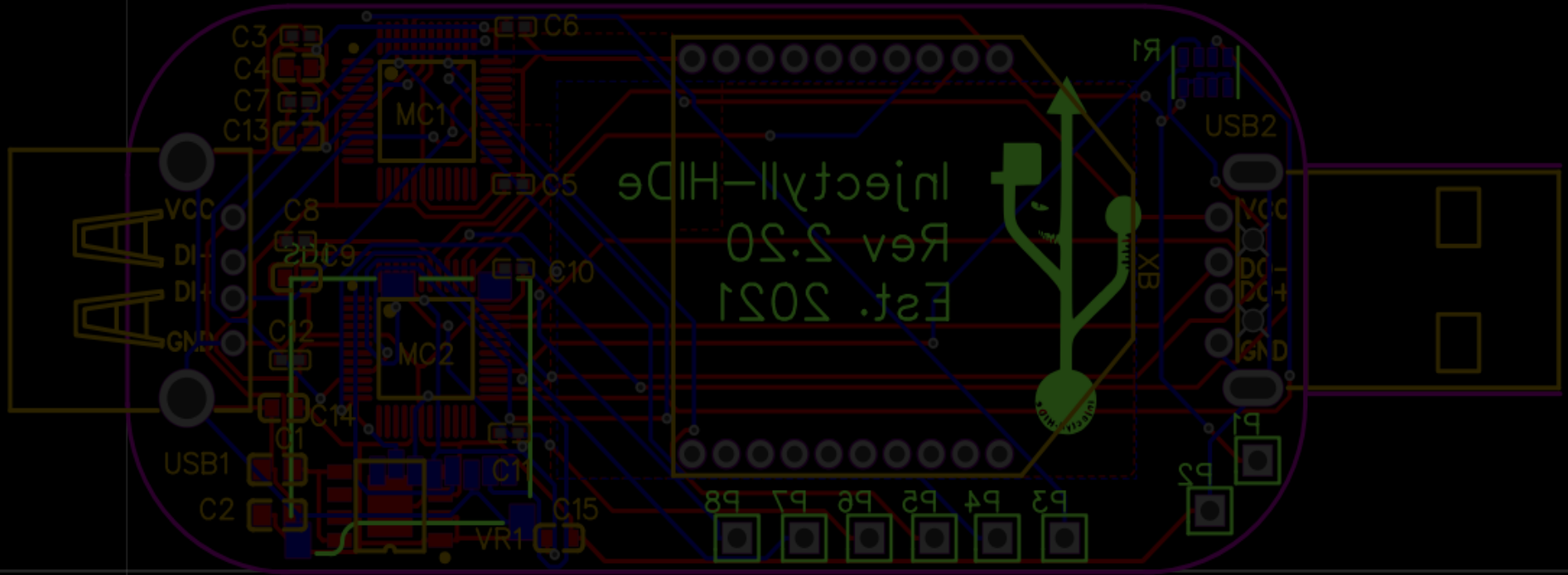
Storage

- Currently using a micro SD card on board.
- Looking to move to NAND for smaller footprint.





Hardware Design Evolution

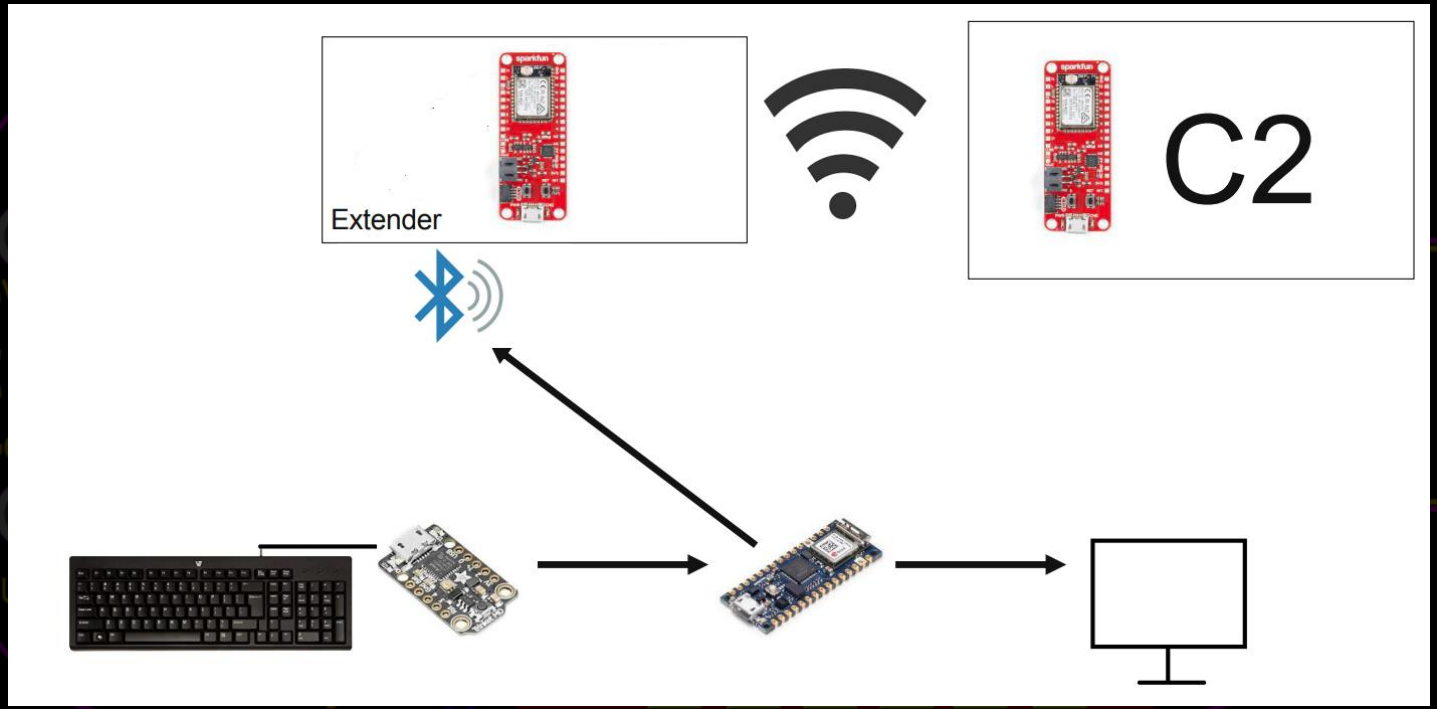


@c4m0ufl4g3

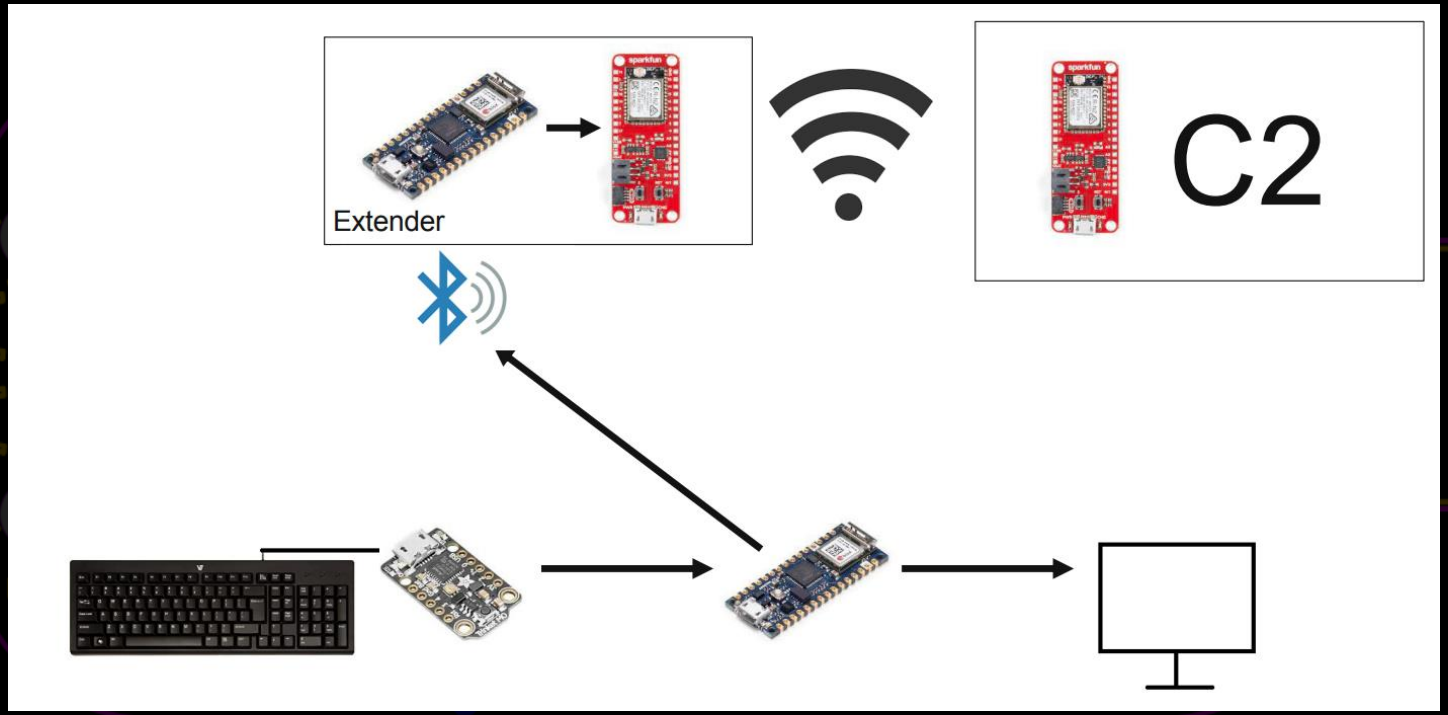
@Injectyll_HIDe

@allTheJurm

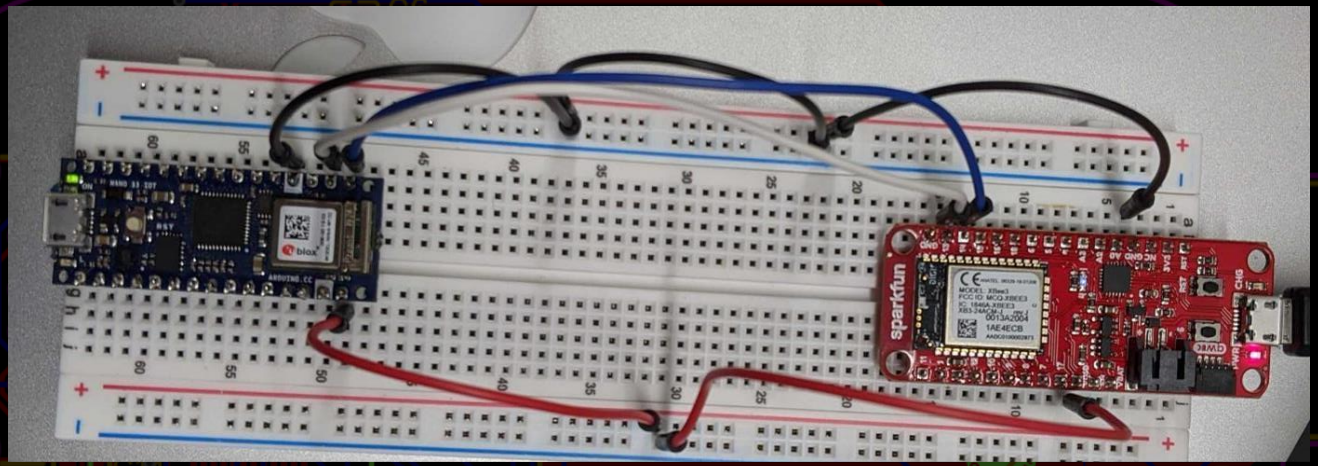
Proof of Concept Layout



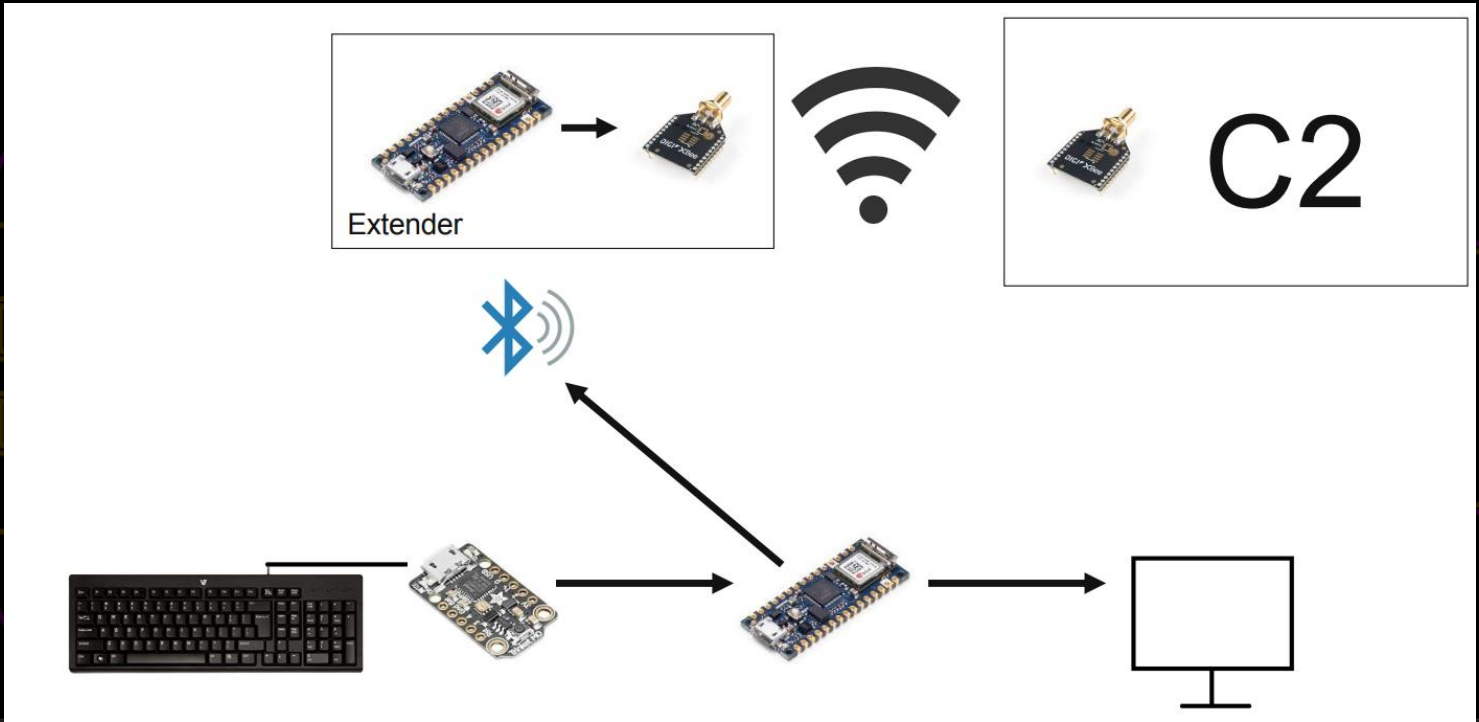
Prototype #1 Layout



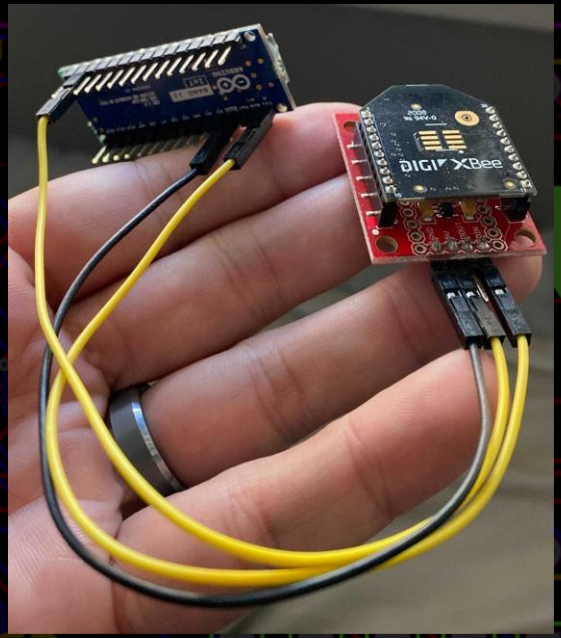
Prototype #1



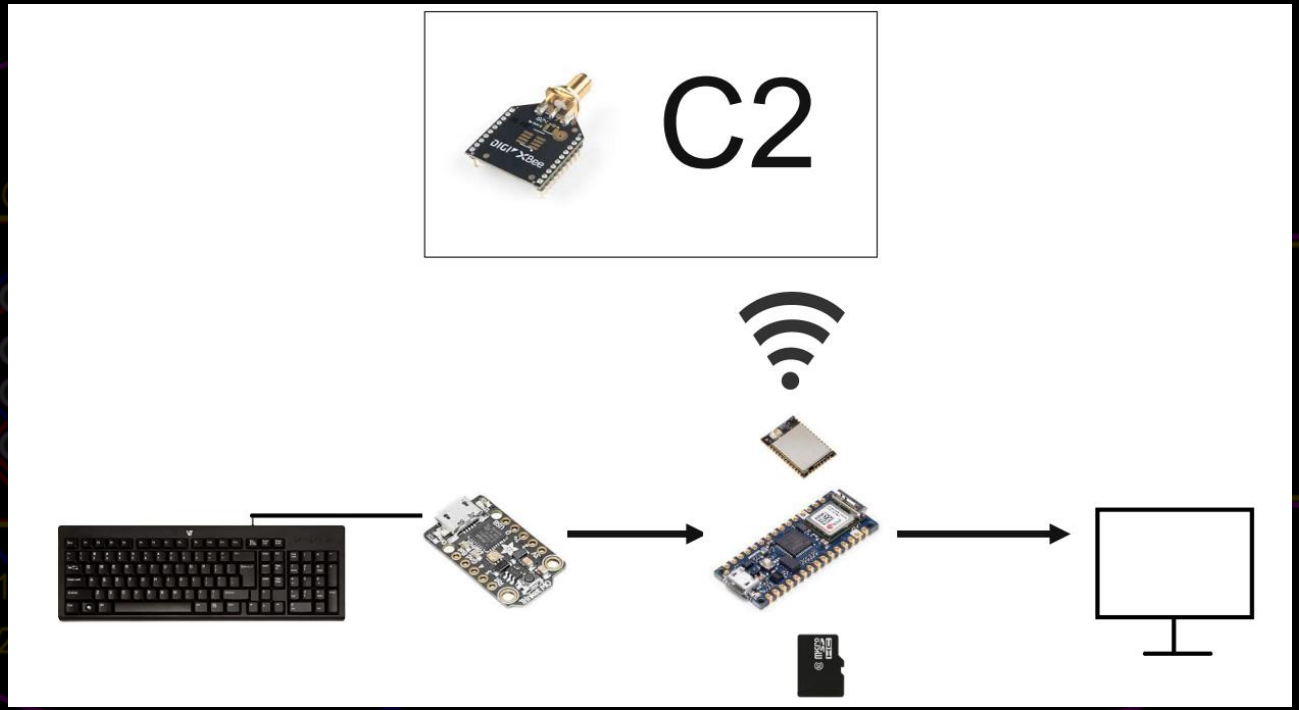
Prototype #2 Layout



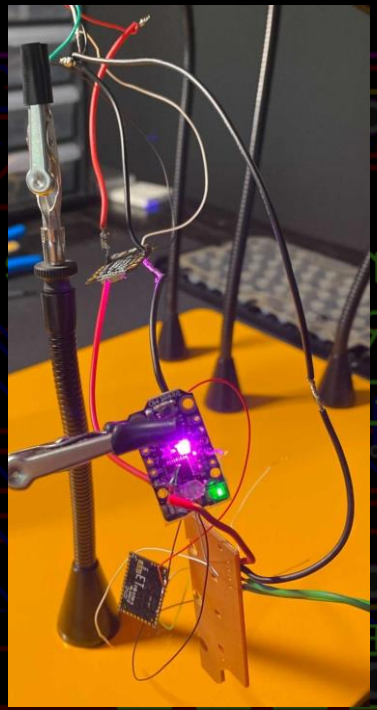
Prototype #2



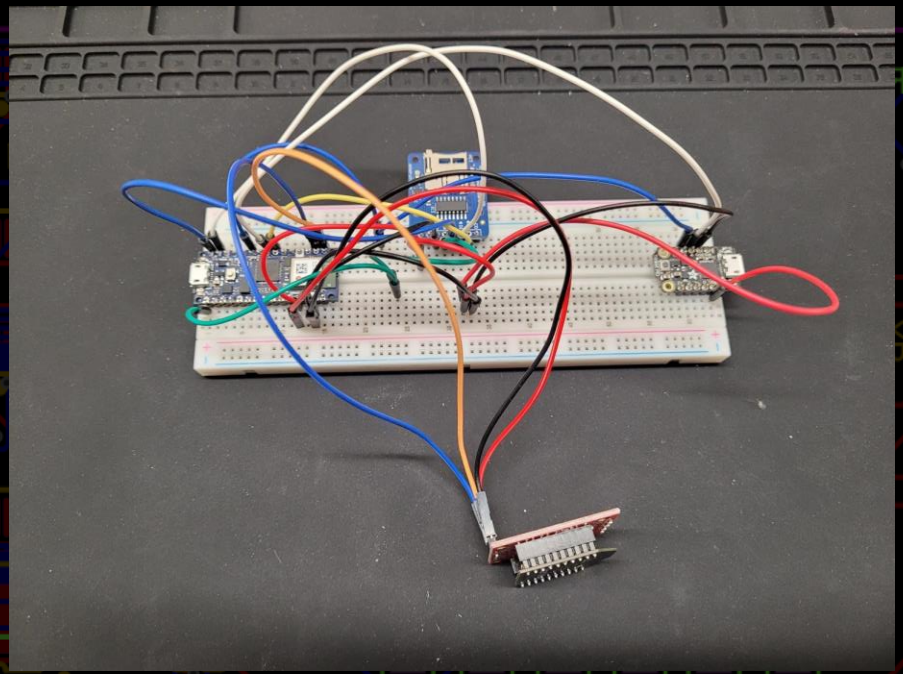
Prototype #3 Layout



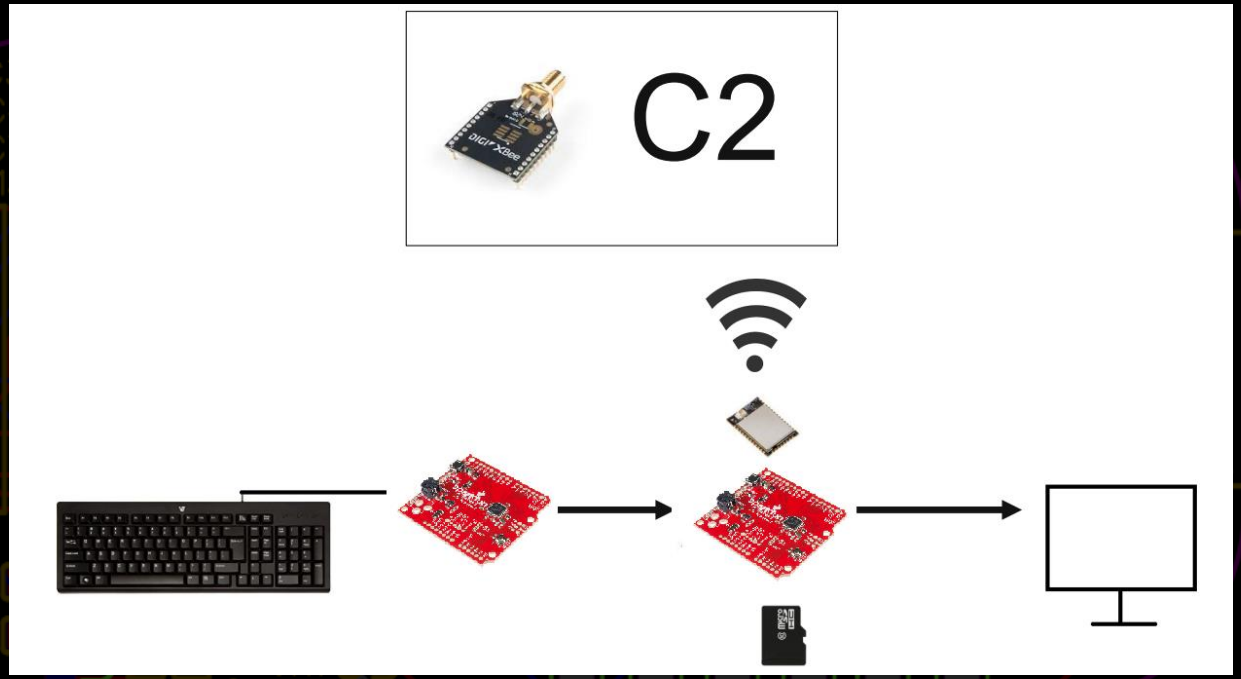
Prototype #3



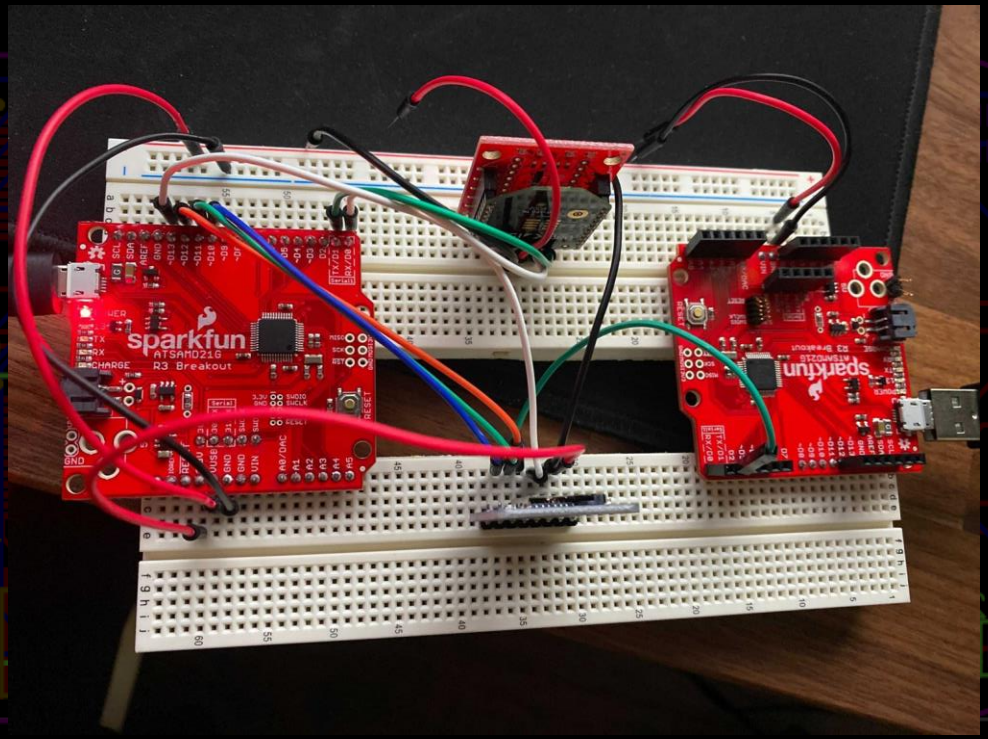
Prototype #3



Prototype #4 Layout



Prototype #4

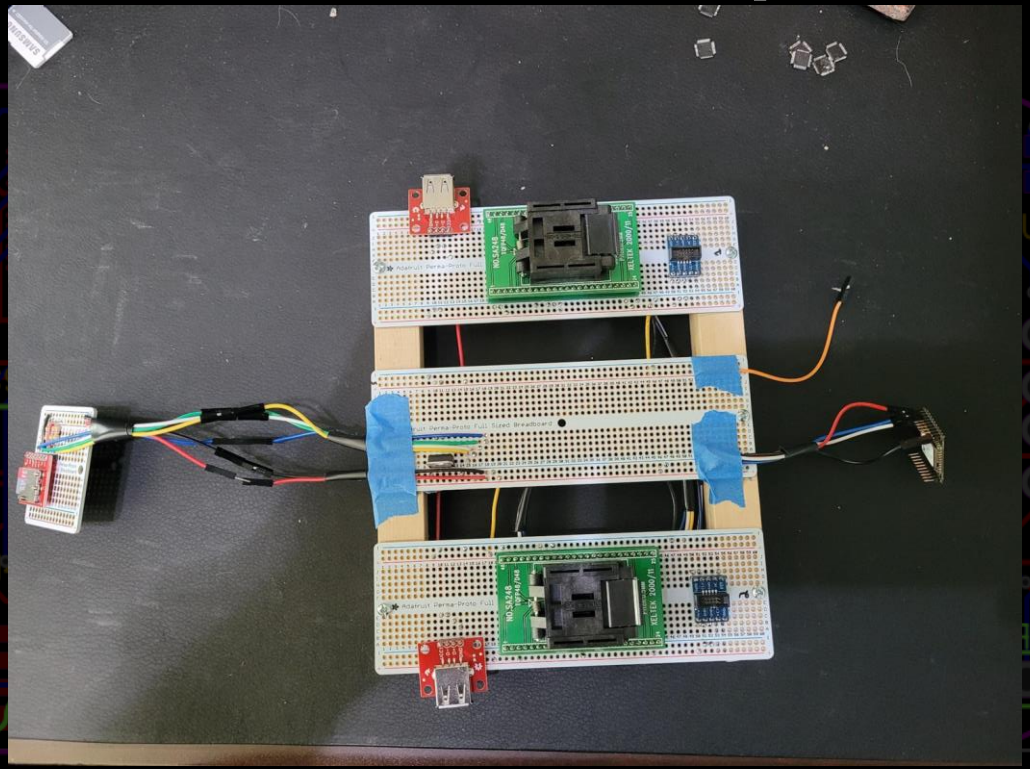


@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

Full Mock Up

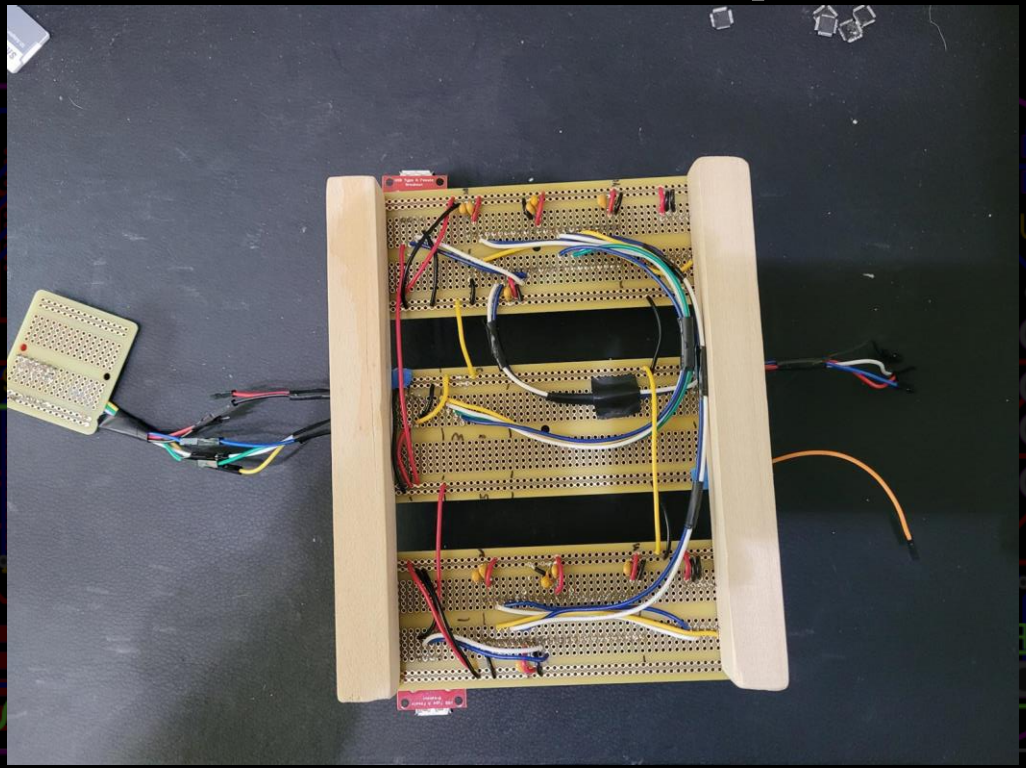


@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

Full Mock Up

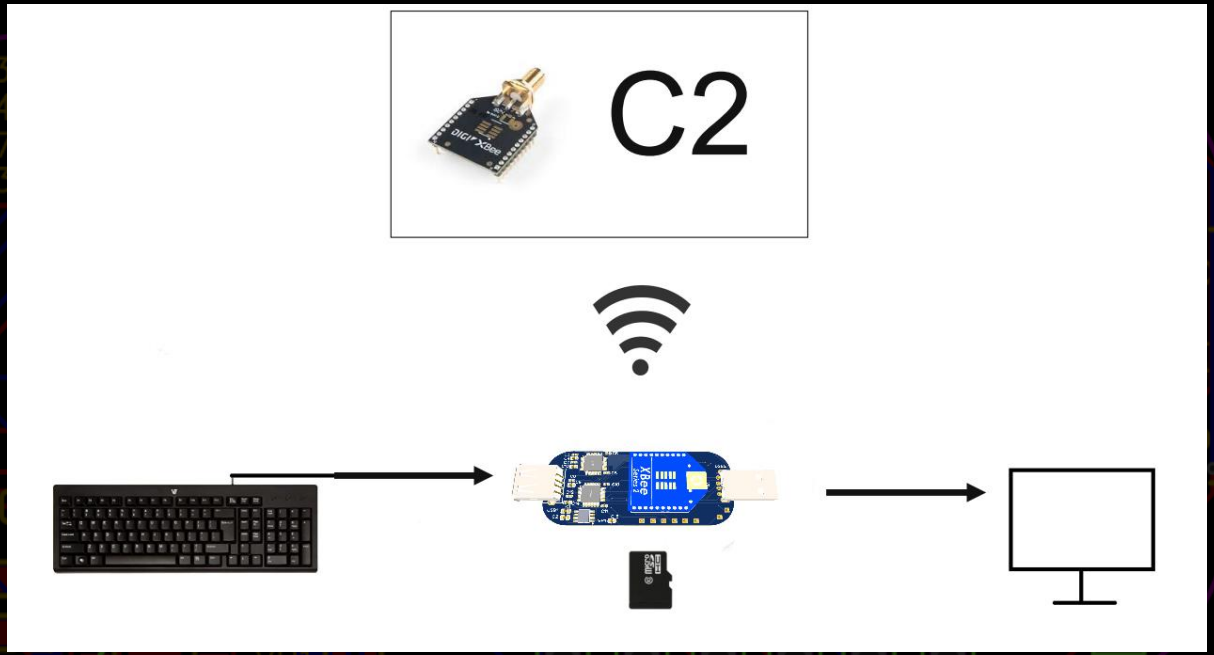


@c4m0ufl4g3

@Injectyll_HIDe

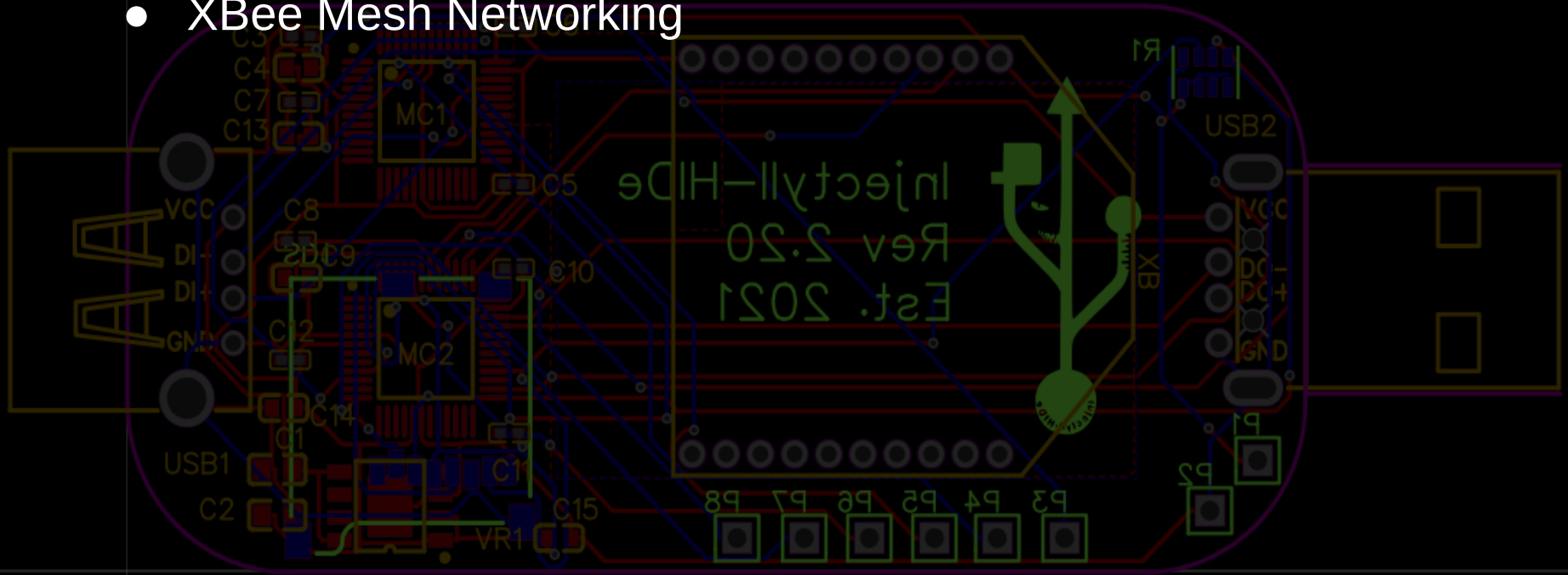
@allTheJurm

PCB Layout



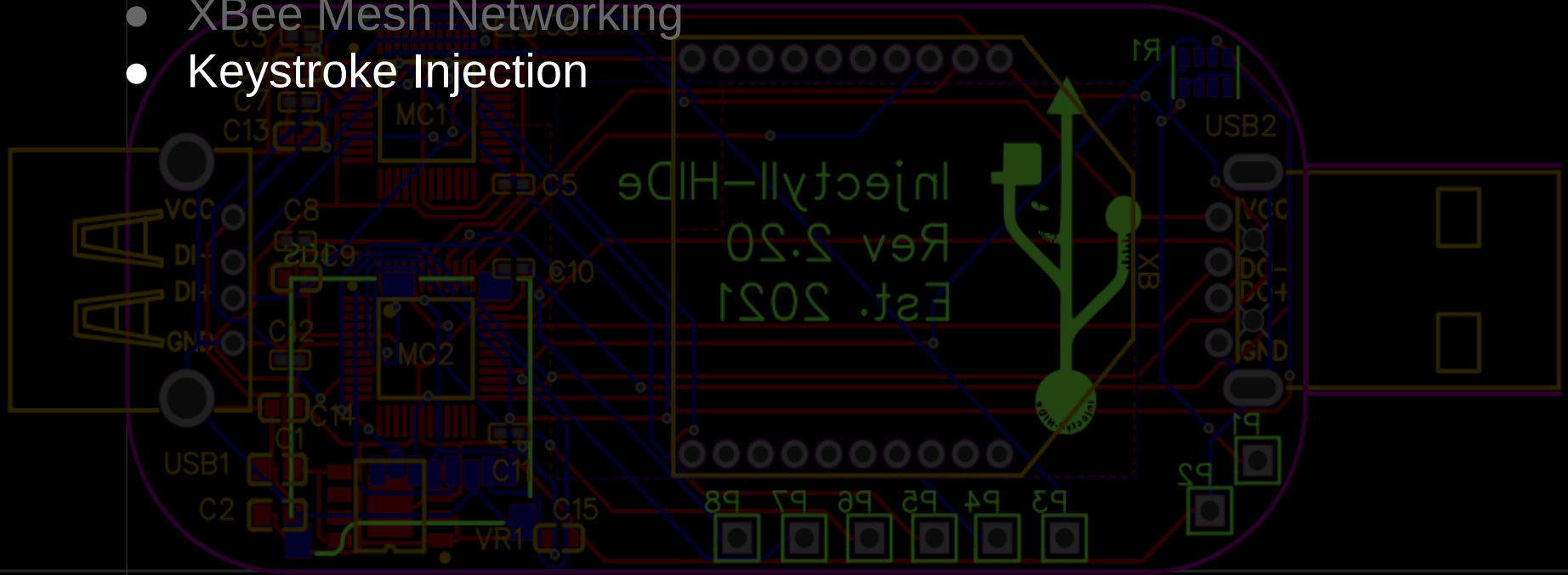
Injectyll-HIDe Features

- XBee Mesh Networking



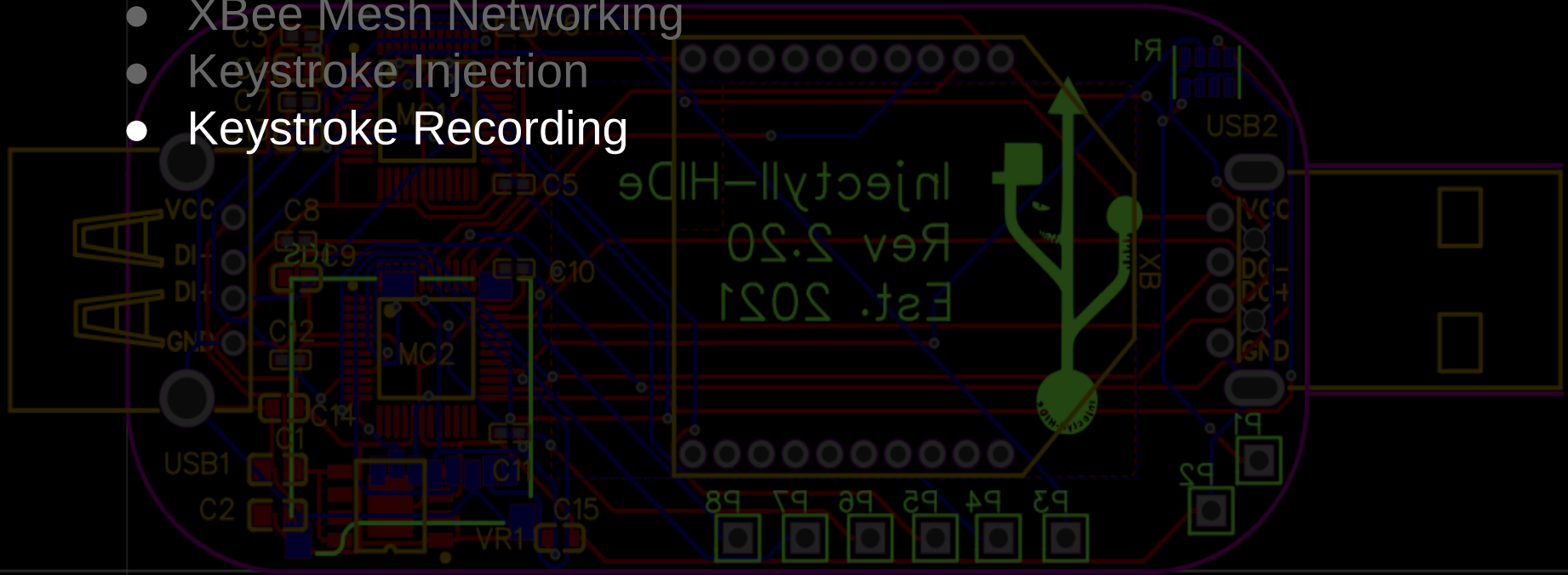
Injectyll-HIDe Features

- XBee Mesh Networking
- Keystroke Injection



Injectyll-HIDe Features

- XBee Mesh Networking
- Keystroke Injection
- Keystroke Recording

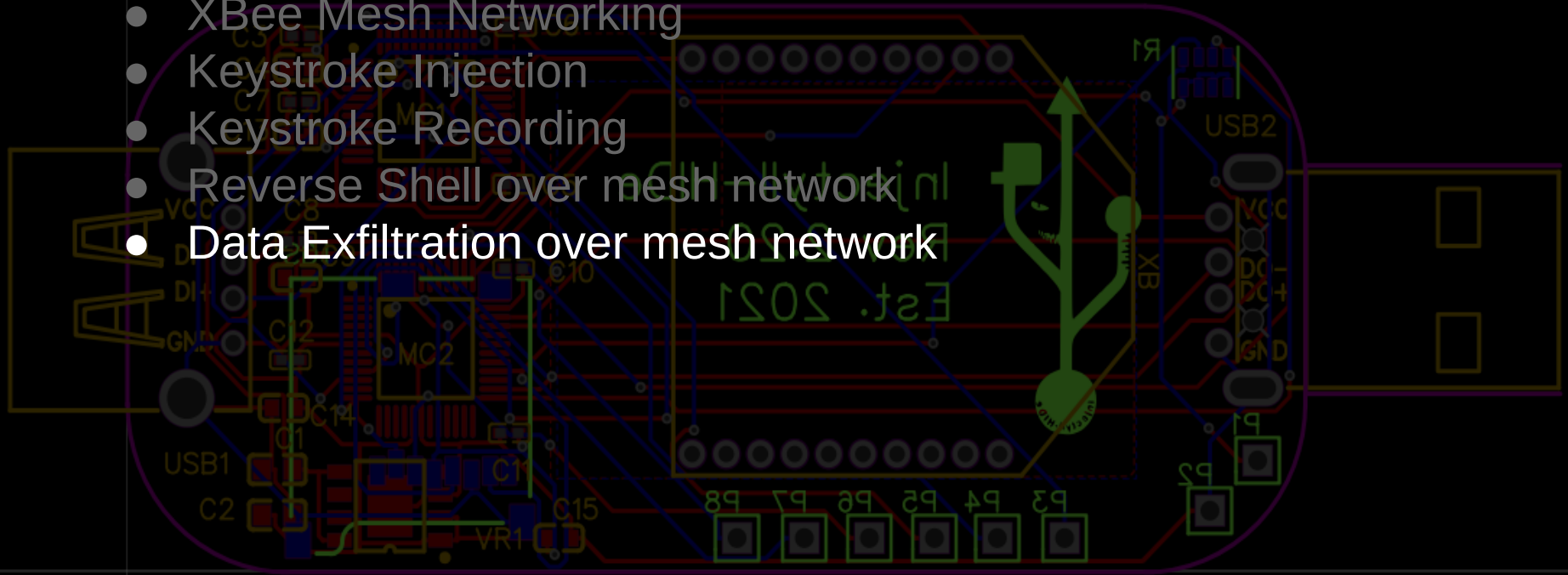


Injectyll-HIDe Features

- XBee Mesh Networking
- Keystroke Injection
- Keystroke Recording
- Reverse Shell over mesh network

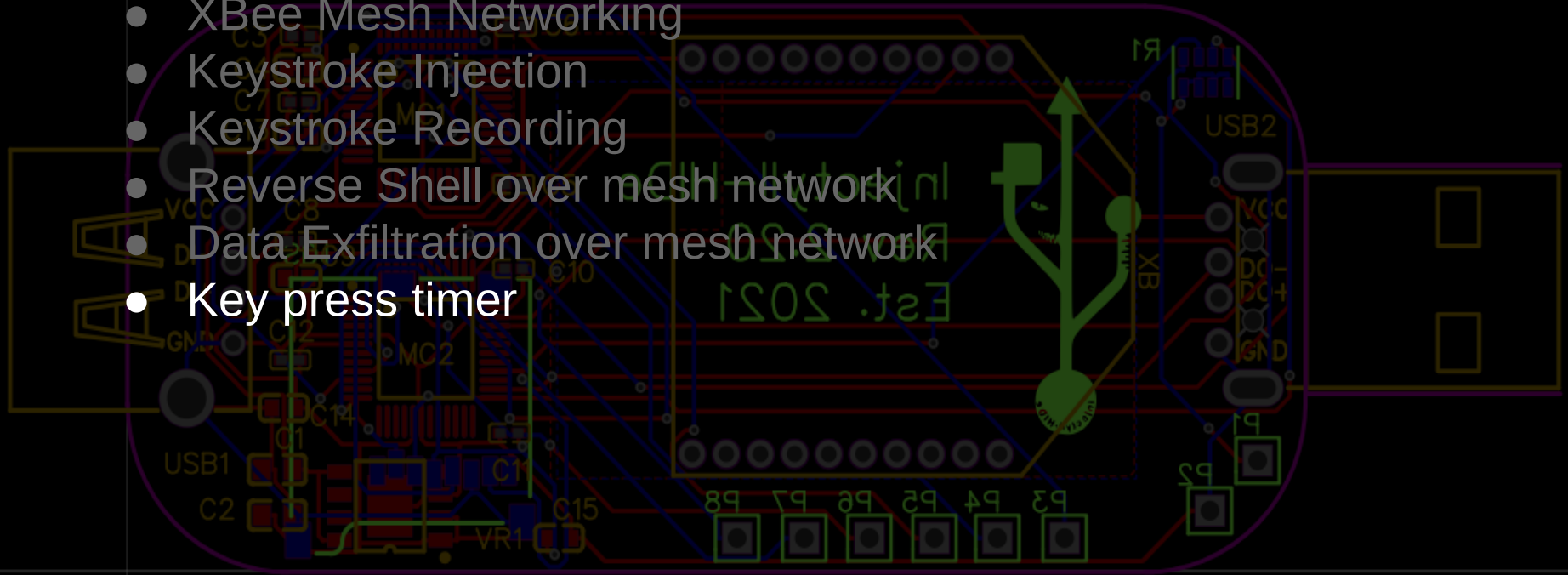
Injectyll-HIDe Features

- XBee Mesh Networking
- Keystroke Injection
- Keystroke Recording
- Reverse Shell over mesh network
- Data Exfiltration over mesh network



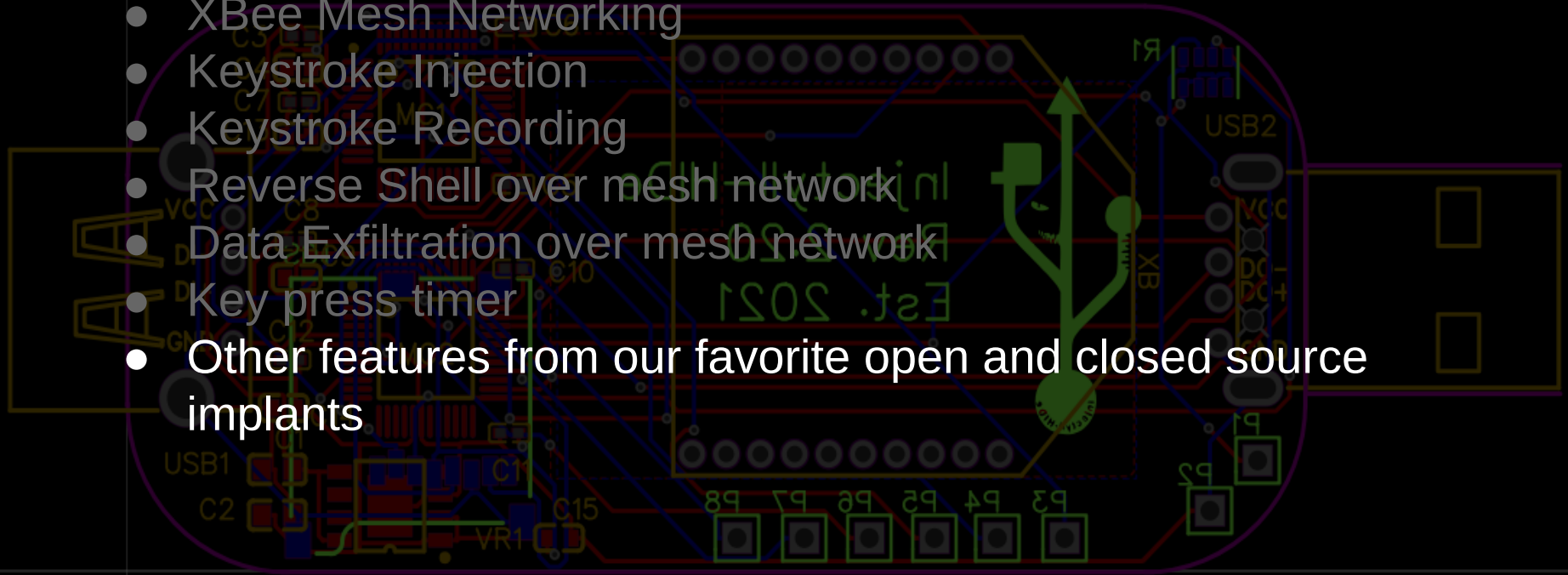
Injectyll-HIDe Features

- XBee Mesh Networking
- Keystroke Injection
- Keystroke Recording
- Reverse Shell over mesh network
- Data Exfiltration over mesh network
- Key press timer



Injectyll-HIDe Features

- XBee Mesh Networking
- Keystroke Injection
- Keystroke Recording
- Reverse Shell over mesh network
- Data Exfiltration over mesh network
- Key press timer
- Other features from our favorite open and closed source implants



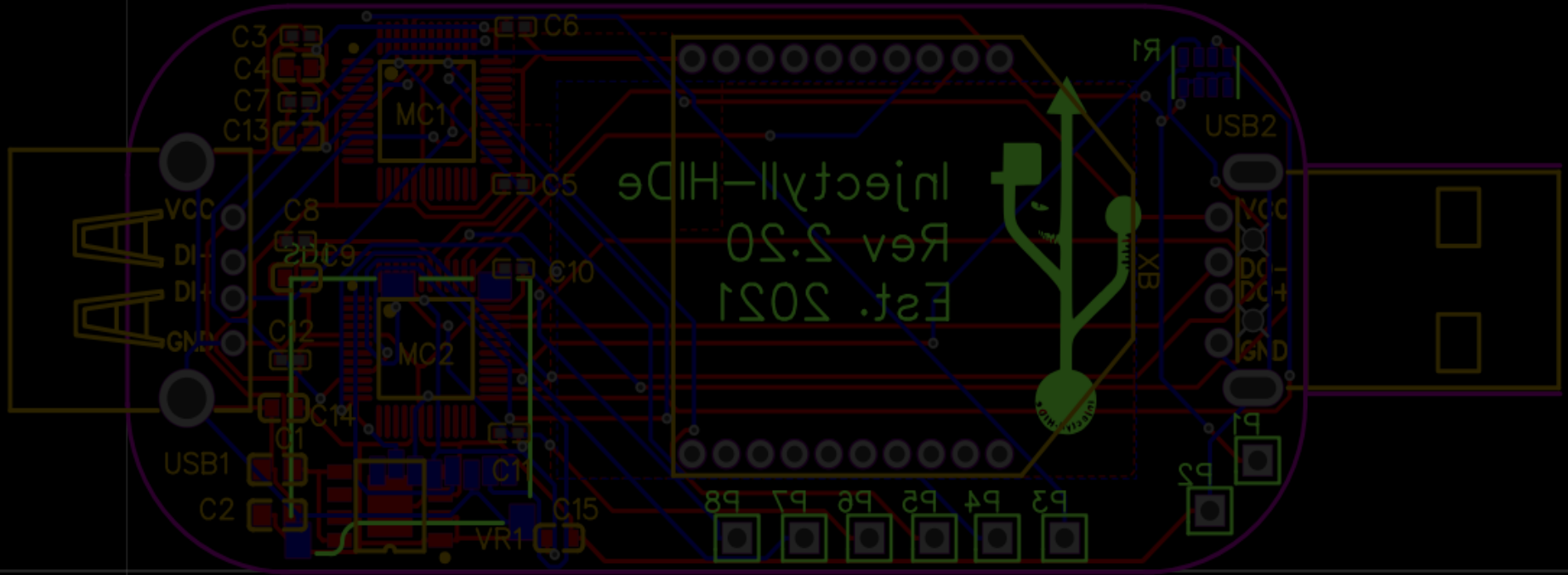
Custom C2

@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

Demo 1



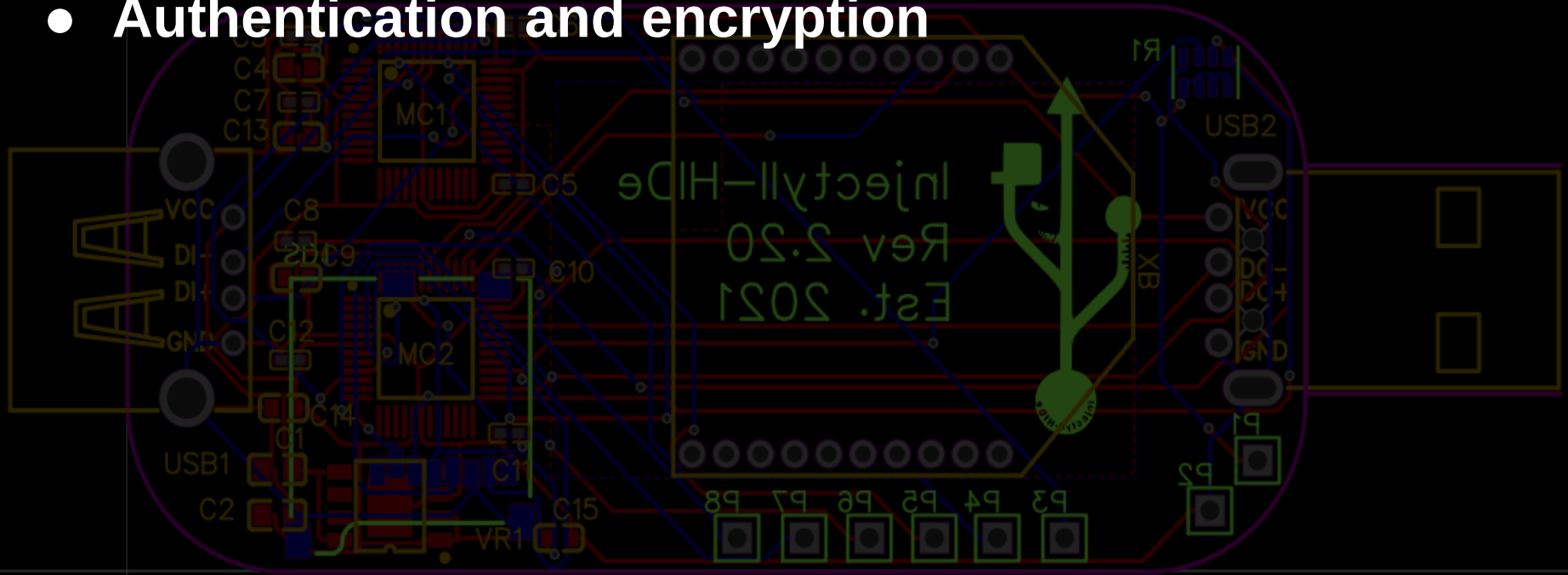
@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

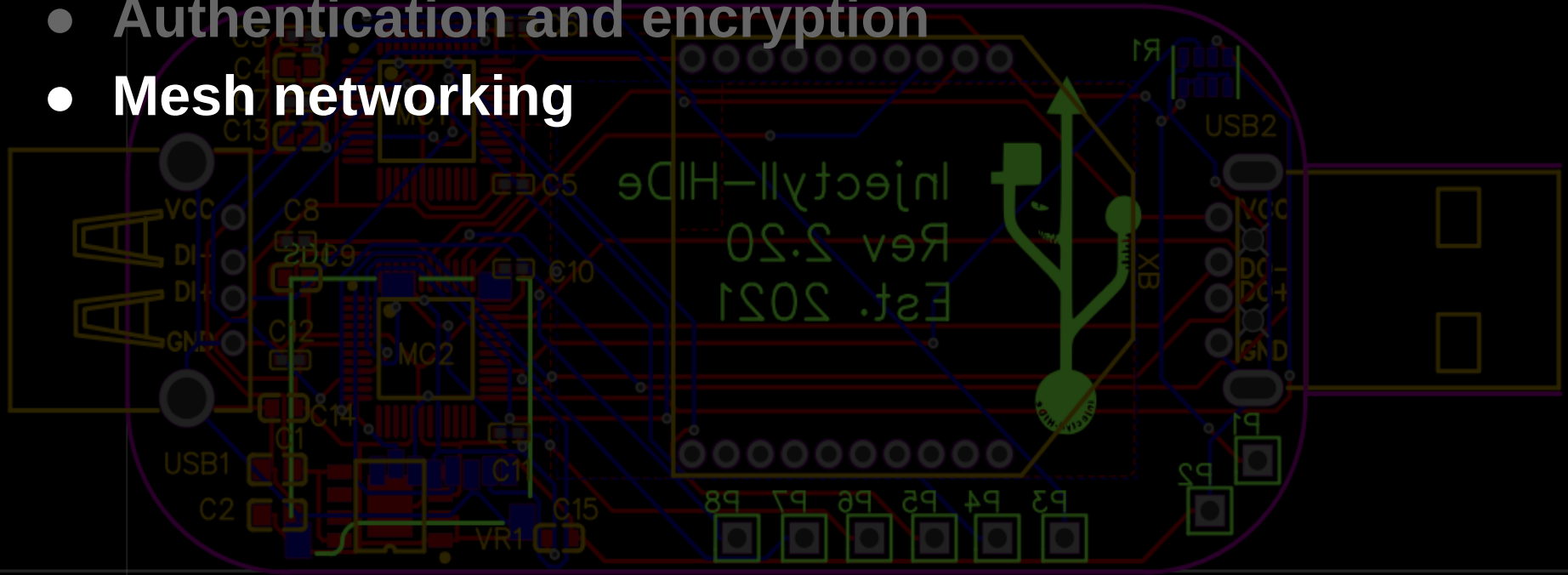
Covert, scalable network

- **Authentication and encryption**



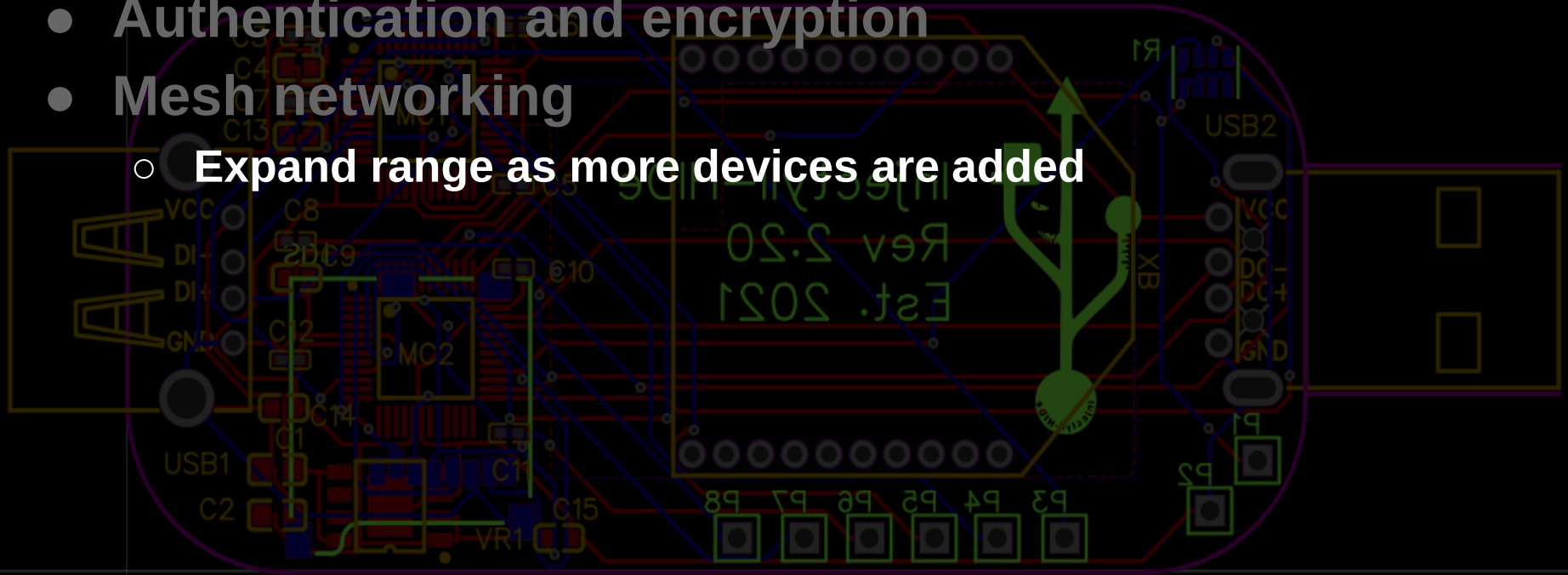
Covert, scalable network

- Authentication and encryption
- **Mesh networking**



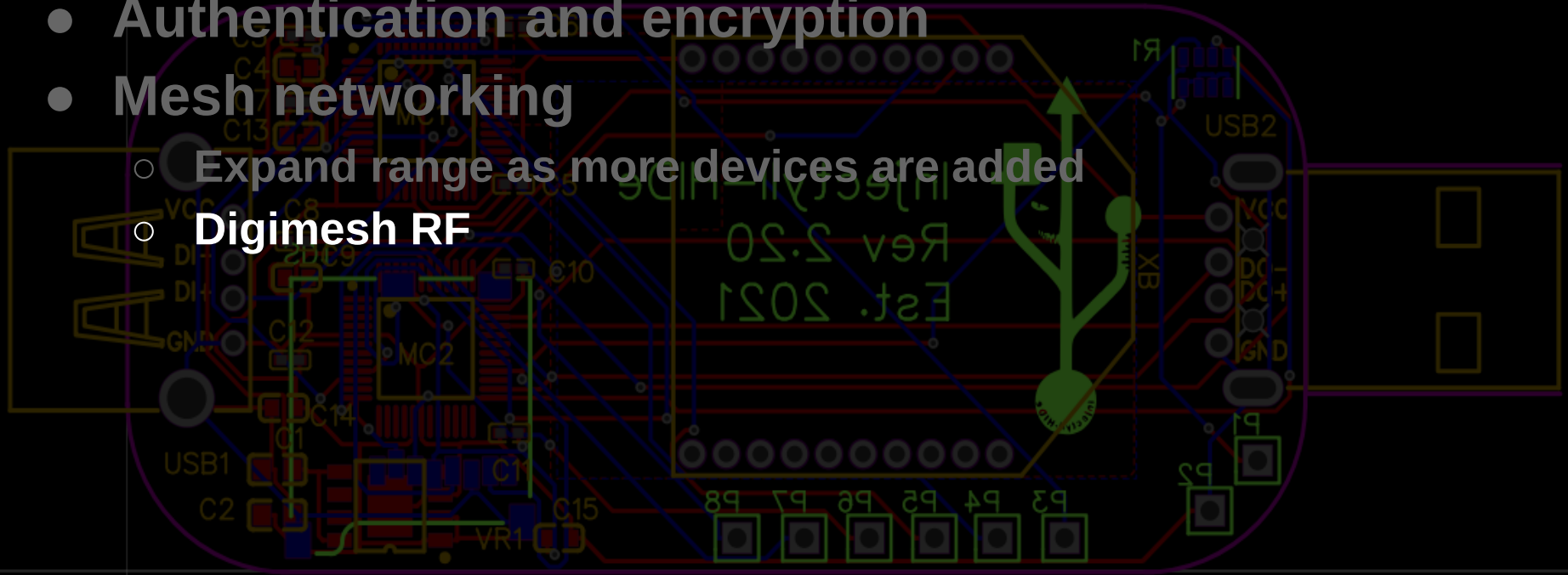
Covert, scalable network

- Authentication and encryption
- Mesh networking
  - **Expand range as more devices are added**



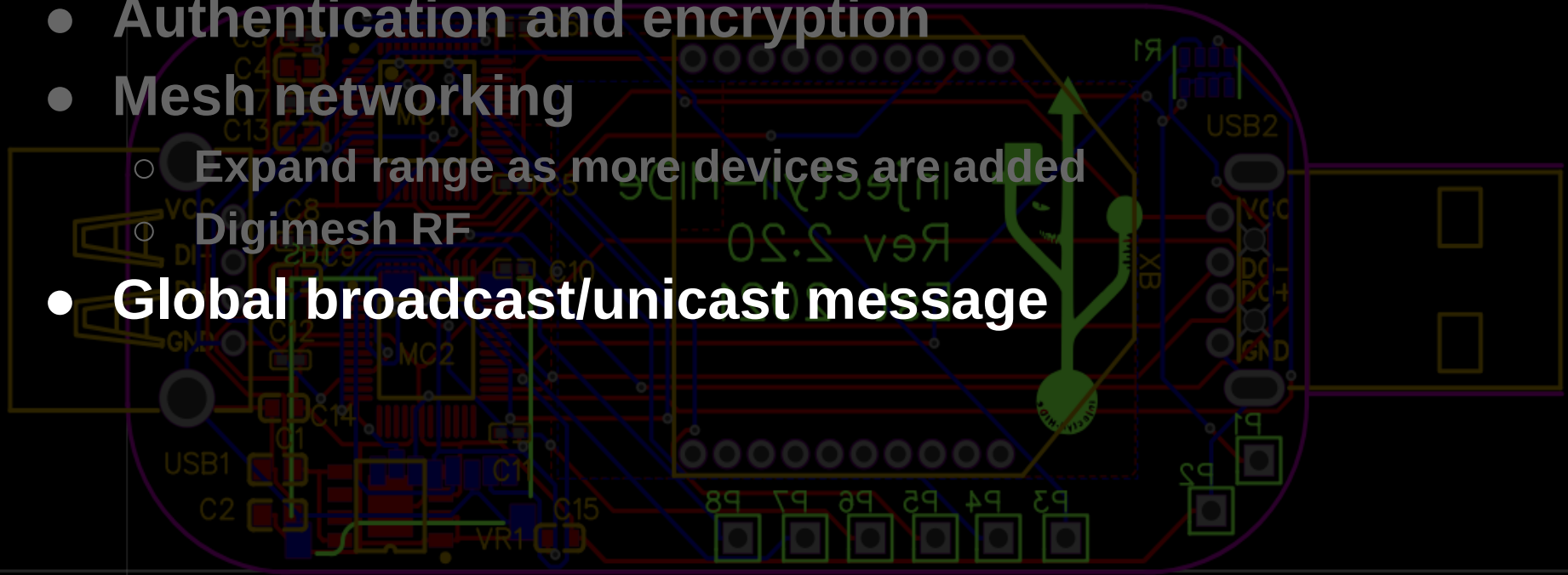
Covert, scalable network

- Authentication and encryption
- Mesh networking
  - Expand range as more devices are added
  - **Digimesh RF**



Covert, scalable network

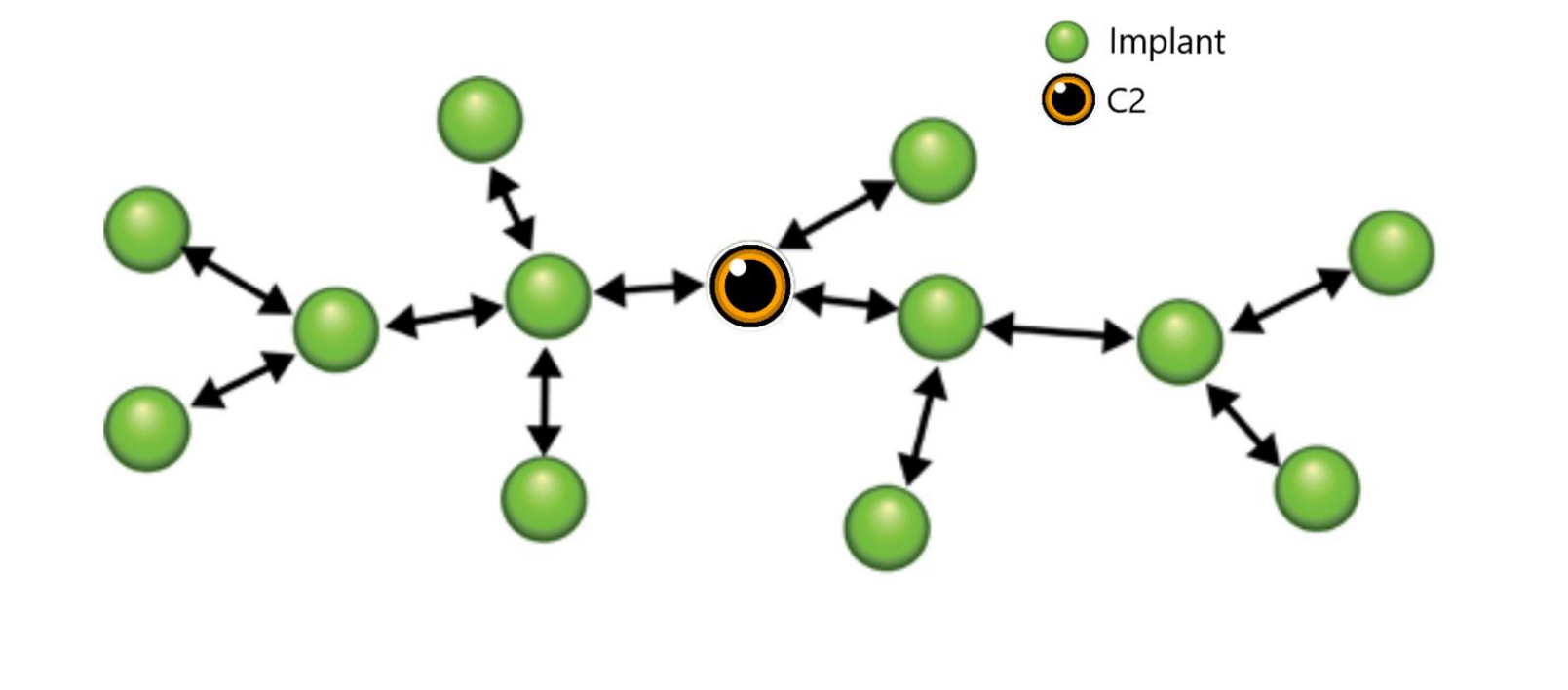
- Authentication and encryption
- Mesh networking
  - Expand range as more devices are added
  - Digimesh RF
- **Global broadcast/unicast message**



Covert, scalable network

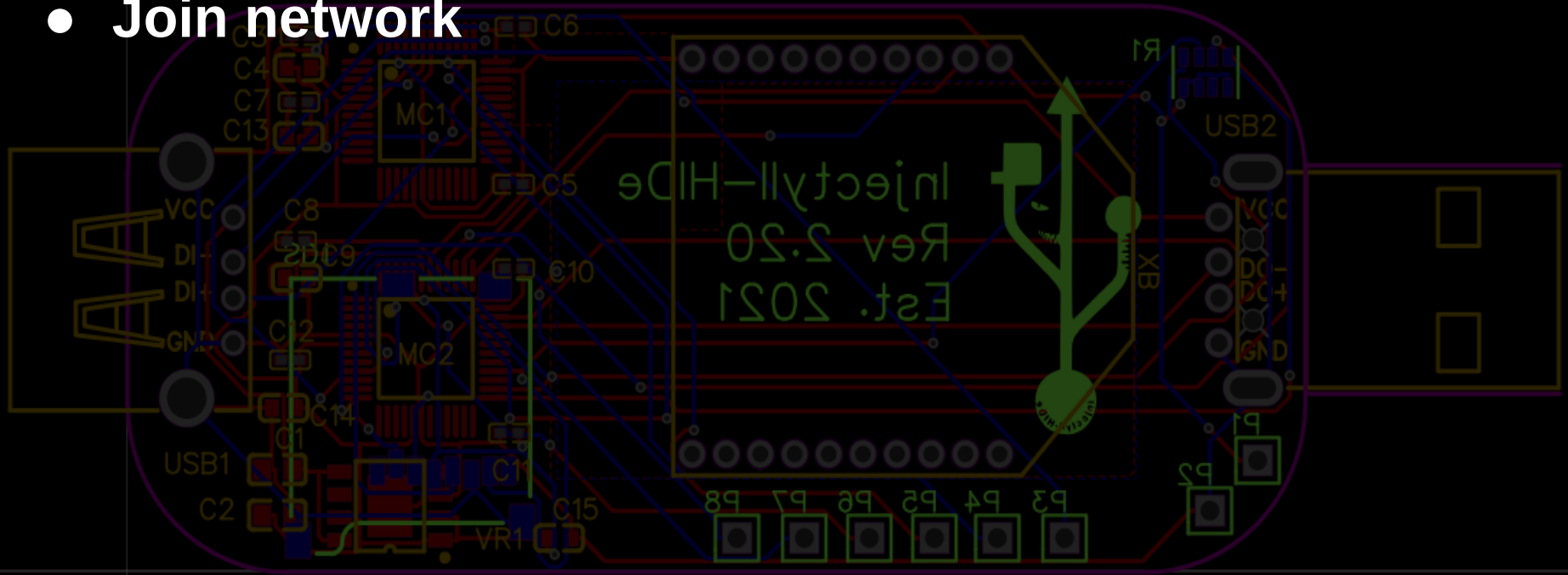
- Authentication and encryption
- Mesh networking
  - Expand range as more devices are added
  - Digimesh RF
- Global broadcast/unicast message
- **Range up to:**
  - **200 - 4,000 ft. (Std version)**
  - **300 ft - 2 mi (Pro version)**

Covert, scalable network



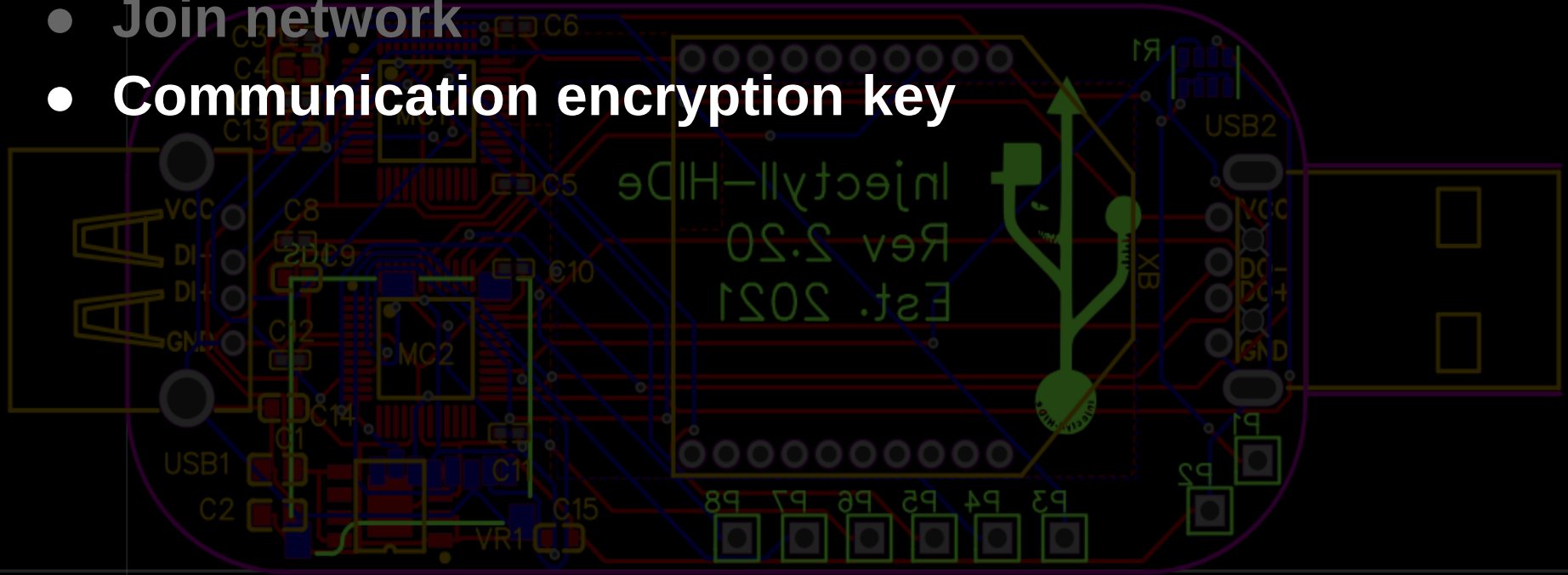
Communication interlocks

- **Join network**



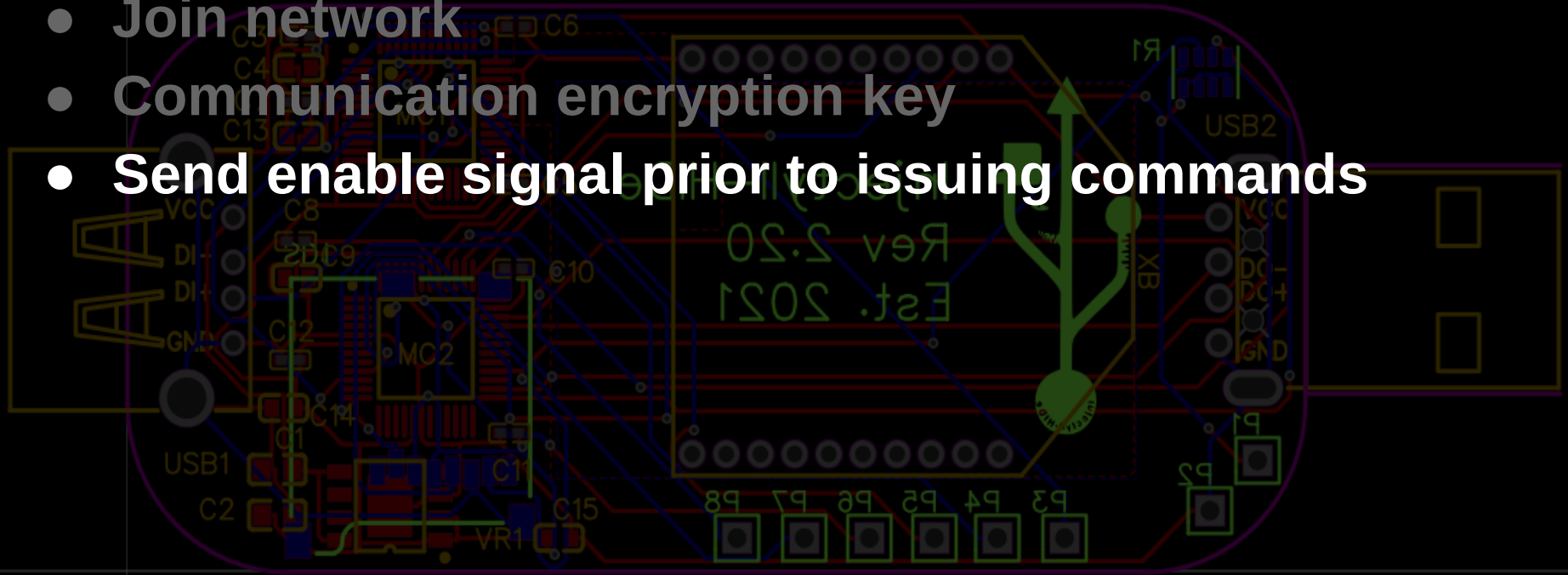
Communication interlocks

- Join network
- **Communication encryption key**



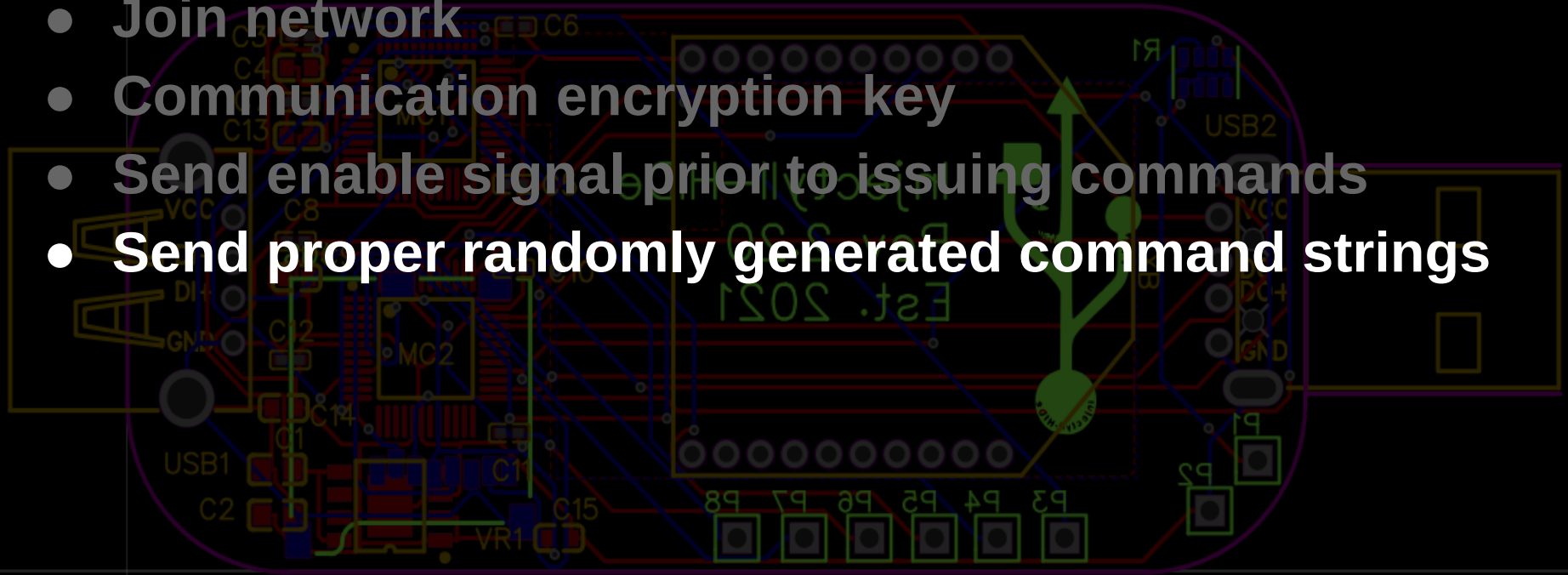
Communication interlocks

- Join network
- Communication encryption key
- **Send enable signal prior to issuing commands**



Communication interlocks

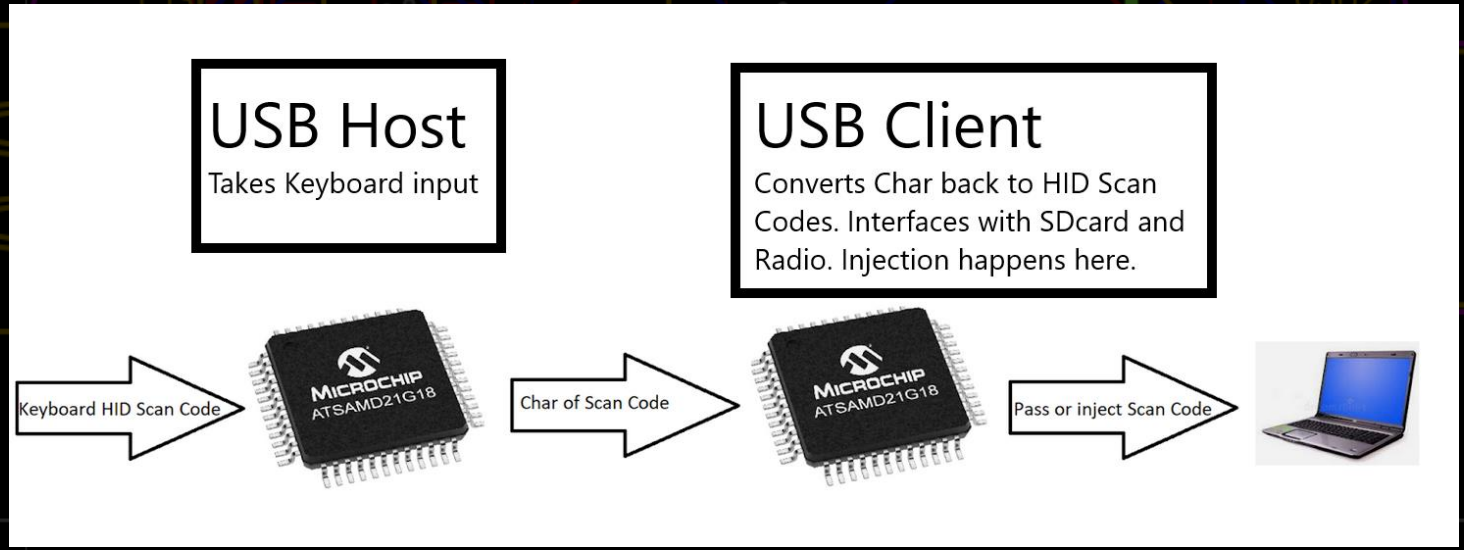
- Join network
- Communication encryption key
- Send enable signal prior to issuing commands
- **Send proper randomly generated command strings**



Keystroke injection/sniffing/recording

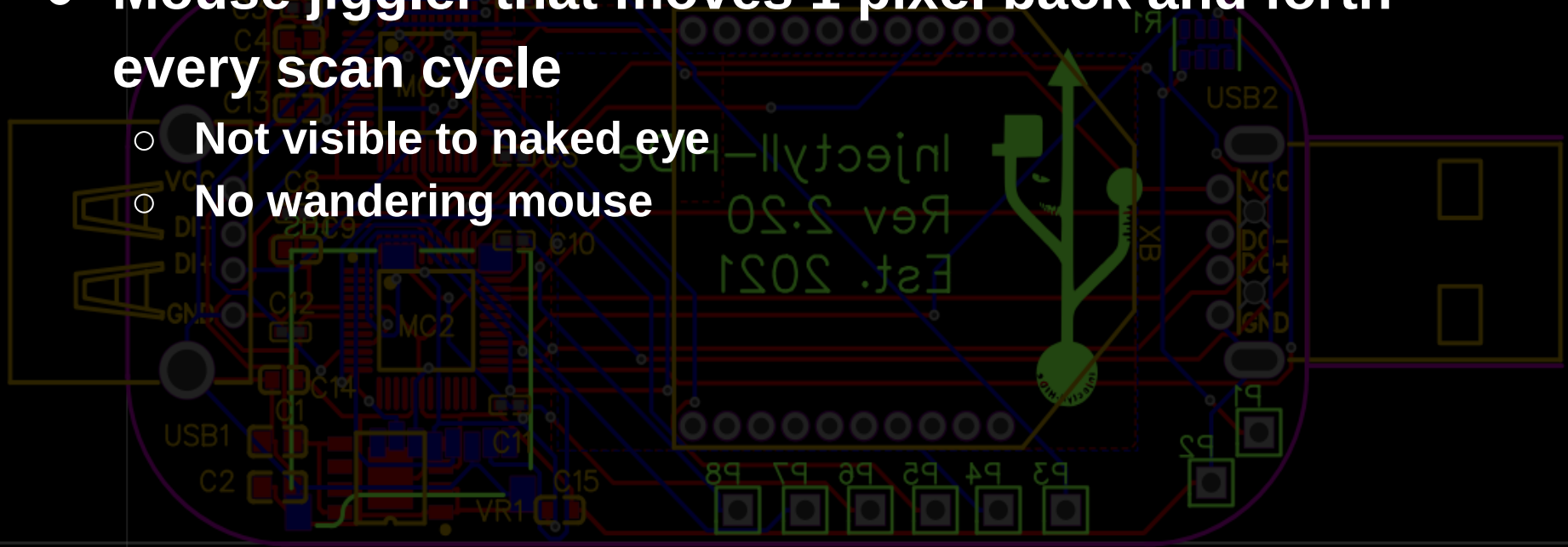
Started from USB Metamorph

- https://github.com/gdsports/usb-metamorph



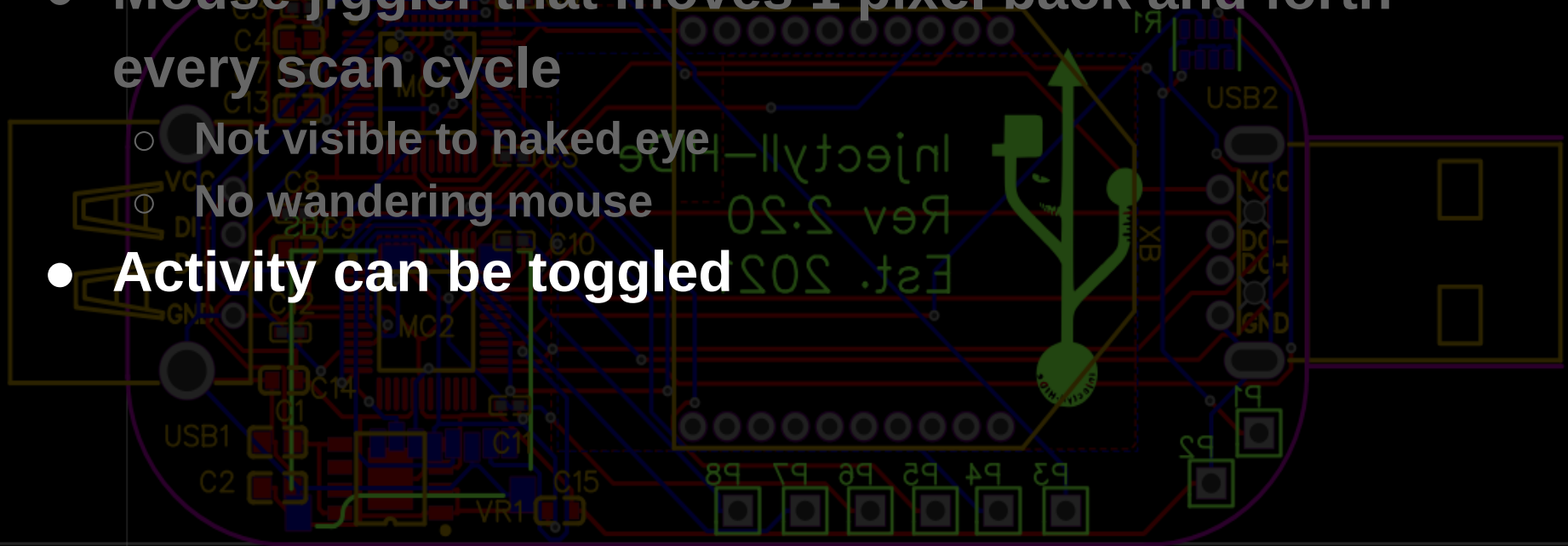
Insomnia Mode

- **Mouse jiggler that moves 1 pixel back and forth every scan cycle**
  - **Not visible to naked eye**
  - **No wandering mouse**



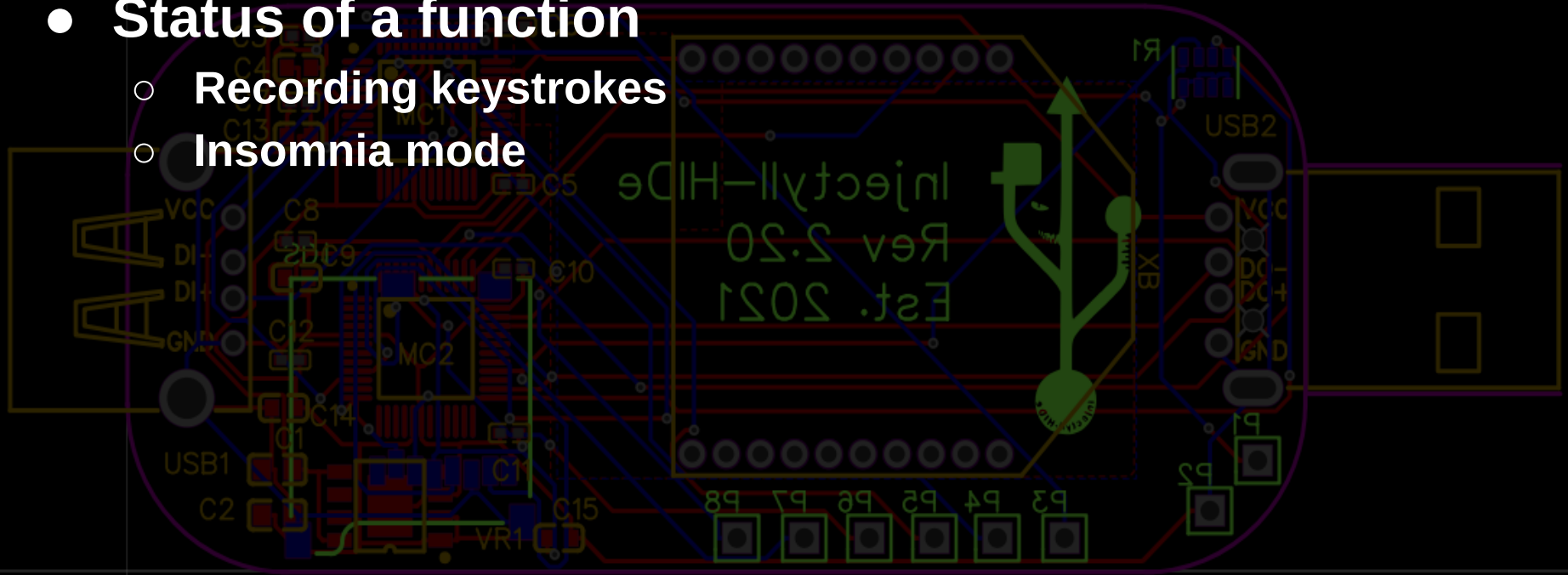
Insomnia Mode

- Mouse jiggler that moves 1 pixel back and forth every scan cycle
  - Not visible to naked eye
  - No wandering mouse
- **Activity can be toggled**



Status Update

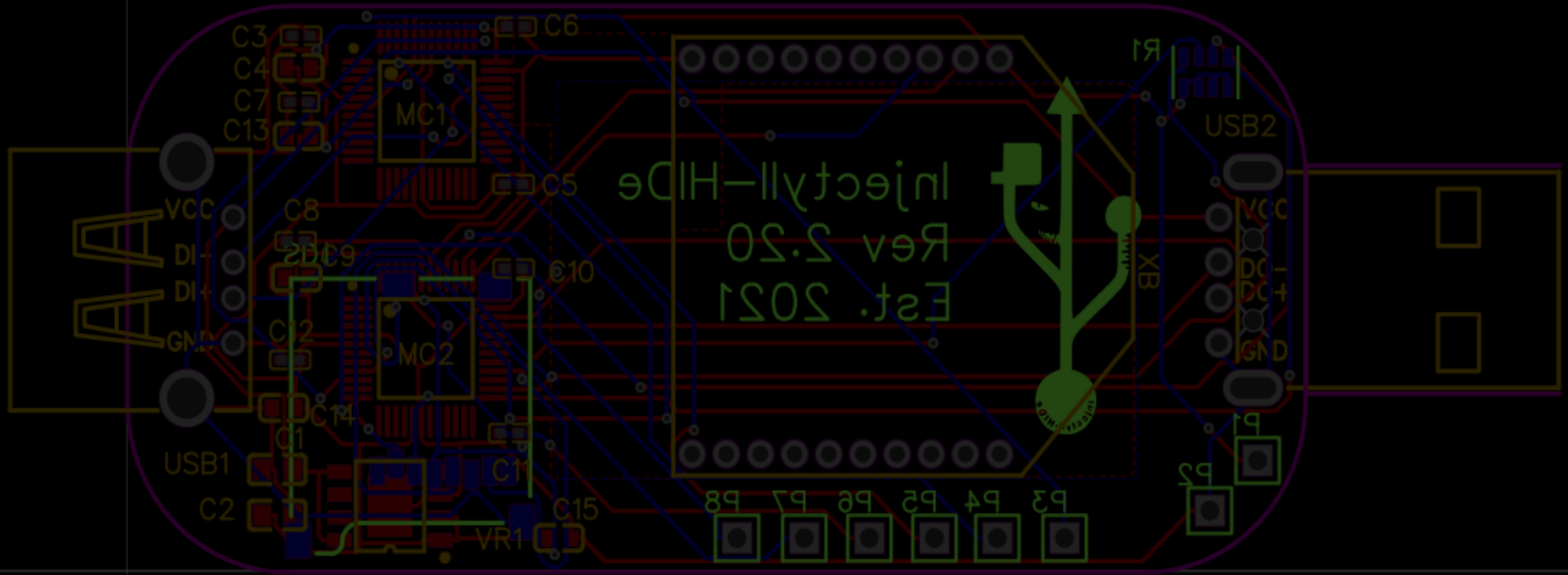
- **Status of a function**
  - **Recording keystrokes**
  - **Insomnia mode**



Status Update

- Status of a function
  - Recording keystrokes
  - Insomnia mode
- **Time elapsed since last key press detected**

Storage and memory management

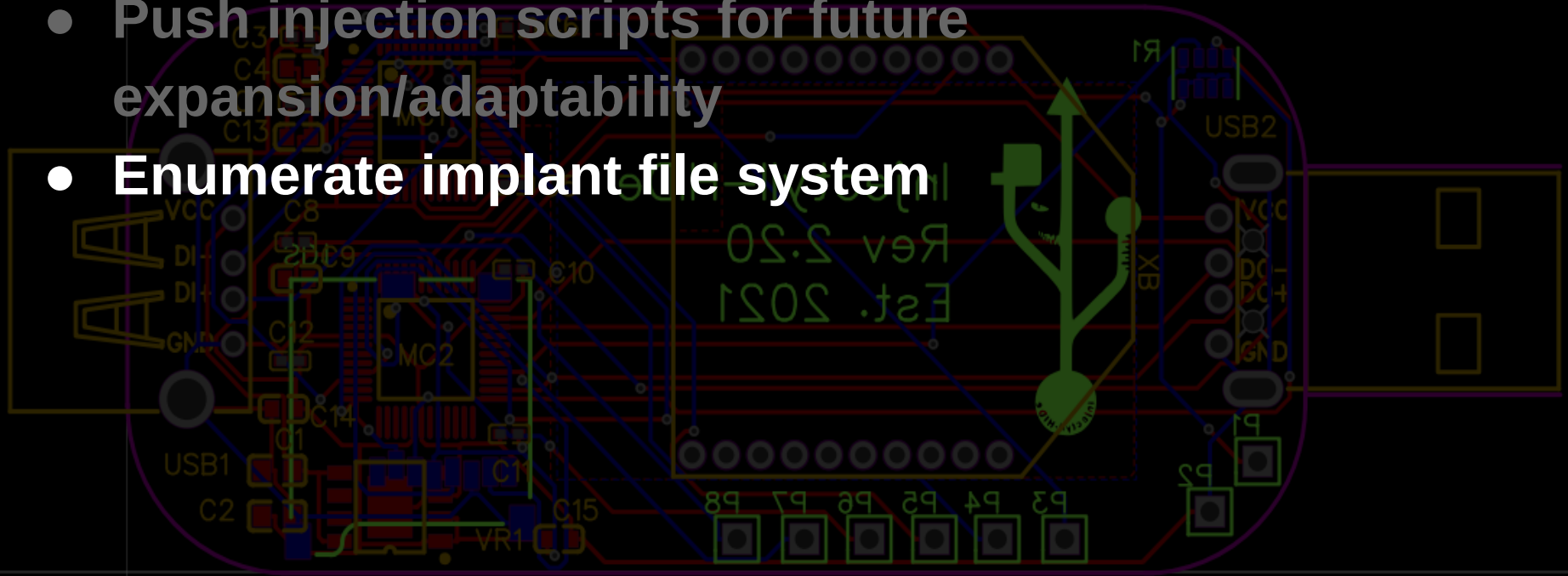


Storage and memory management

- **Push injection scripts for future expansion/adaptability**

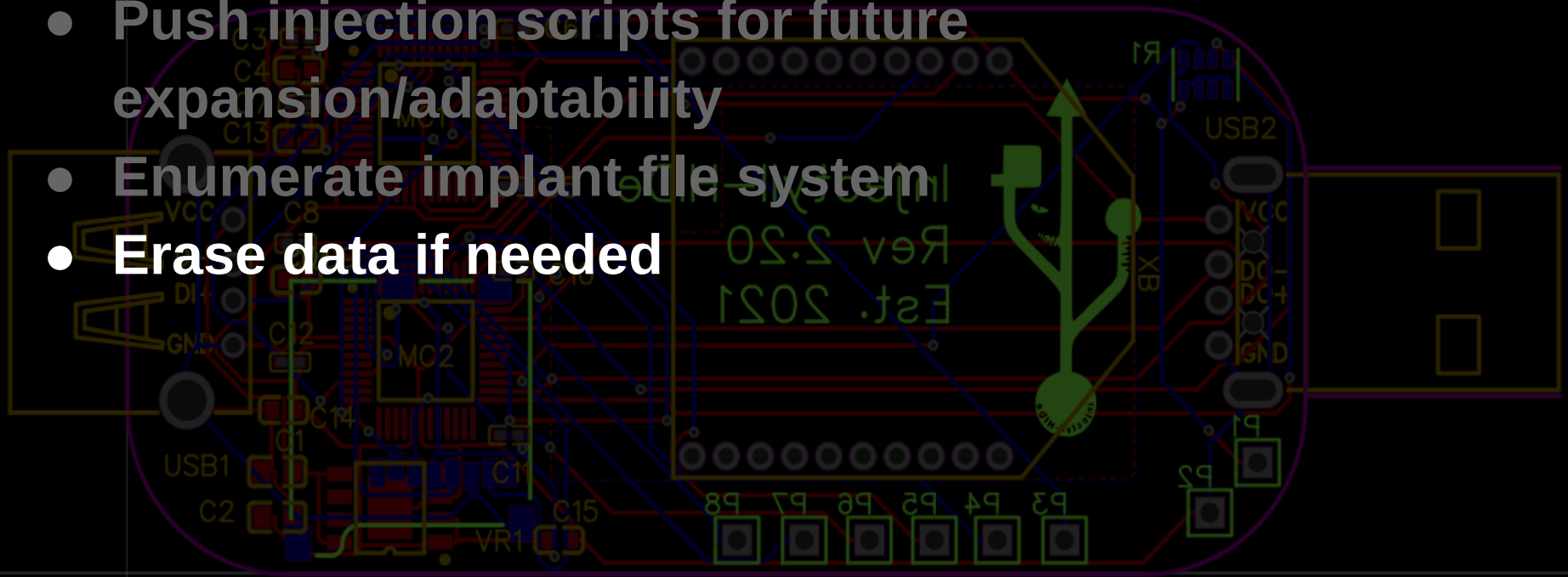
Storage and memory management

- Push injection scripts for future expansion/adaptability
- **Enumerate implant file system**

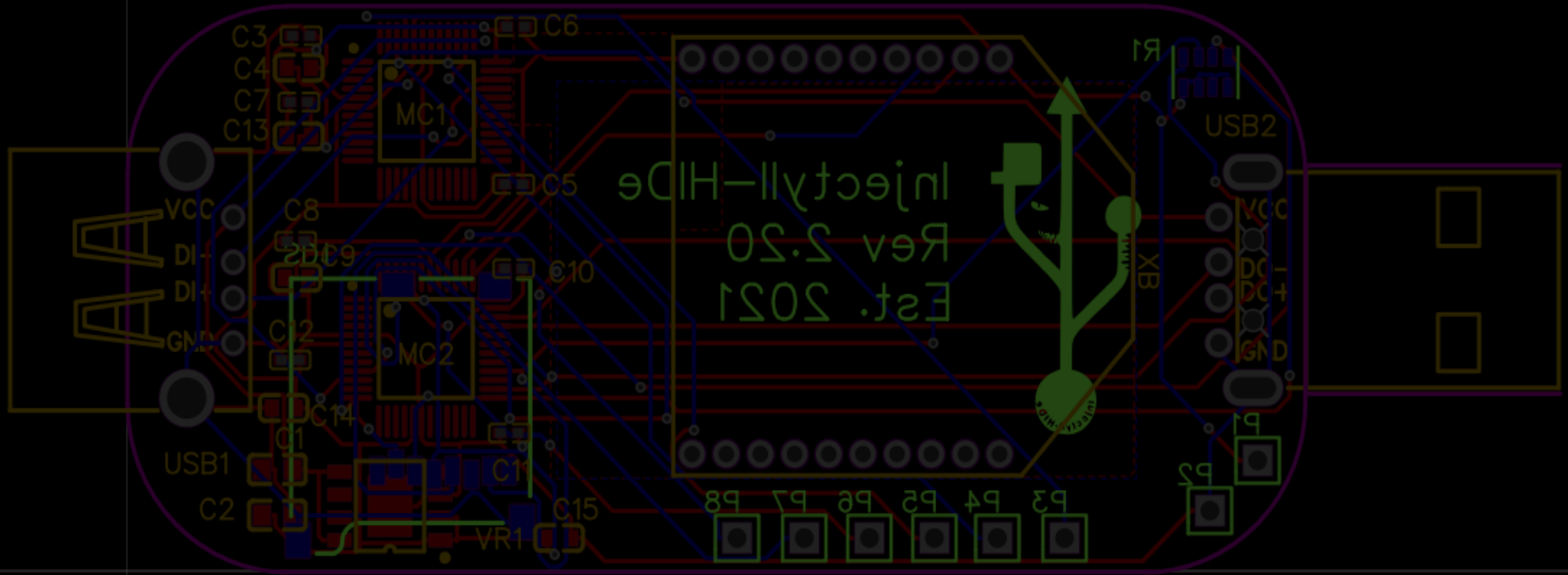


Storage and memory management

- Push injection scripts for future expansion/adaptability
- Enumerate implant file system
- **Erase data if needed**



Go Dark mode



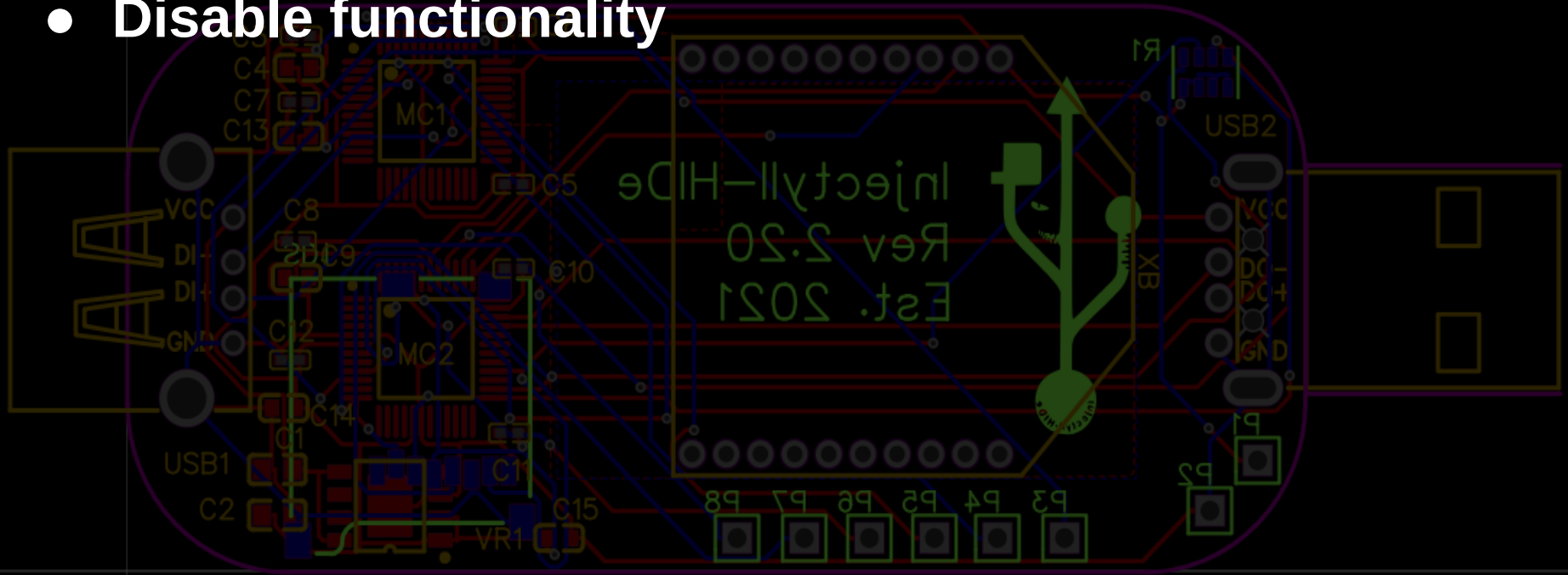
@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

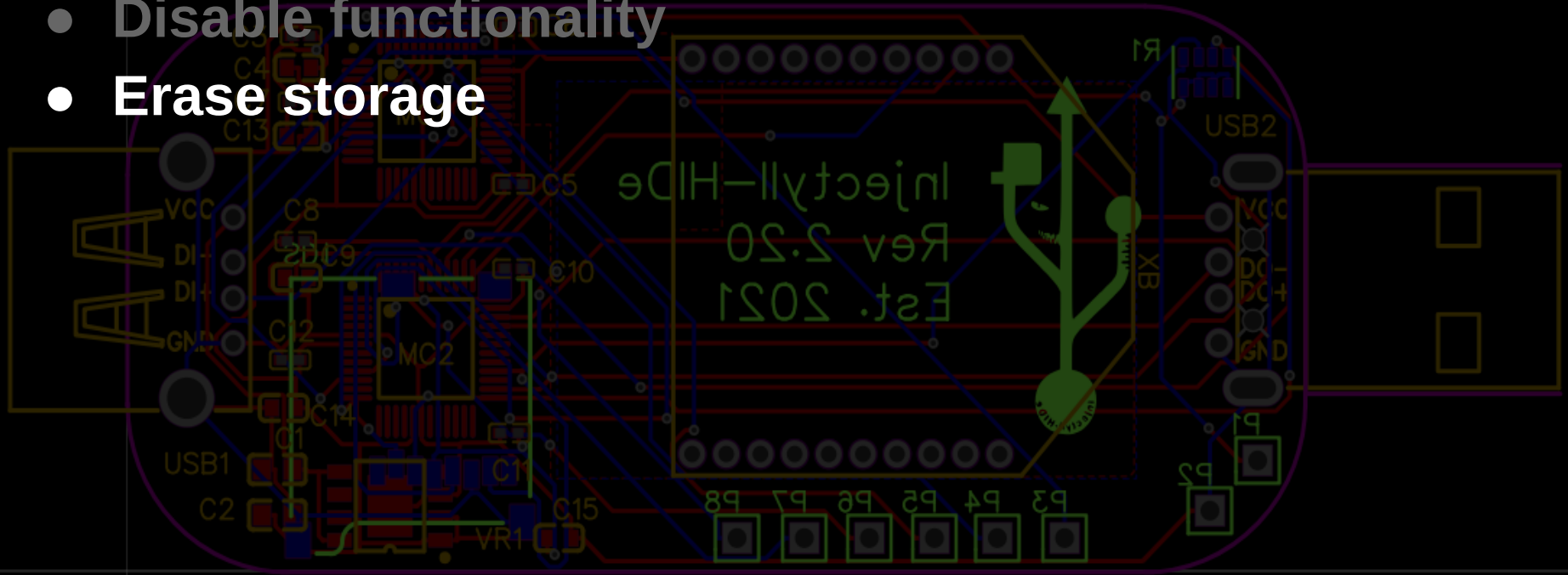
Go Dark mode

- **Disable functionality**



Go Dark mode

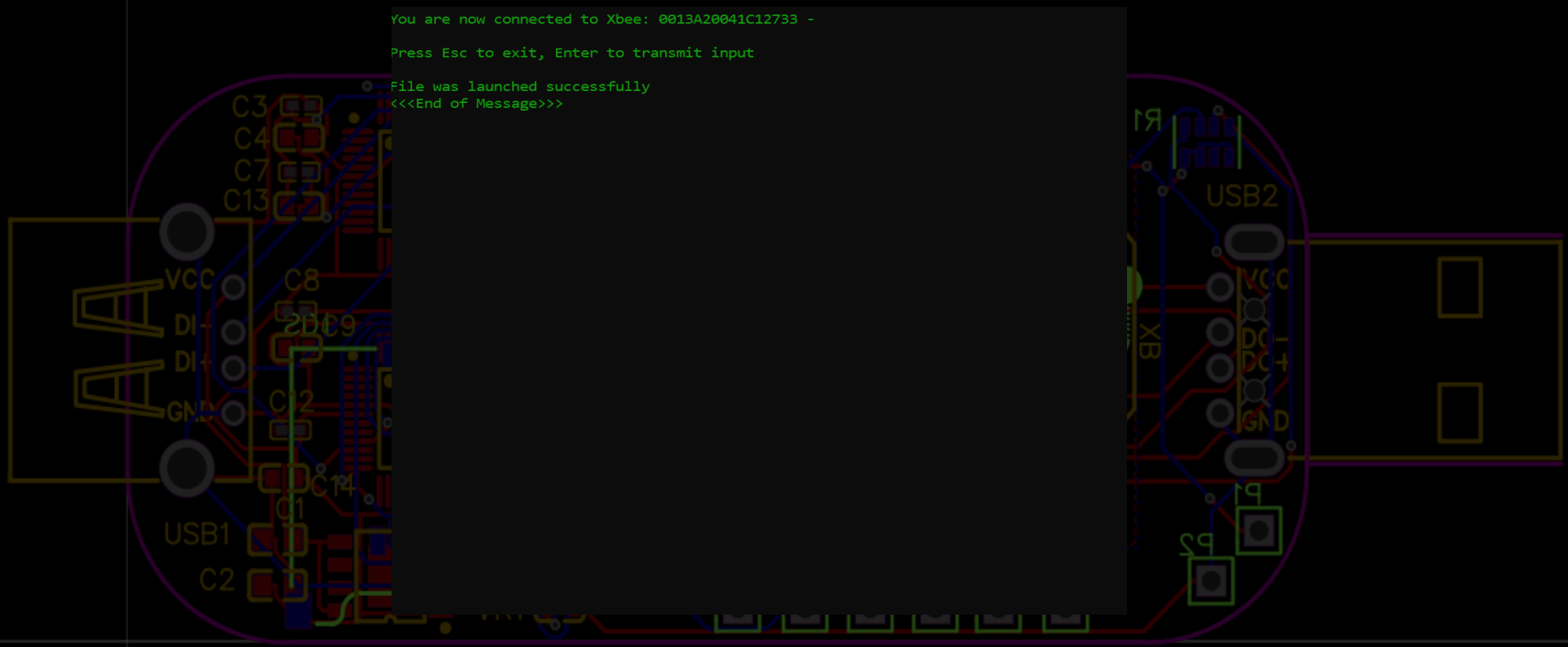
- Disable functionality
- **Erase storage**



Go Dark mode

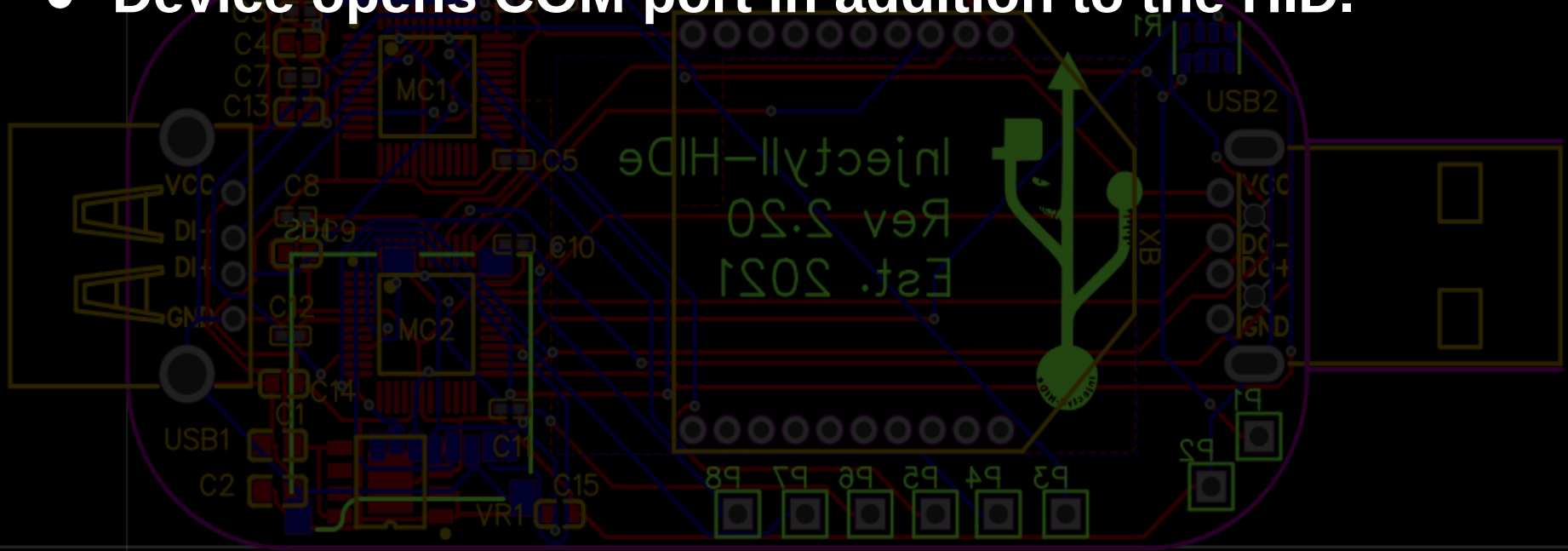
- Disable functionality
- Erase storage
- **Wait for enable message**

reverse shell script (Windows)



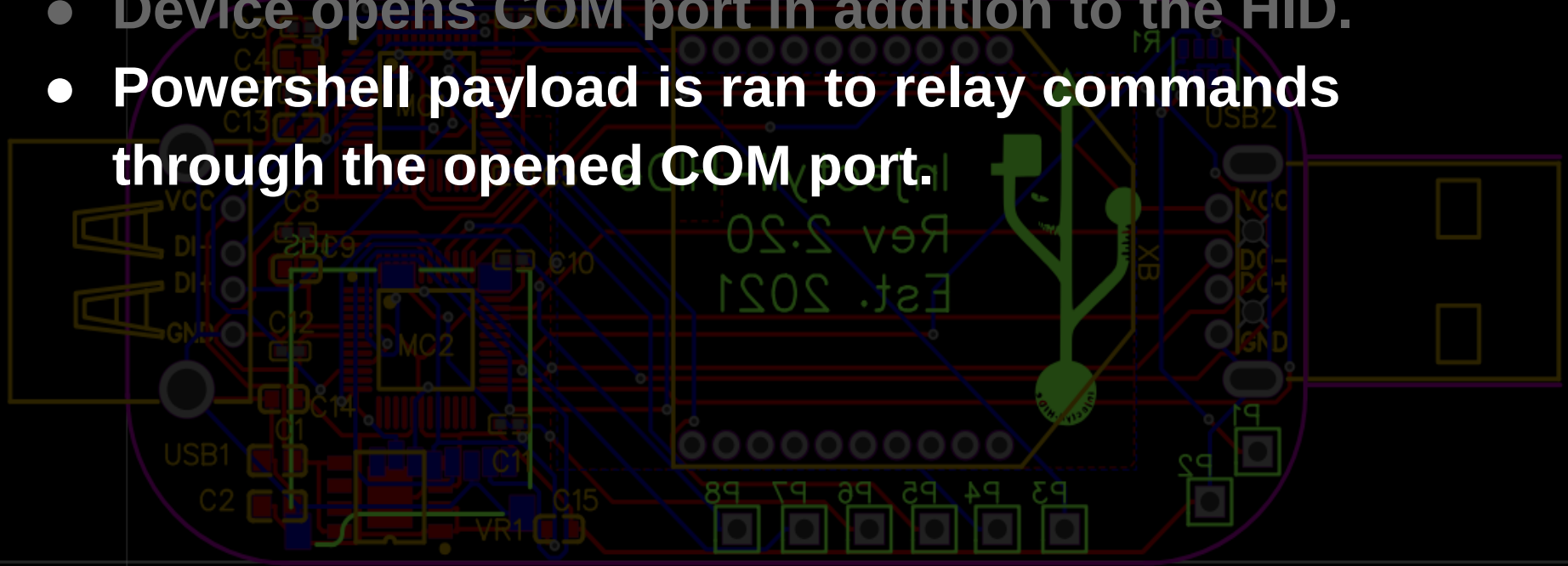
reverse shell script (Windows)

- **Device opens COM port in addition to the HID.**



reverse shell script (Windows)

- Device opens COM port in addition to the HID.
- **Powershell payload is ran to relay commands through the opened COM port.**



reverse shell script (Windows)

- Device opens COM port in addition to the HID.
- Powershell payload is ran to relay commands through the opened COM port.
- **Commands sent to this COM port are sent through the radio and then to the C2 over the Digimesh protocol. (Works even when screen is locked)**

data exfil script

```
2)  Scan for Implants
3)  Activate Implants
4)  Get implant information
5)  Sniff keystrokes
6)  Enable Insomnia mode
7)  Disable Insomnia mode
8)  Enable Keystroke Recorder
9)  Disable Keystroke Recorder
10) Download keystroke record
11) Self-destruct mode
12) Get file list from target
13) Receive data file
14) Launch attack from script
15) Send attack script
16) Connect to Interactive Powershell Terminal
17) Delete a file on target implant
18) Reset target implant
19) Exit

Choose your function: 13
Choose which device to receive file from.

Pick your target:

0) Enter your own target address

1) 0013A20041C12733 -

Choose target: 1
Enter file name with extension to get (FULL PATH): C:\Users\Jerm\Desktop\loot.txt
```

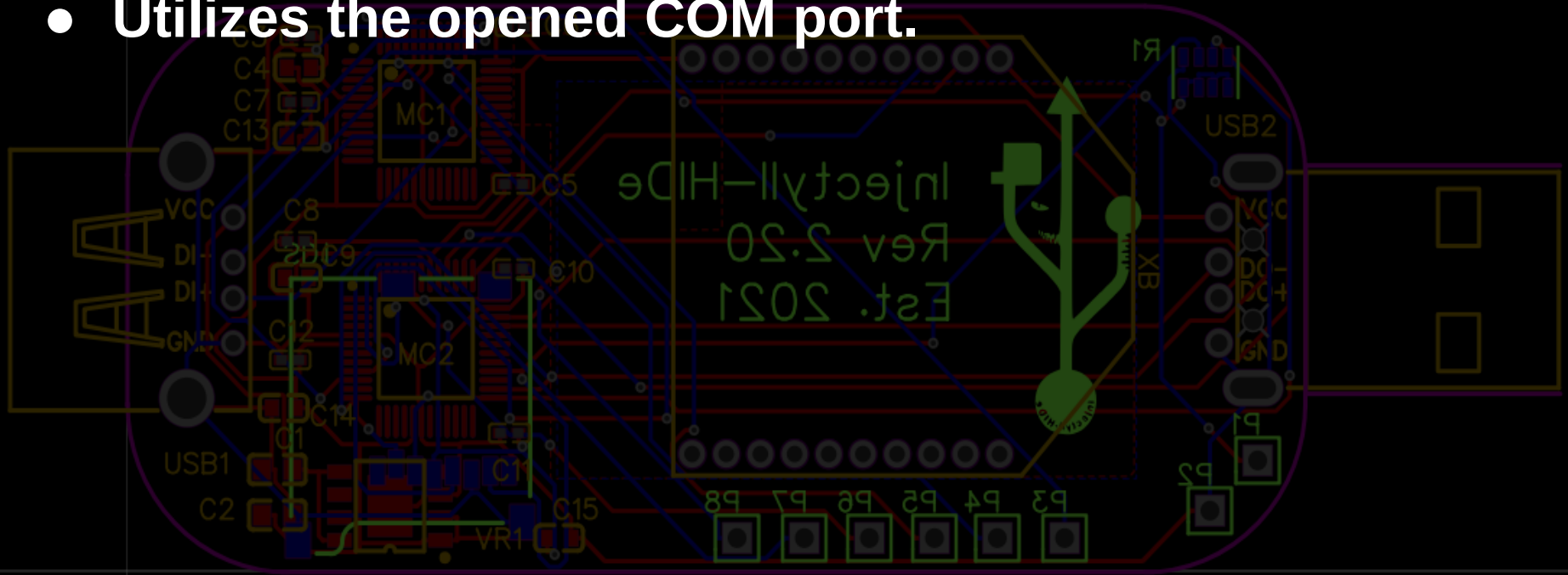
@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

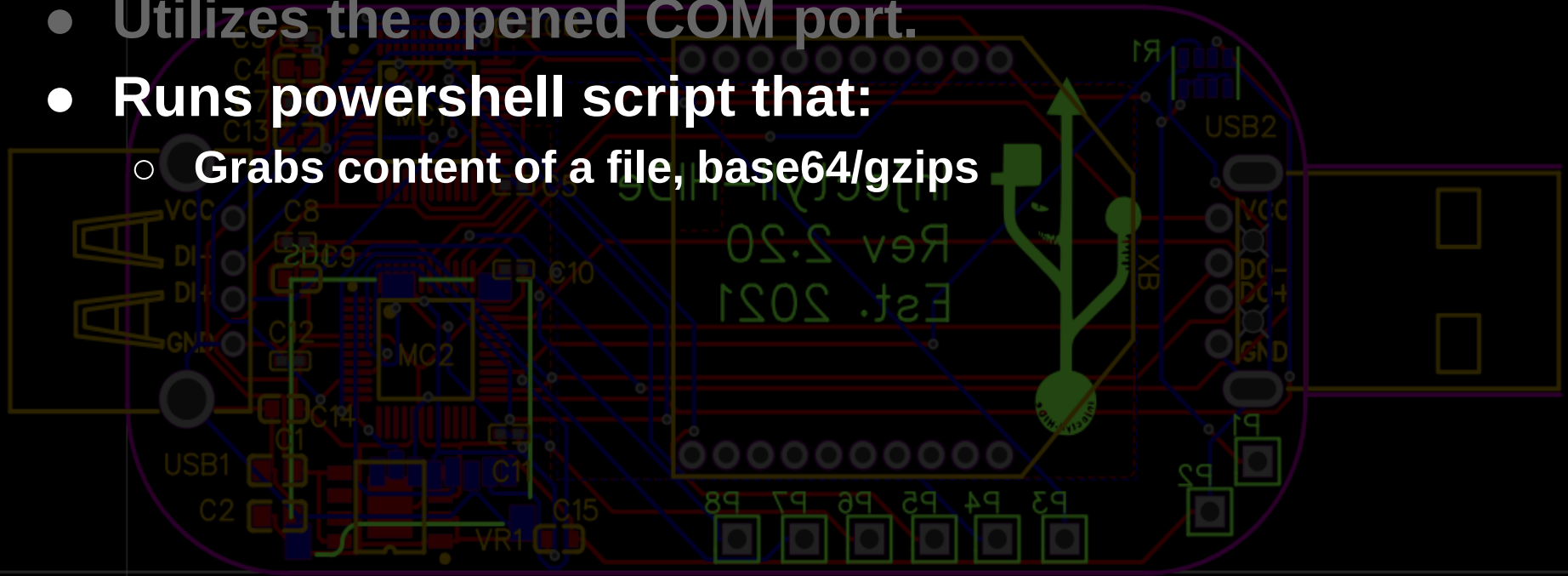
data exfil script

- **Utilizes the opened COM port.**



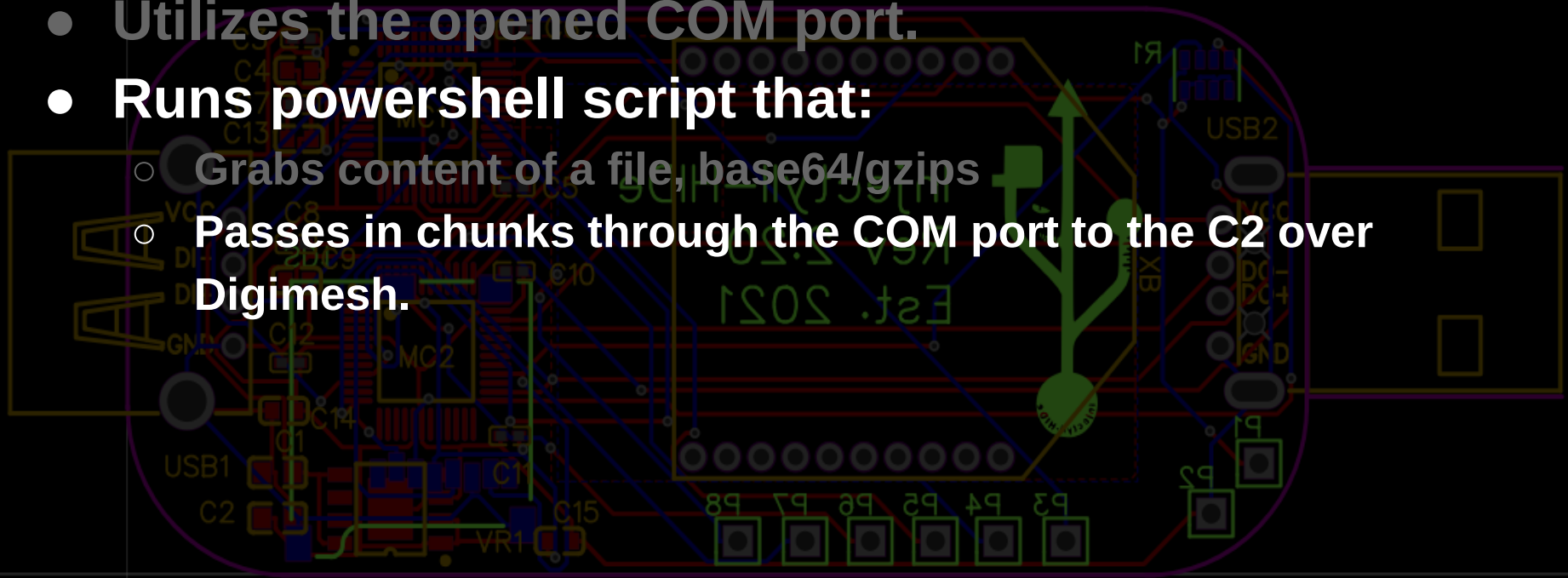
data exfil script

- Utilizes the opened COM port.
- **Runs powershell script that:**
  - **Grabs content of a file, base64/gzips**



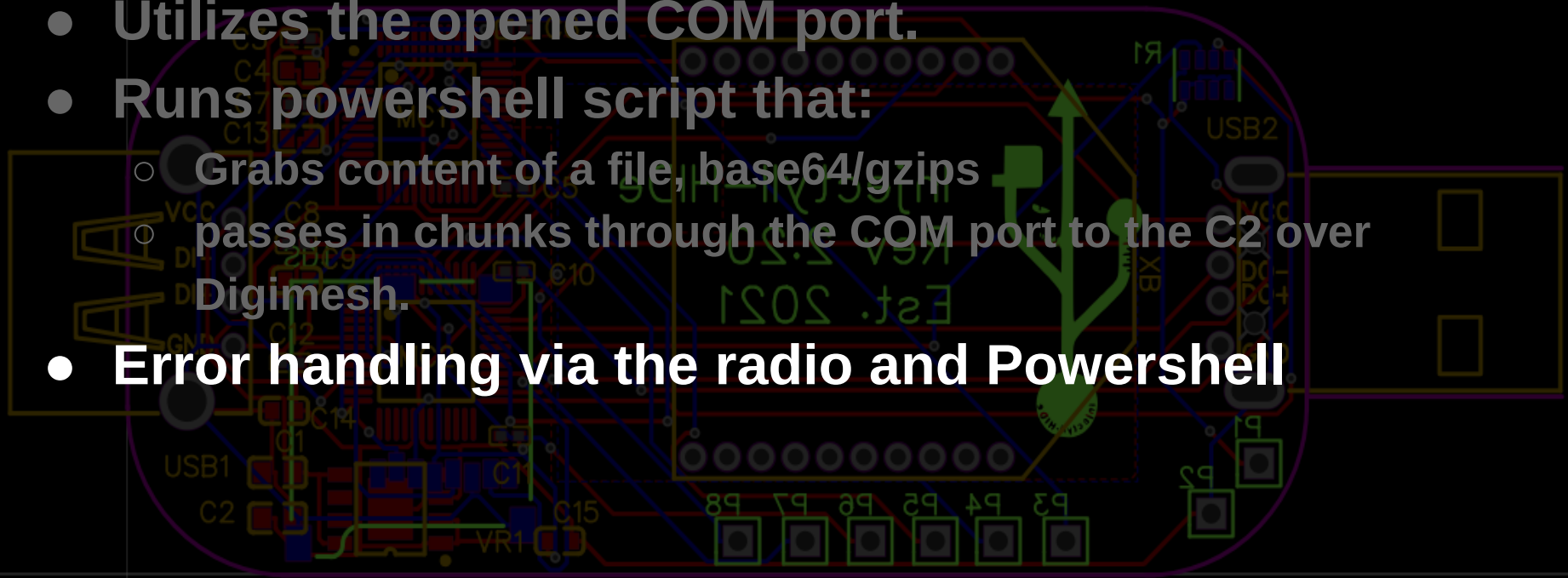
data exfil script

- Utilizes the opened COM port.
- **Runs powershell script that:**
  - Grabs content of a file, base64/gzips
  - **Passes in chunks through the COM port to the C2 over Digimesh.**



data exfil script

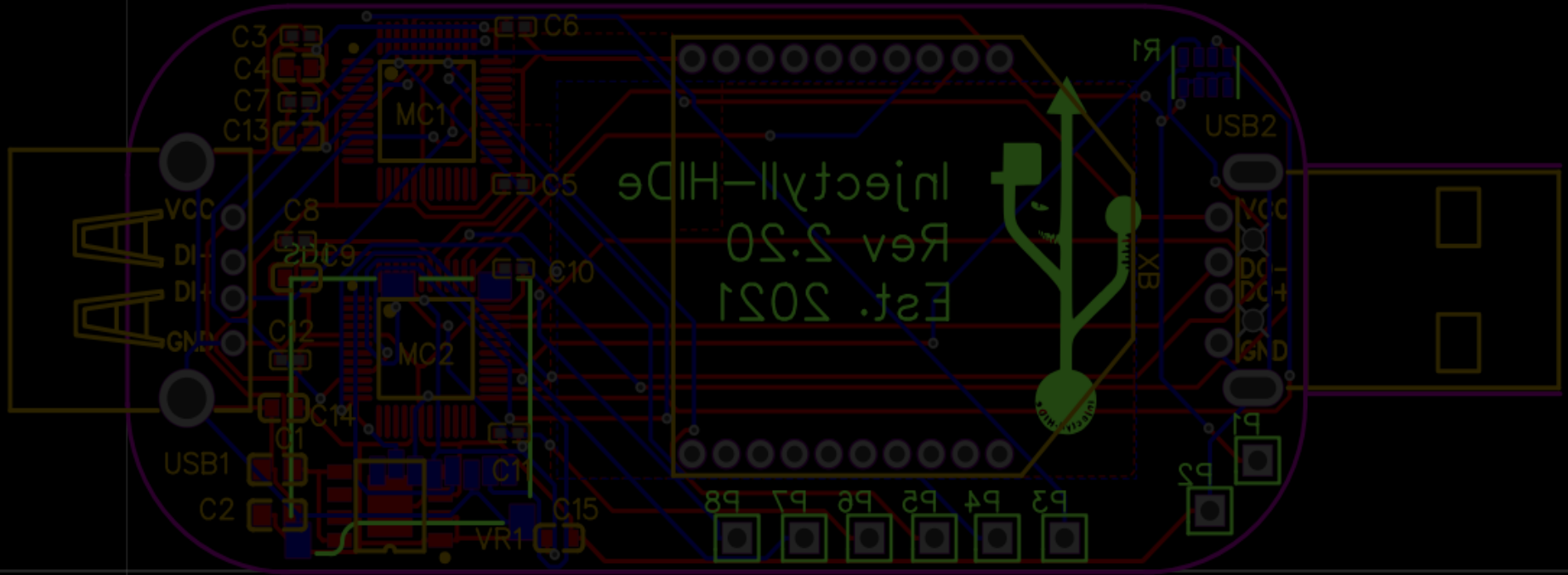
- Utilizes the opened COM port.
- Runs powershell script that:
  - Grabs content of a file, base64/gzips
  - passes in chunks through the COM port to the C2 over Digimesh.
- **Error handling via the radio and Powershell**



data exfil script

- Utilizes the opened COM port.
- Runs powershell script that:
  - Grabs content of a file, base64/gzips
  - passes in chunks through the COM port to the C2 over Digimesh.
- Error handling via the radio and Powershell
- **Script can run through previous made reverse shell using COM port. (Hidden from user)**

Demo 2

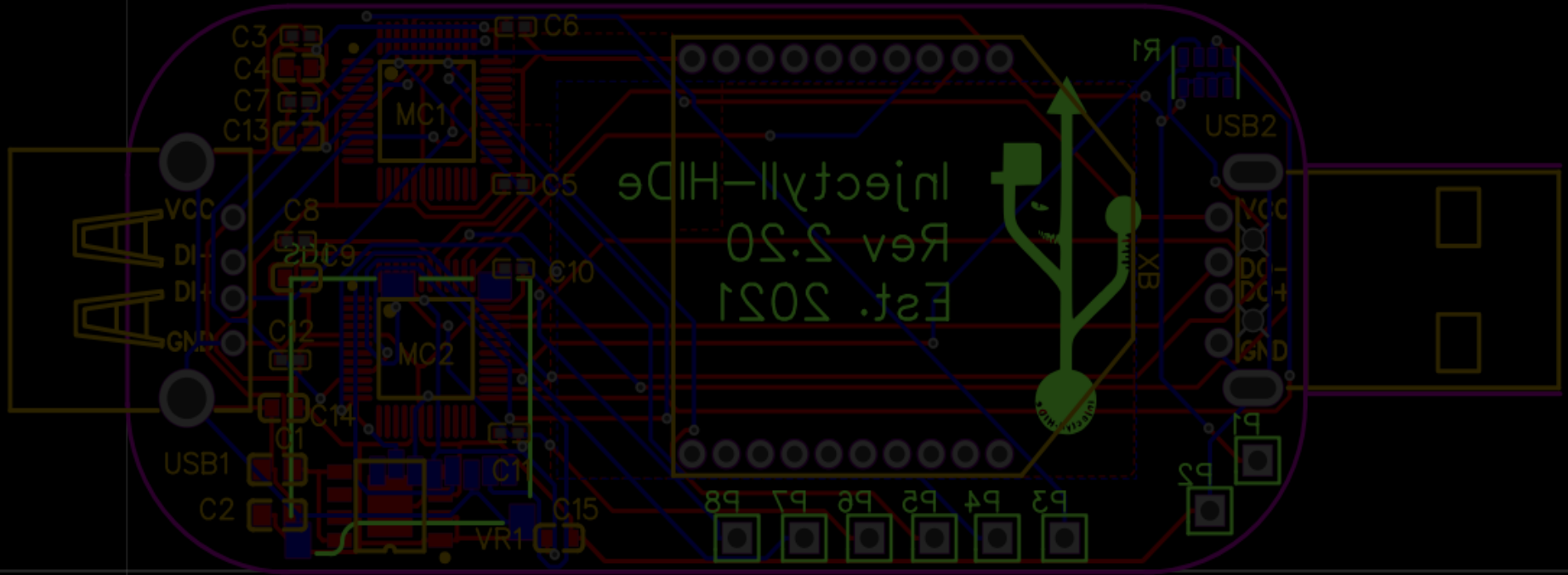


@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

How it meets our needs

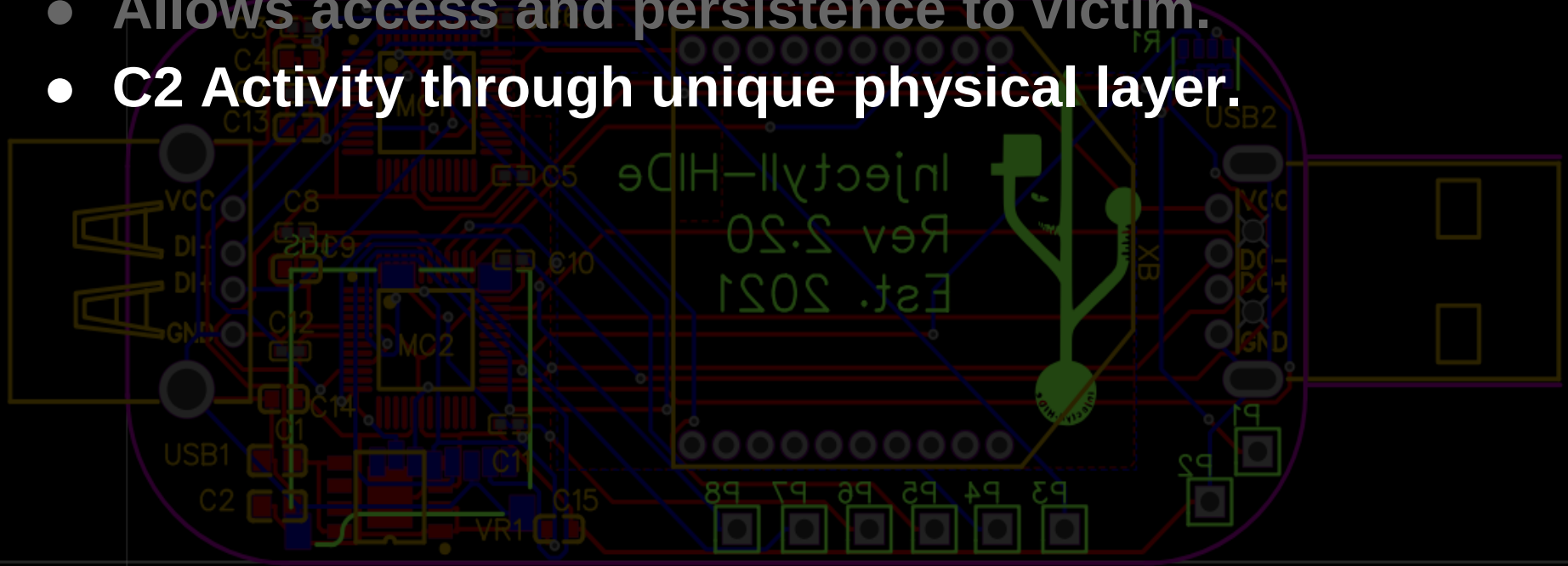


How it meets our needs

- **Allows access and persistence to victim.**

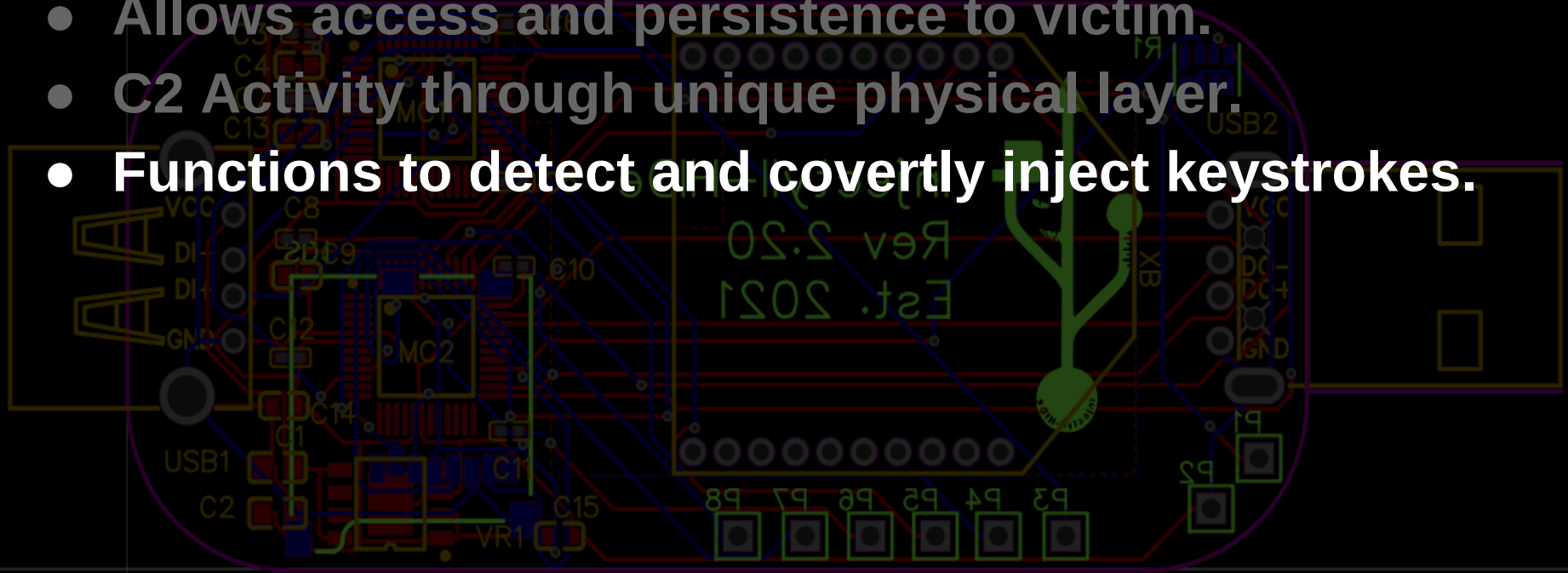
How it meets our needs

- Allows access and persistence to victim.
- **C2 Activity through unique physical layer.**



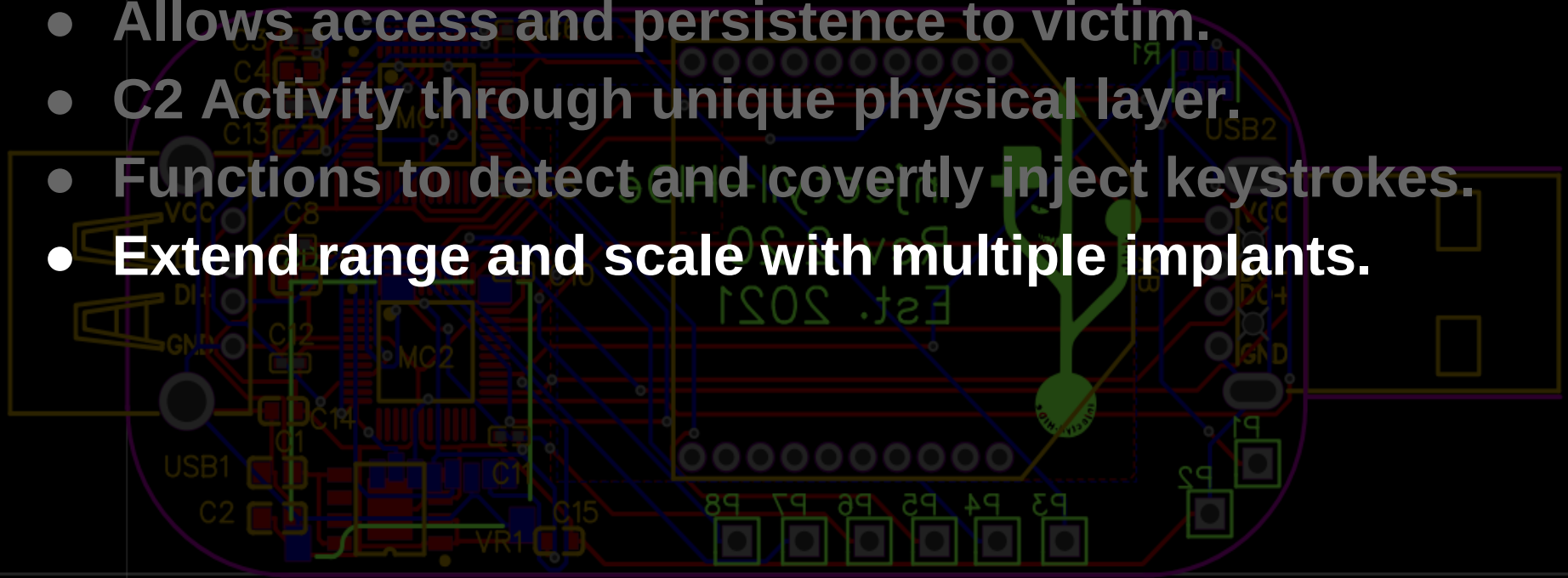
How it meets our needs

- Allows access and persistence to victim.
- C2 Activity through unique physical layer.
- **Functions to detect and covertly inject keystrokes.**

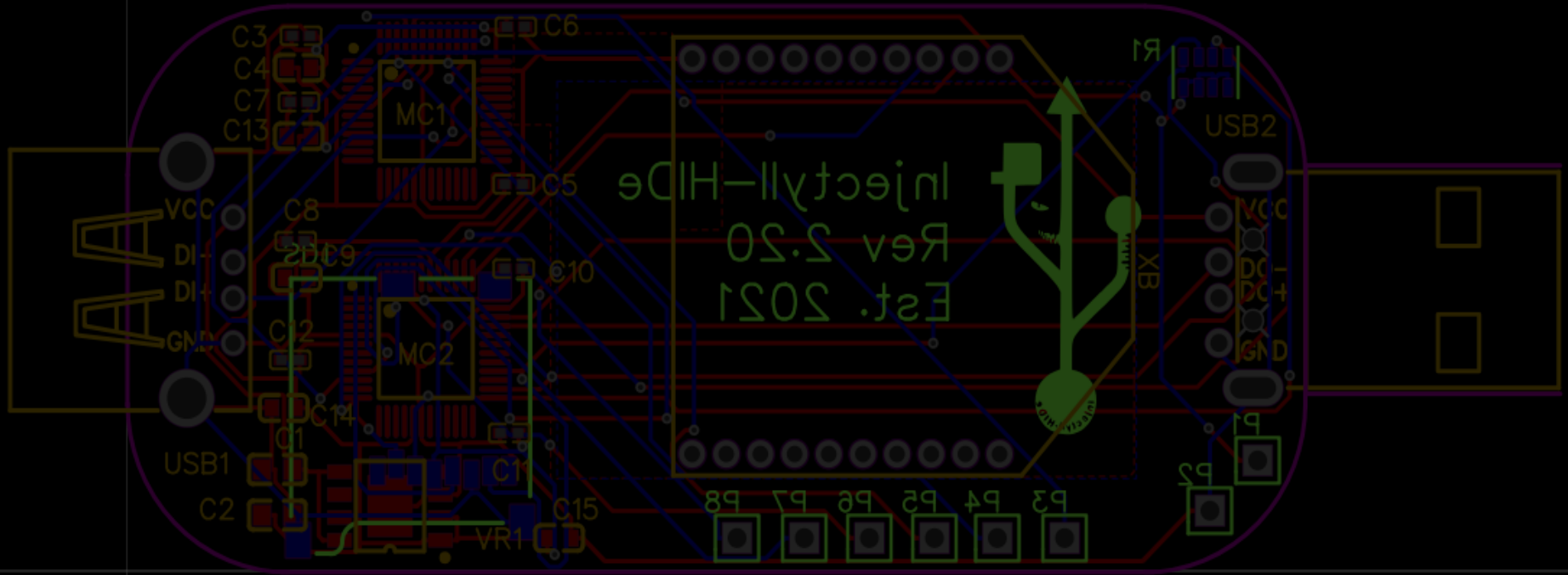


How it meets our needs

- Allows access and persistence to victim.
- C2 Activity through unique physical layer.
- Functions to detect and covertly inject keystrokes.
- **Extend range and scale with multiple implants.**



Defense



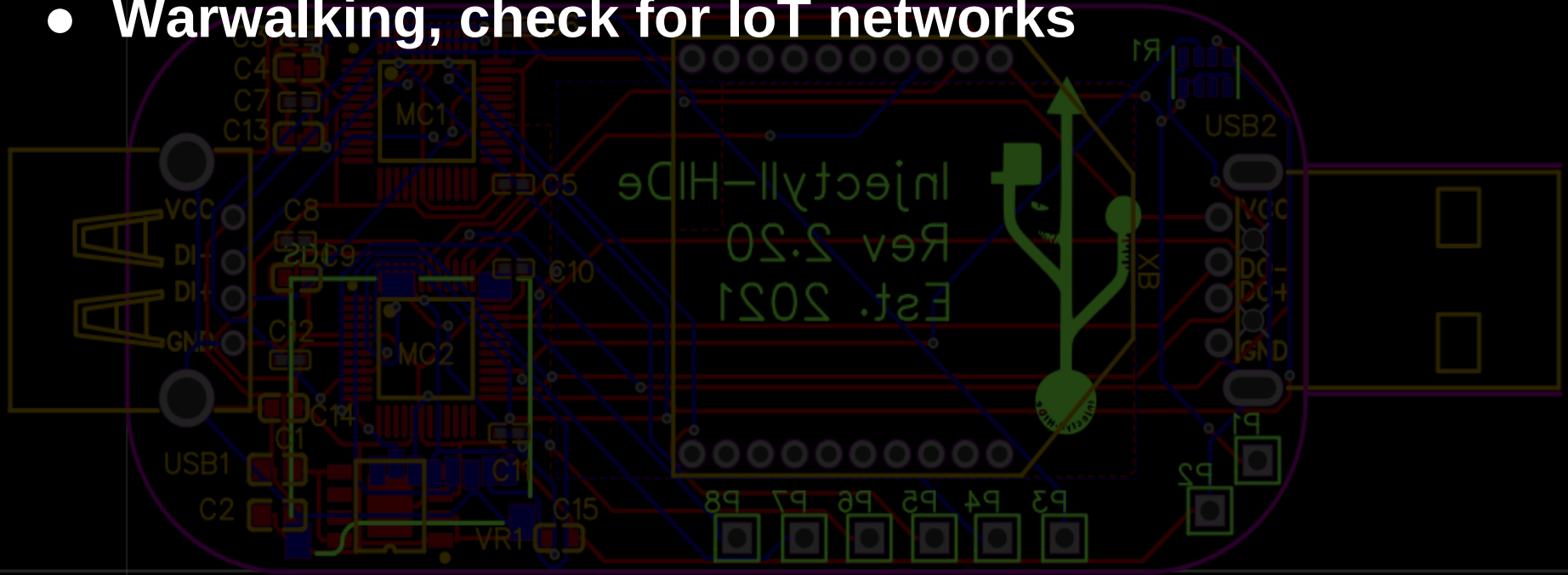
@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

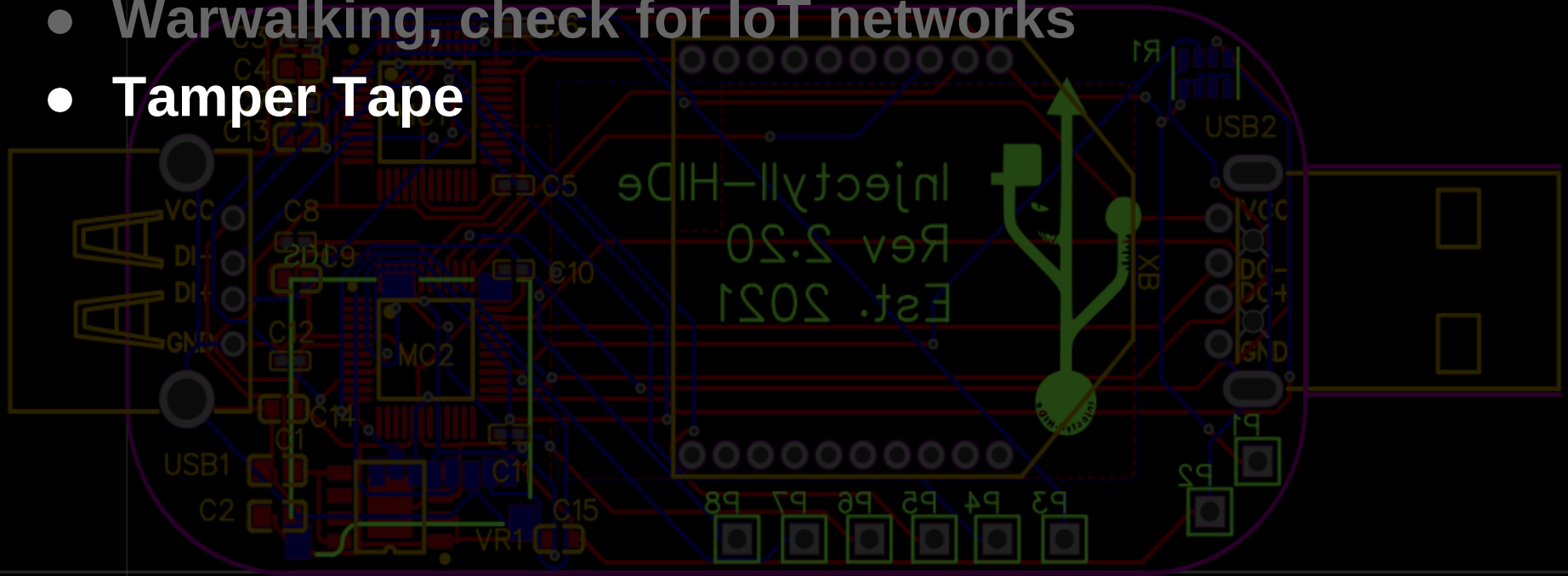
Defense

- **Warwalking, check for IoT networks**



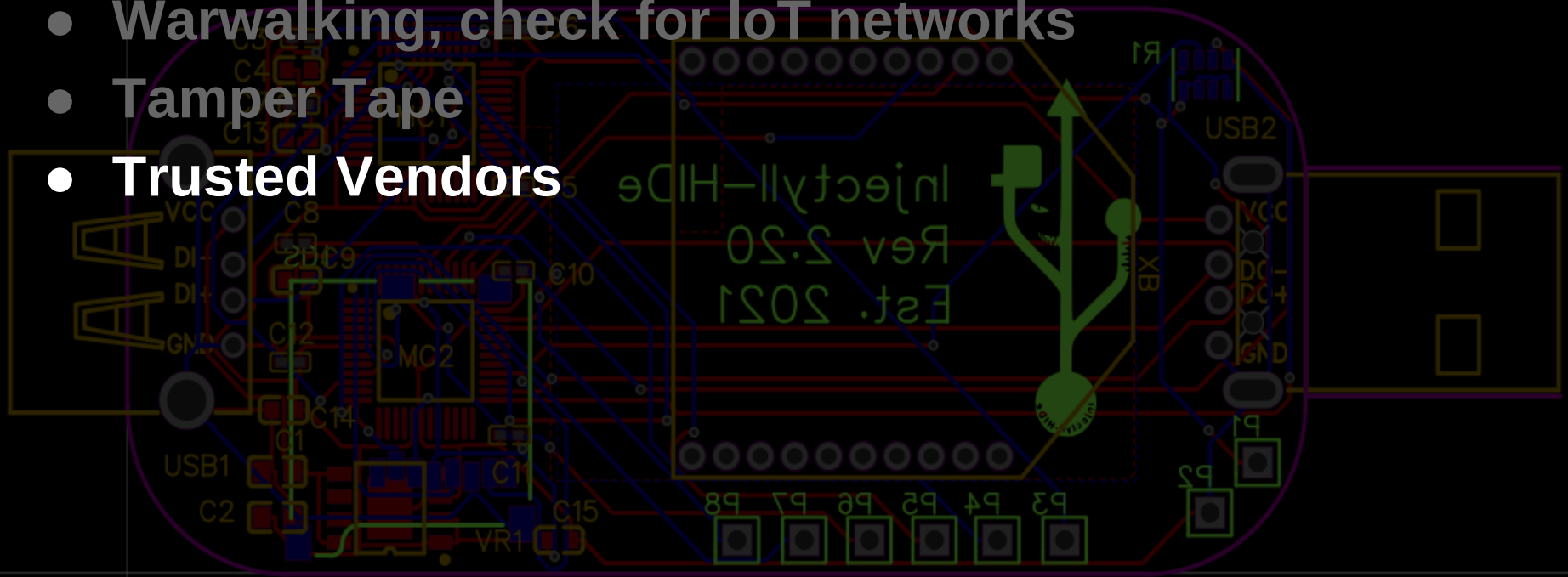
Defense

- Warwalking, check for IoT networks
- **Tamper Tape**

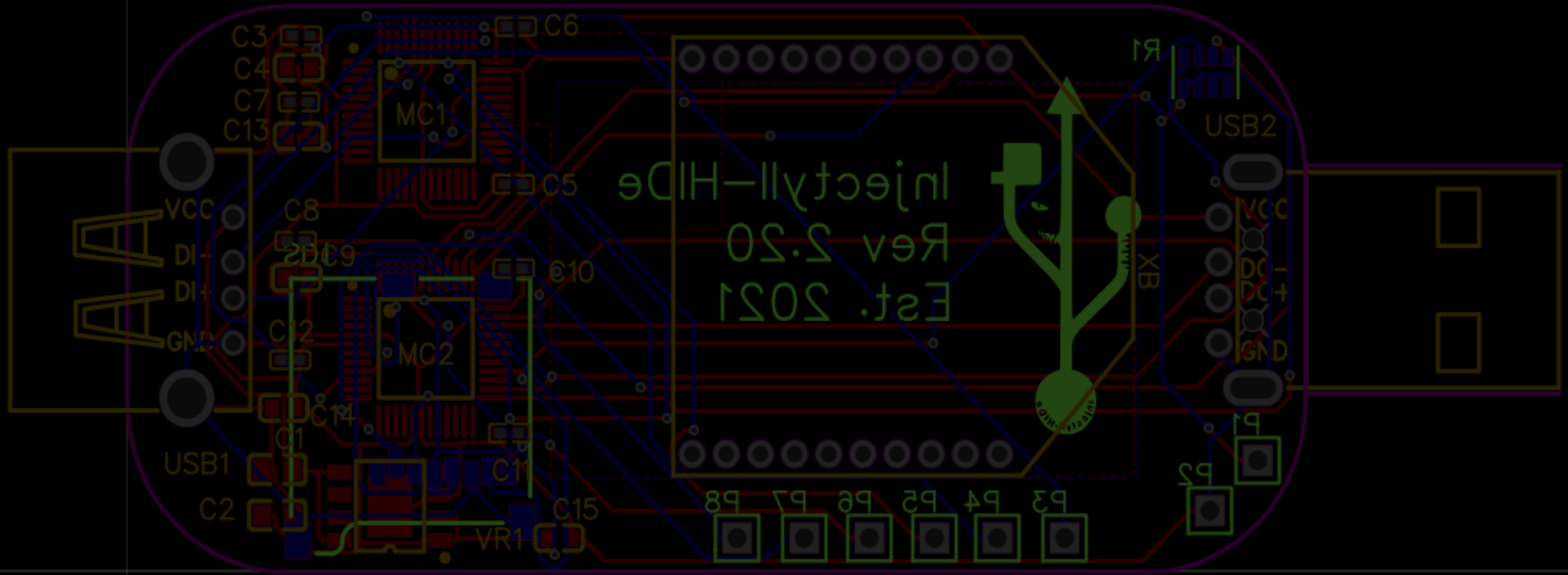


Defense

- Warwalking, check for IoT networks
- Tamper Tape
- **Trusted Vendors**



Version 2.0?



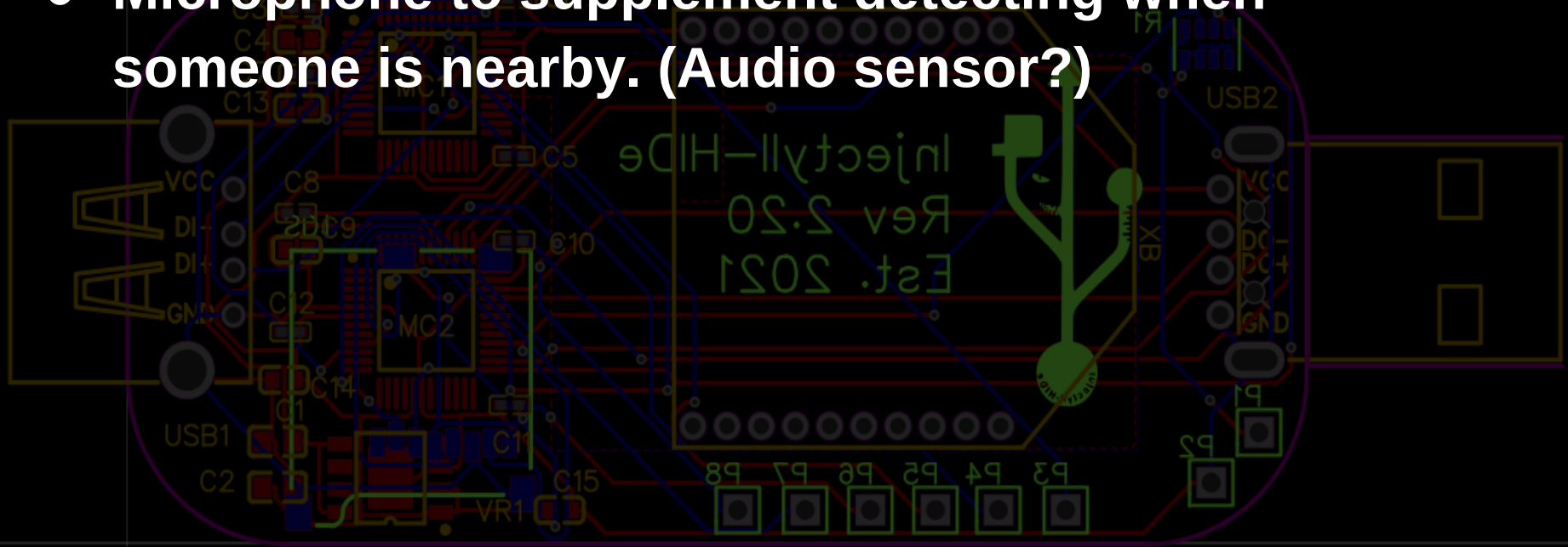
@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

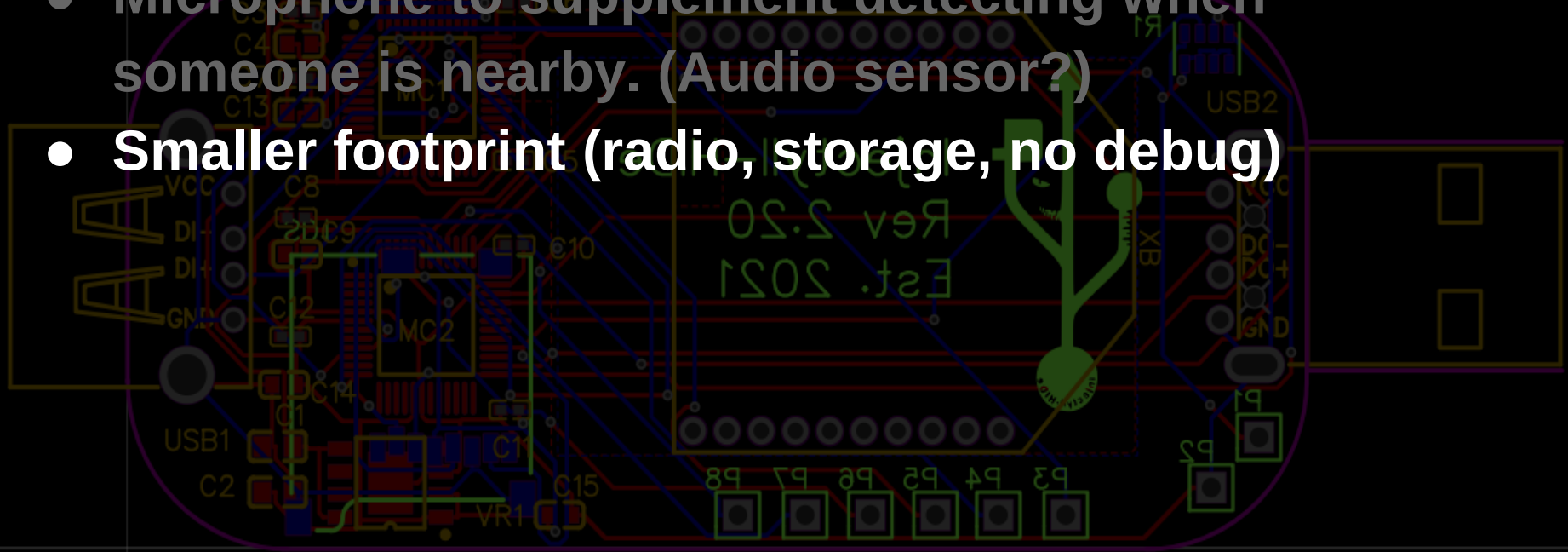
Version 2.0?

- **Microphone to supplement detecting when someone is nearby. (Audio sensor?)**



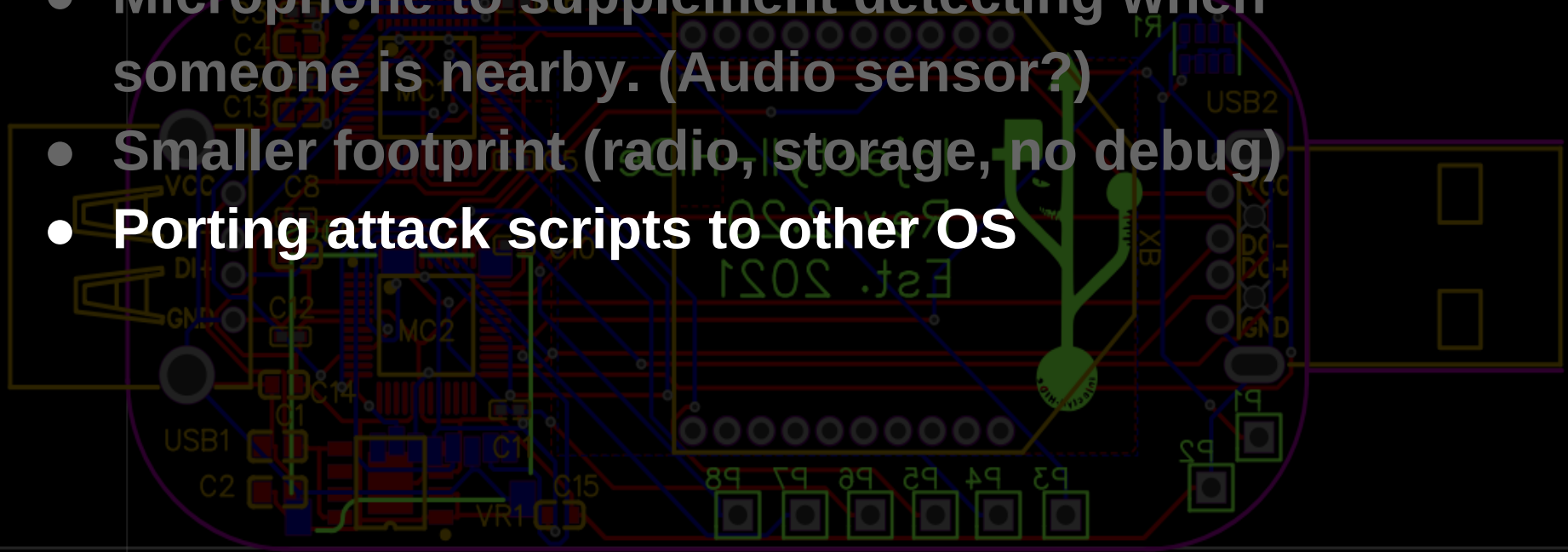
Version 2.0?

- Microphone to supplement detecting when someone is nearby. (Audio sensor?)
- **Smaller footprint (radio, storage, no debug)**



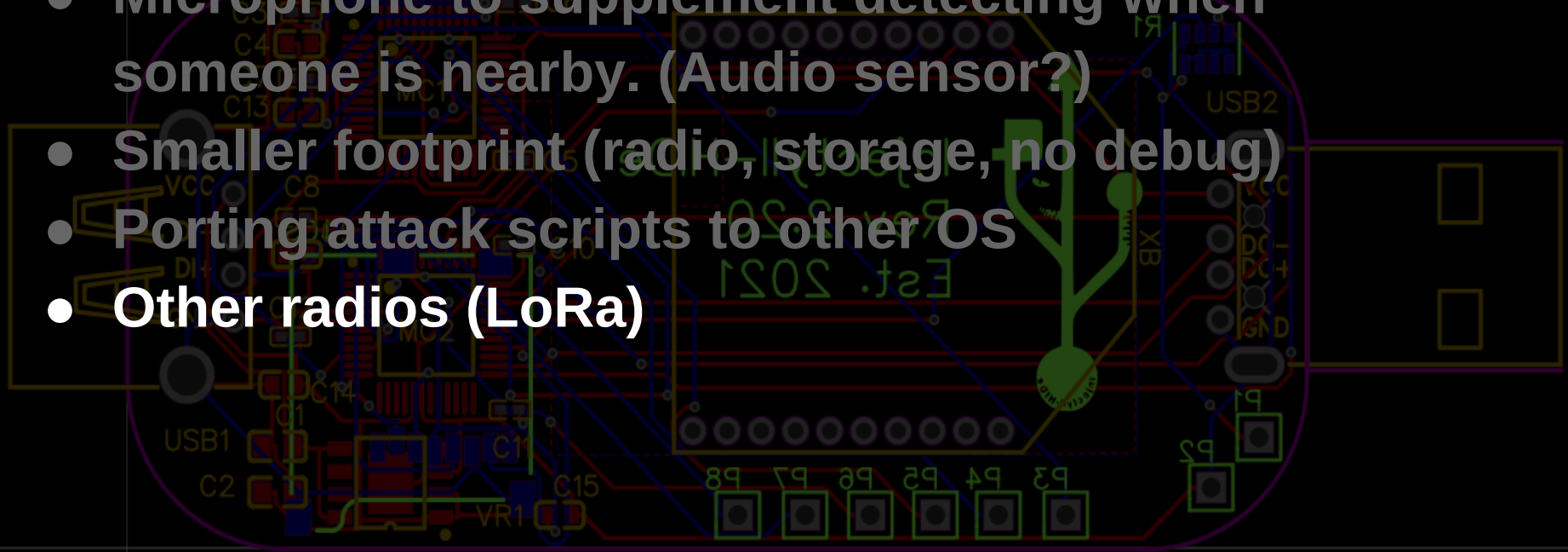
Version 2.0?

- Microphone to supplement detecting when someone is nearby. (Audio sensor?)
- Smaller footprint (radio, storage, no debug)
- **Porting attack scripts to other OS**



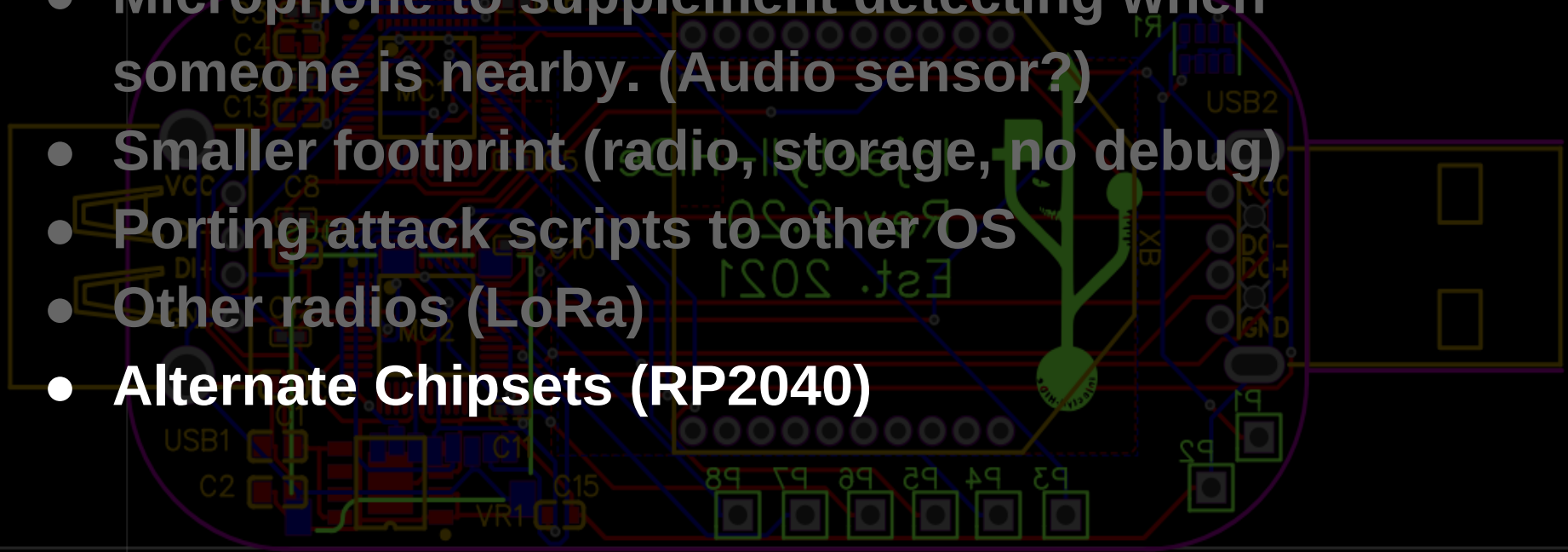
Version 2.0?

- Microphone to supplement detecting when someone is nearby. (Audio sensor?)
- Smaller footprint (radio, storage, no debug)
- Porting attack scripts to other OS
- **Other radios (LoRa)**



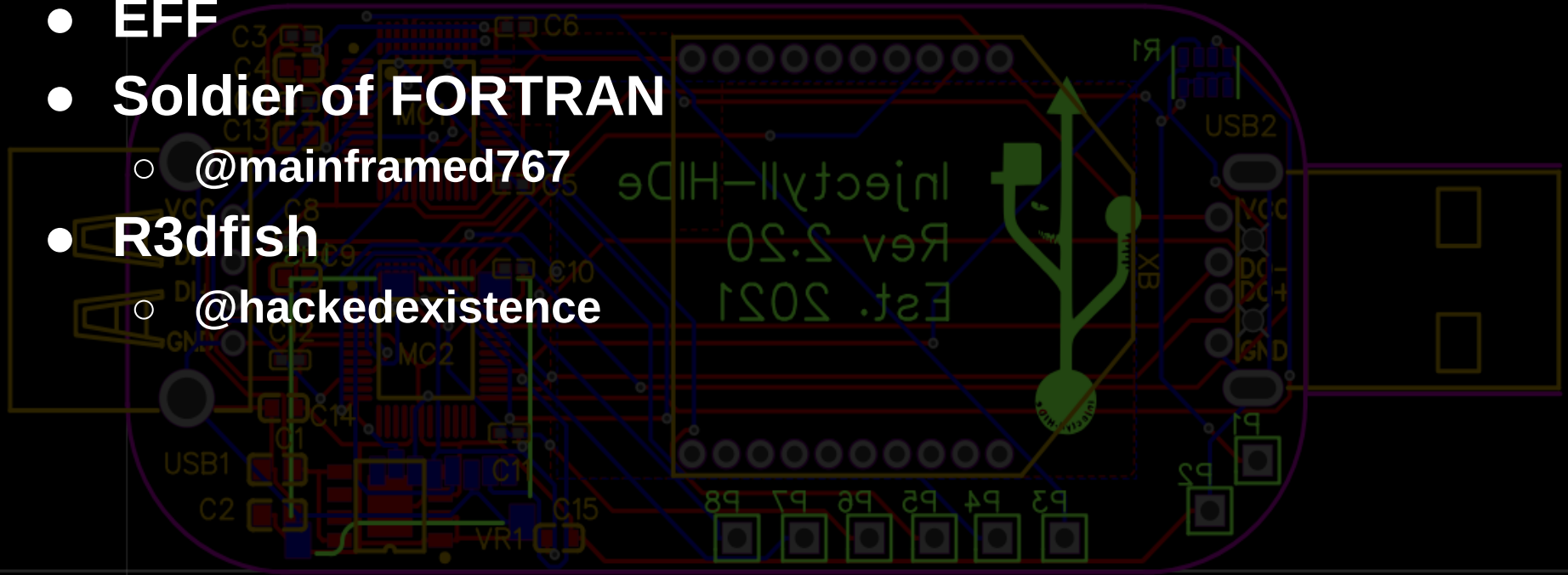
Version 2.0?

- Microphone to supplement detecting when someone is nearby. (Audio sensor?)
- Smaller footprint (radio, storage, no debug)
- Porting attack scripts to other OS
- Other radios (LoRa)
- **Alternate Chipsets (RP2040)**



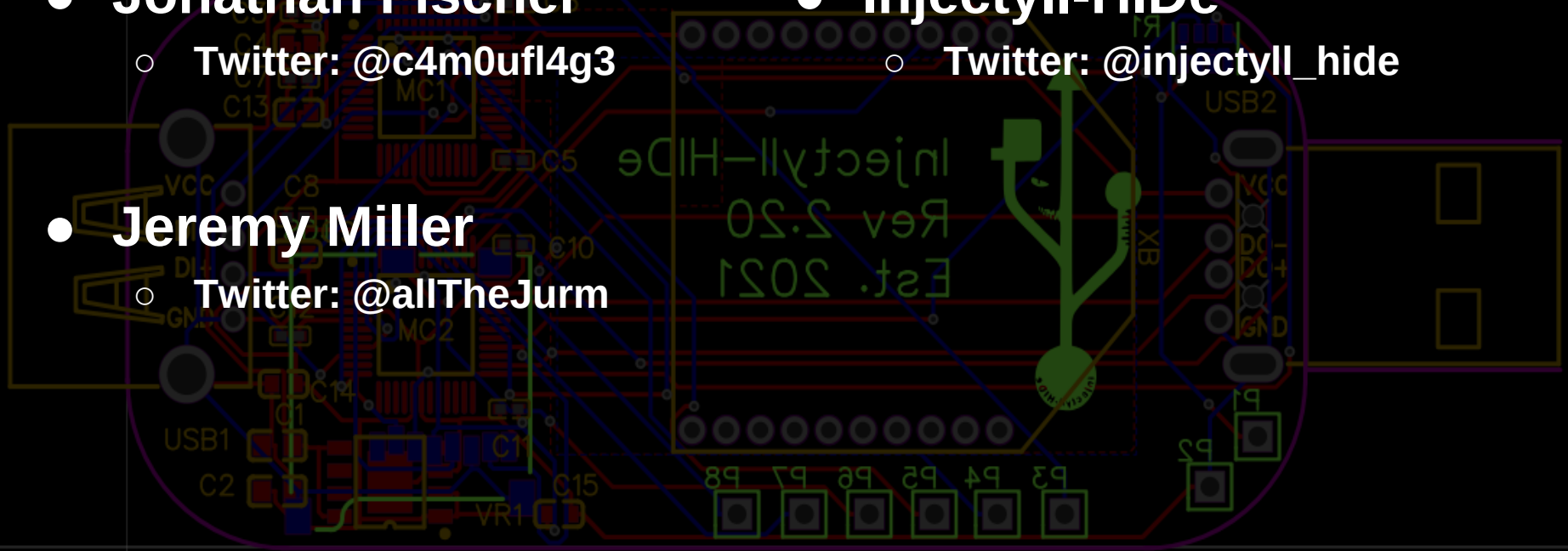
Special Thank You!

- EFF
- Soldier of FORTRAN
  - @mainframed767
- R3dfish
  - @hackedexistence



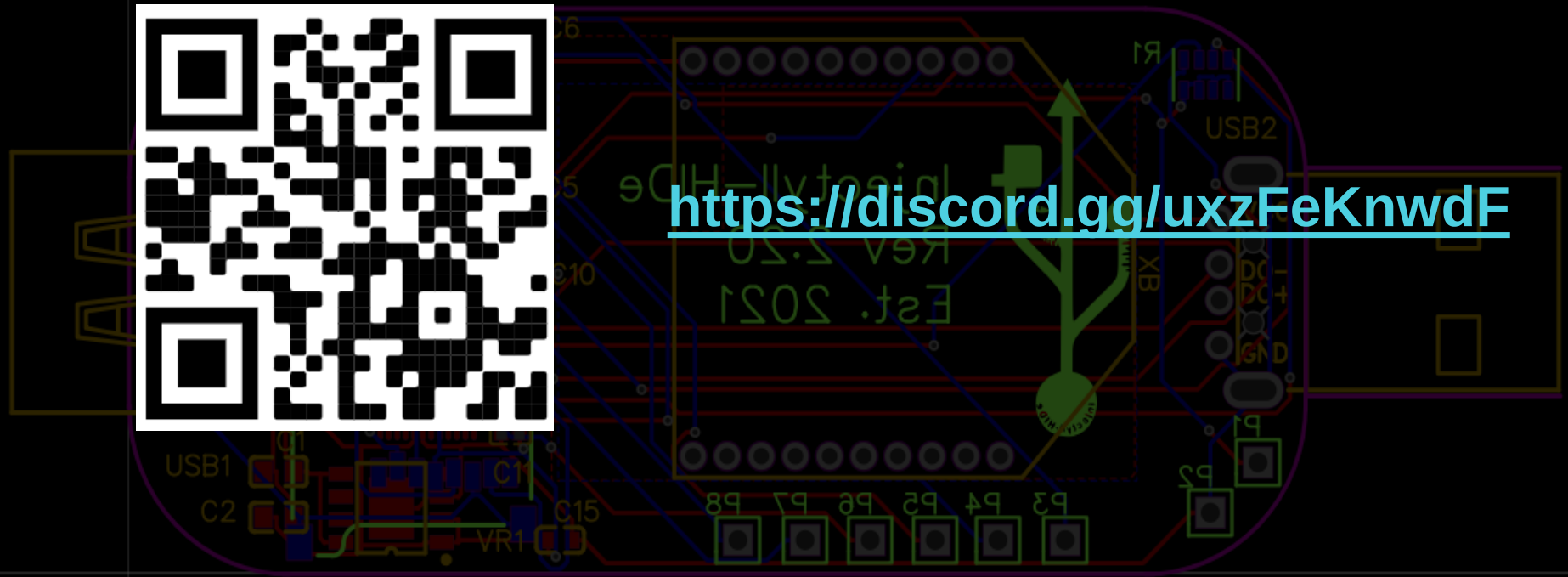
Contact Twitter

- **Jonathan Fischer**
  - **Twitter: @c4m0ufl4g3**
- **Jeremy Miller**
  - **Twitter: @allTheJurm**
- **Injectyll-HIDe**
  - **Twitter: @injectyll_hide**



Contact Discord

https://discord.gg/uxzFeKnwdF



@c4m0ufl4g3

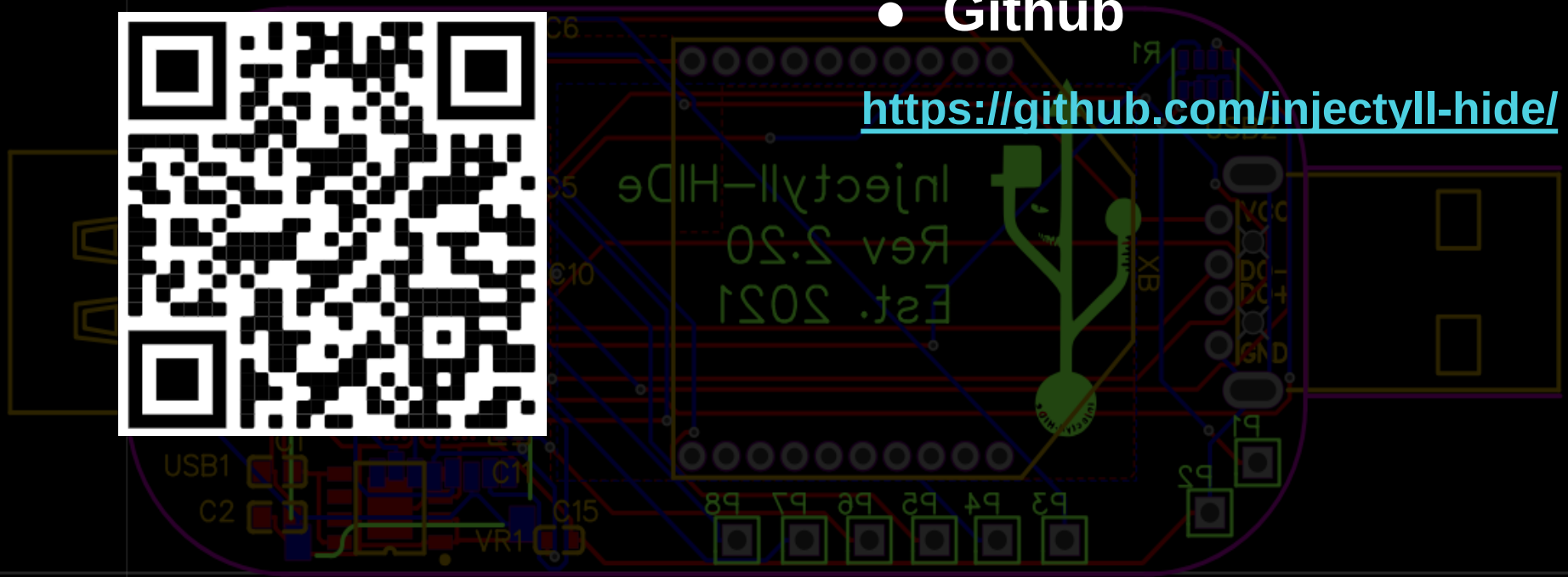
@Injectyll_HIDe

@allTheJurm

Contribute

- **Github**

https://github.com/injectyll-hide/



Come see us!

- **Hardware Hacking Village**
  - **Friday (8/12/22) @ 15:00:**
    Injectyll-HIDe: Build-Your-Own Hardware Implants
- **DEF CON Demo Labs**
  - **Saturday (8/13/22) @ 10:00 - 11:55:**
    Injectyll-HIDe: Pushing the Future of Hardware Implants to the Next Level

@c4m0ufl4g3
@Injectyll_HIDe
@allTheJurm