INJECTYLL-HIDE

Pushing the Future of Hardware Implants to the Next Level

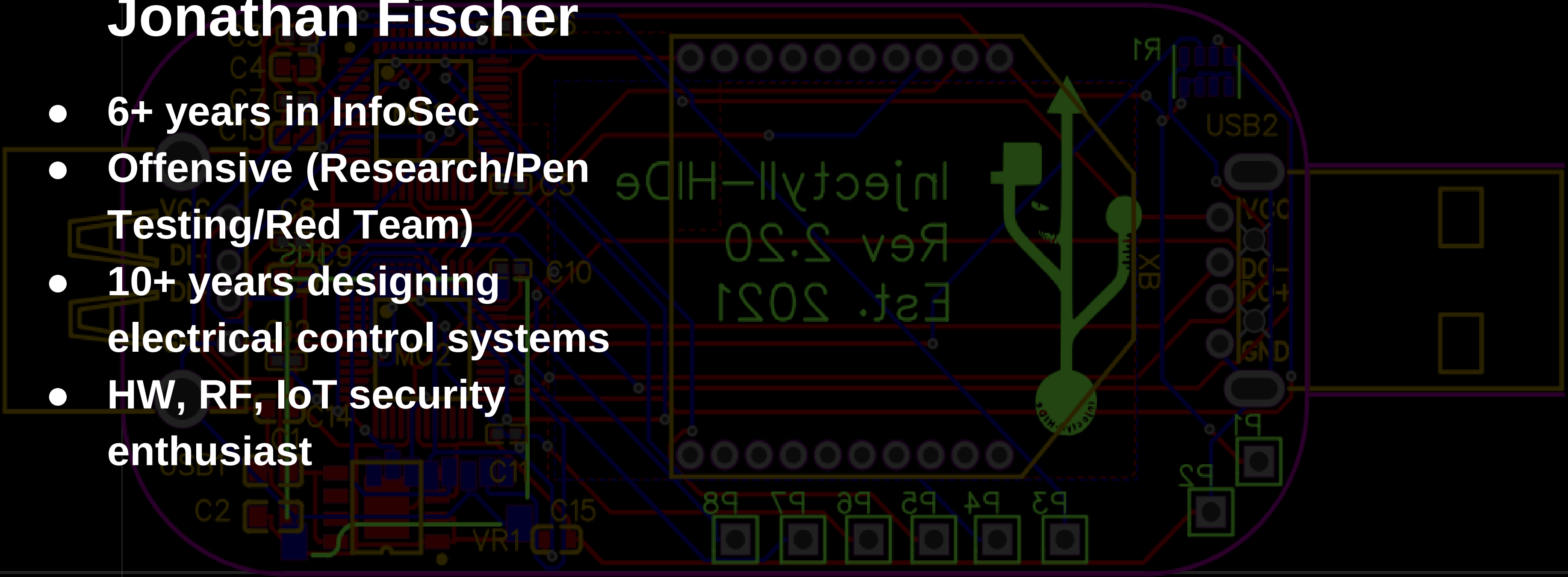
Jonathan Fischer, Jeremy Miller

@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

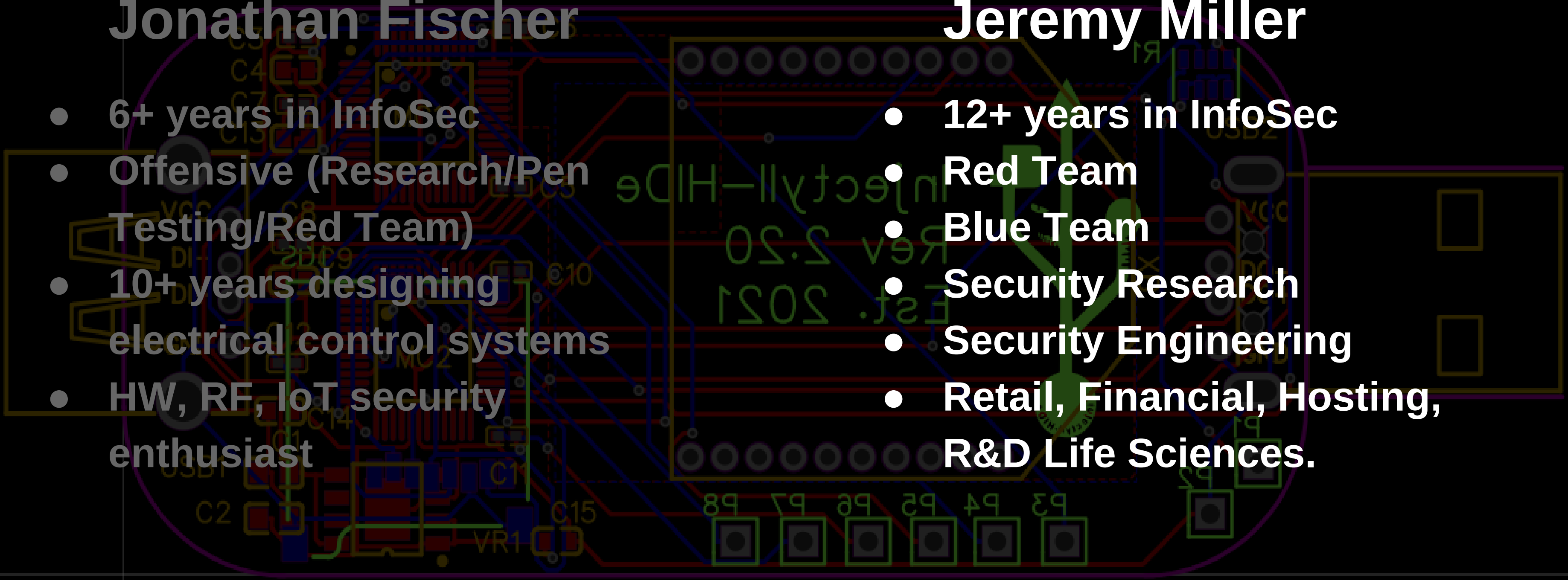
Who are we?



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

@c4m0ufl4g3

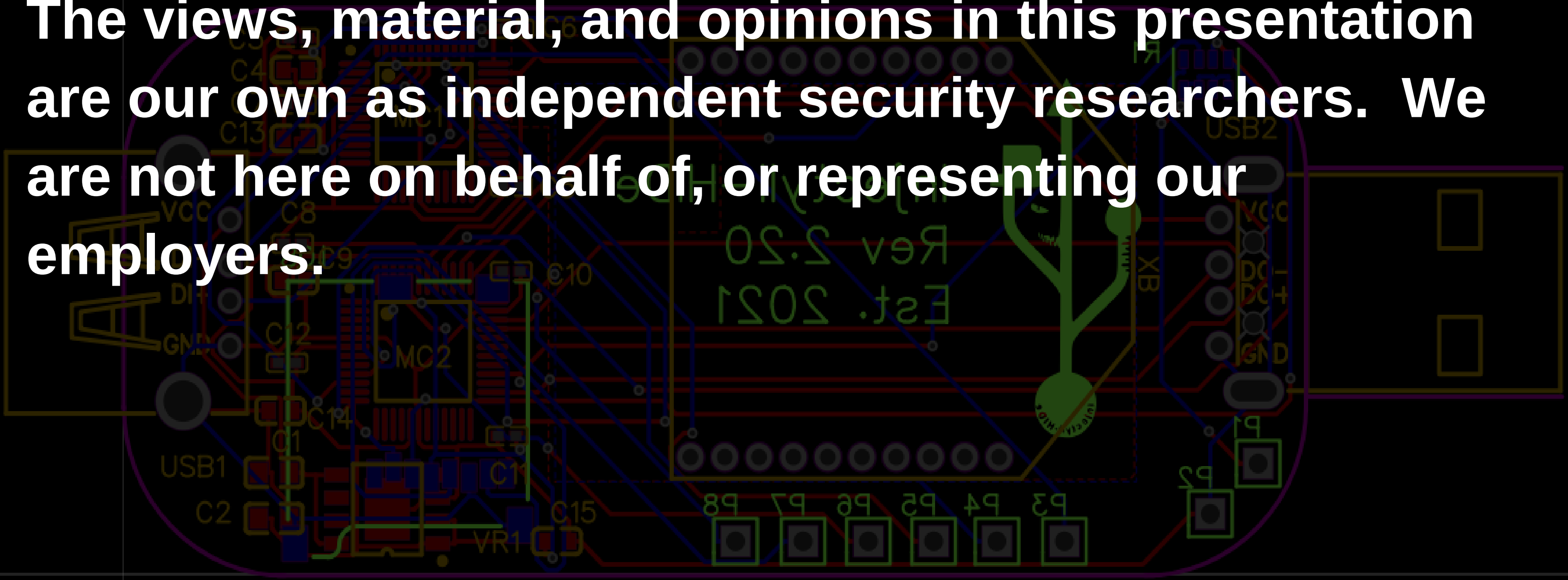
Jeremy Miller

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

@allTheJurm

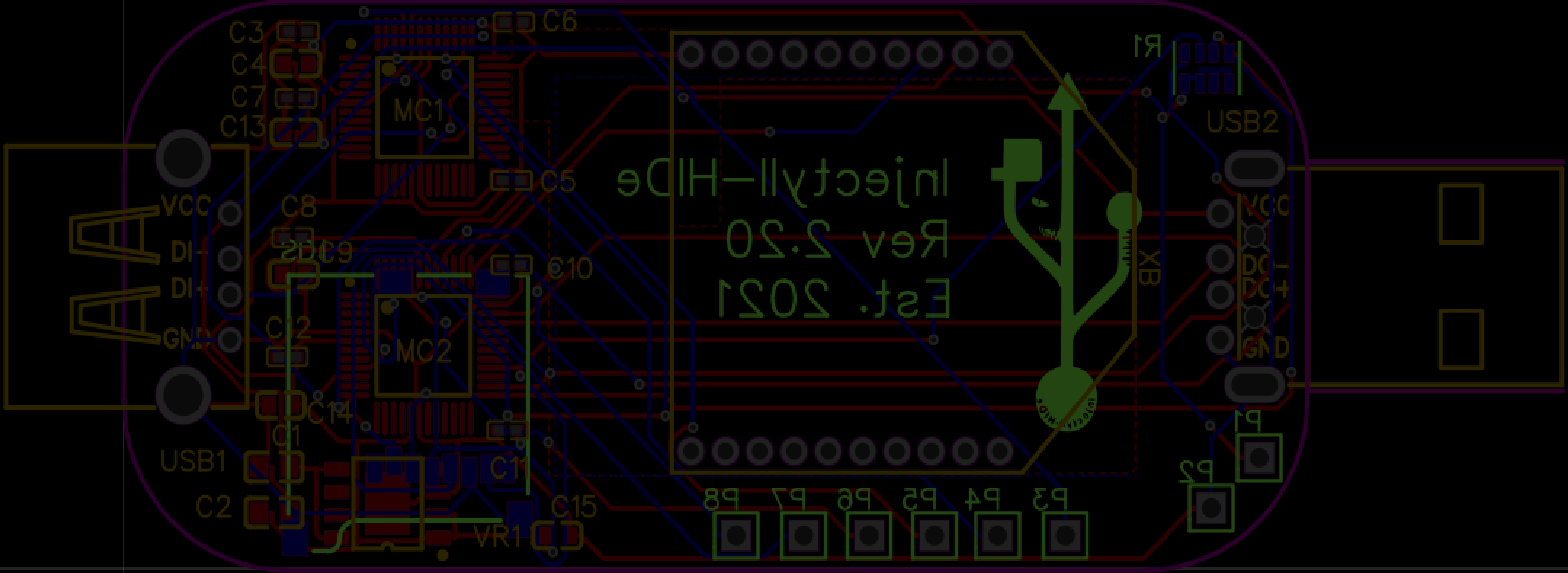
@Injectyll_HIDe

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.

Hardware Attacks. Why?



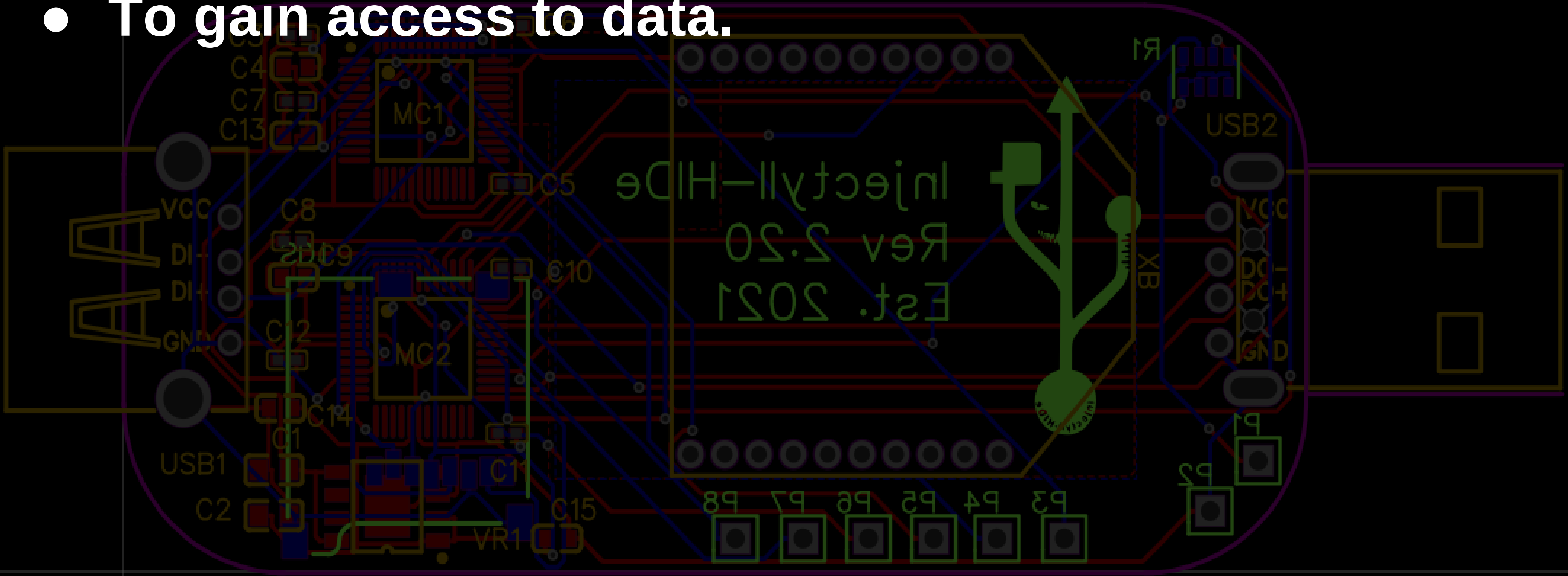
@c4m0ufl4g3

@Injectyll_HIDe

@allTheJurm

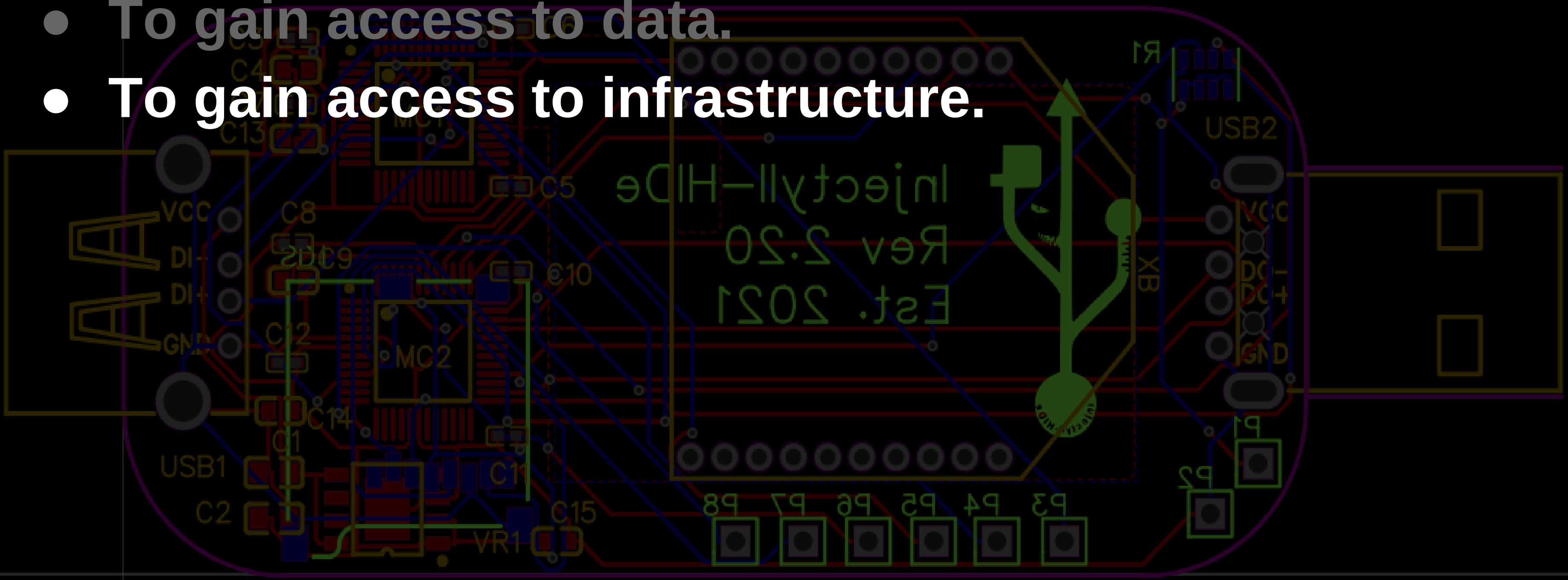
Hardware Attacks. Why?

- To gain access to data.



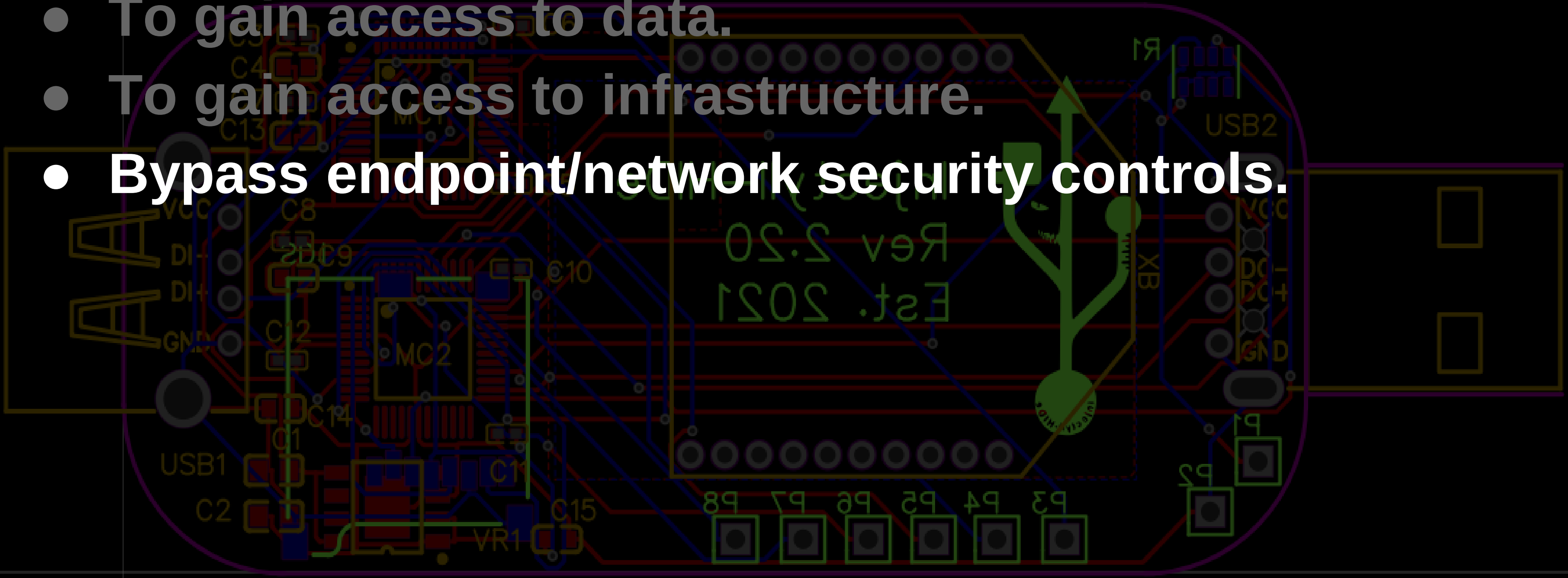
Hardware Attacks. Why?

- To gain access to data.
- **To gain access to infrastructure.**

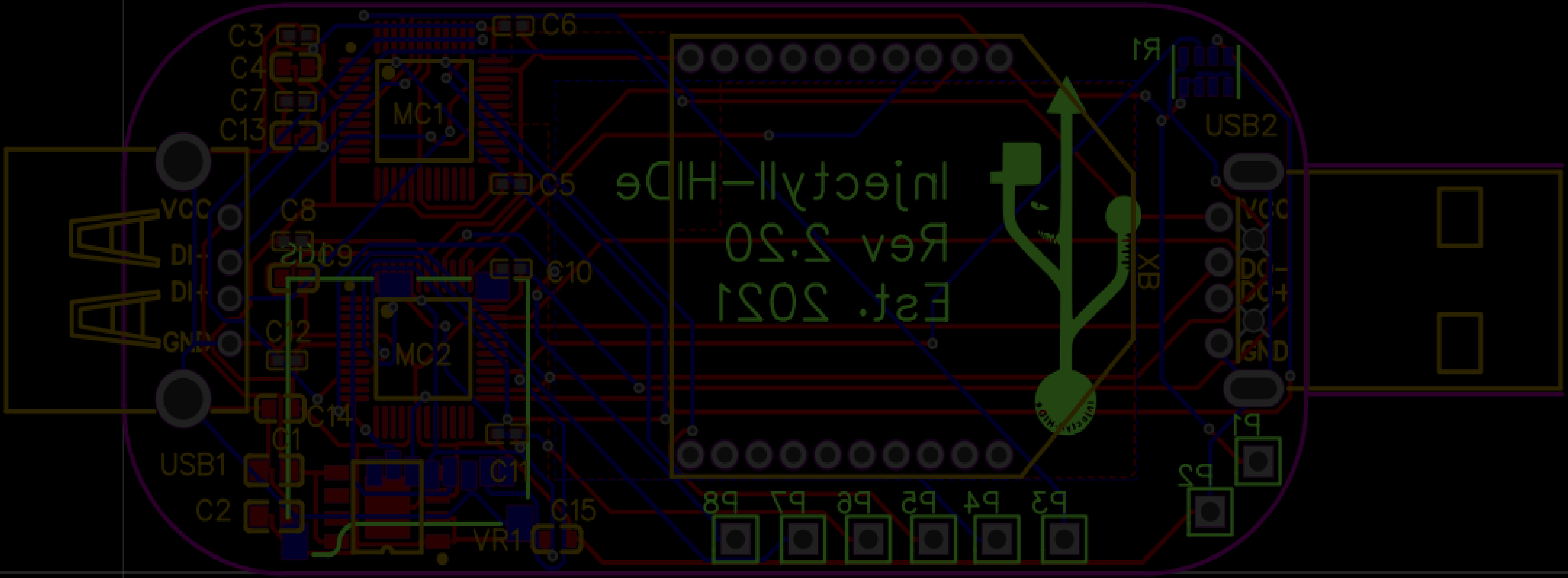


Hardware Attacks. Why?

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



Why create our own?



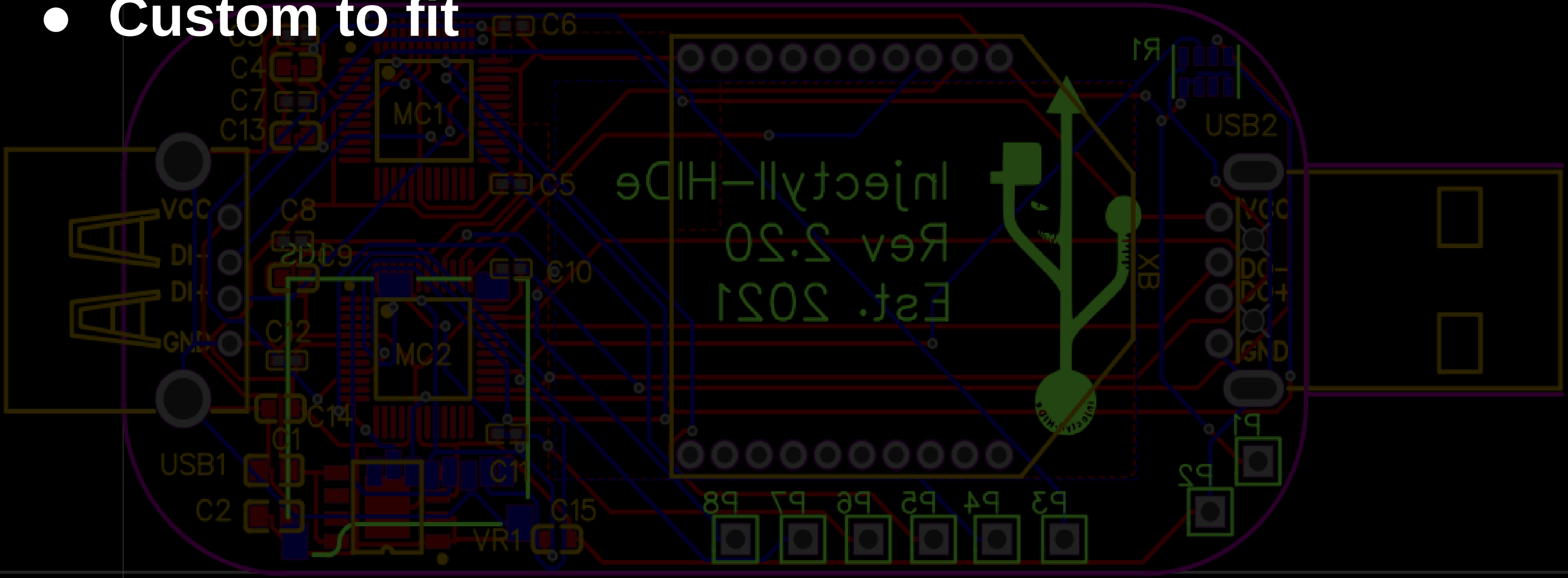
@c4m0ufl4g3

@allTheJurm

@Injectyll_HIDe

Why create our own?

- **Custom to fit**

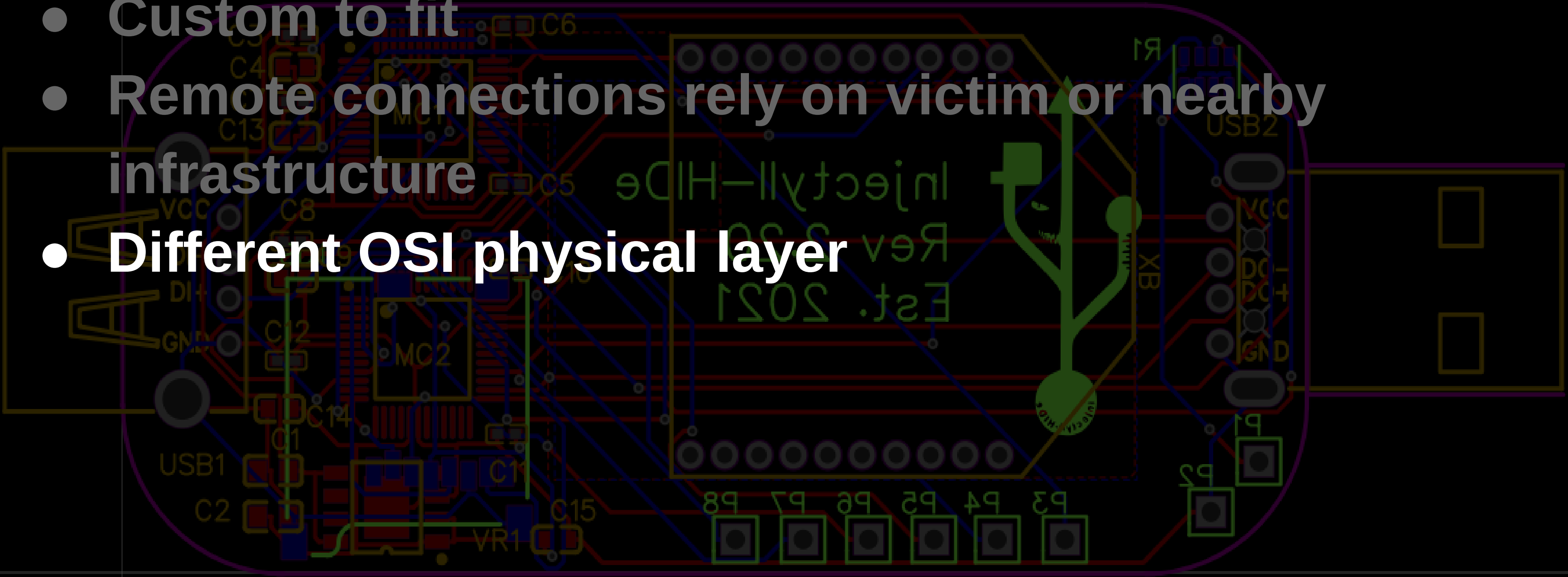


Why create our own?

- 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**

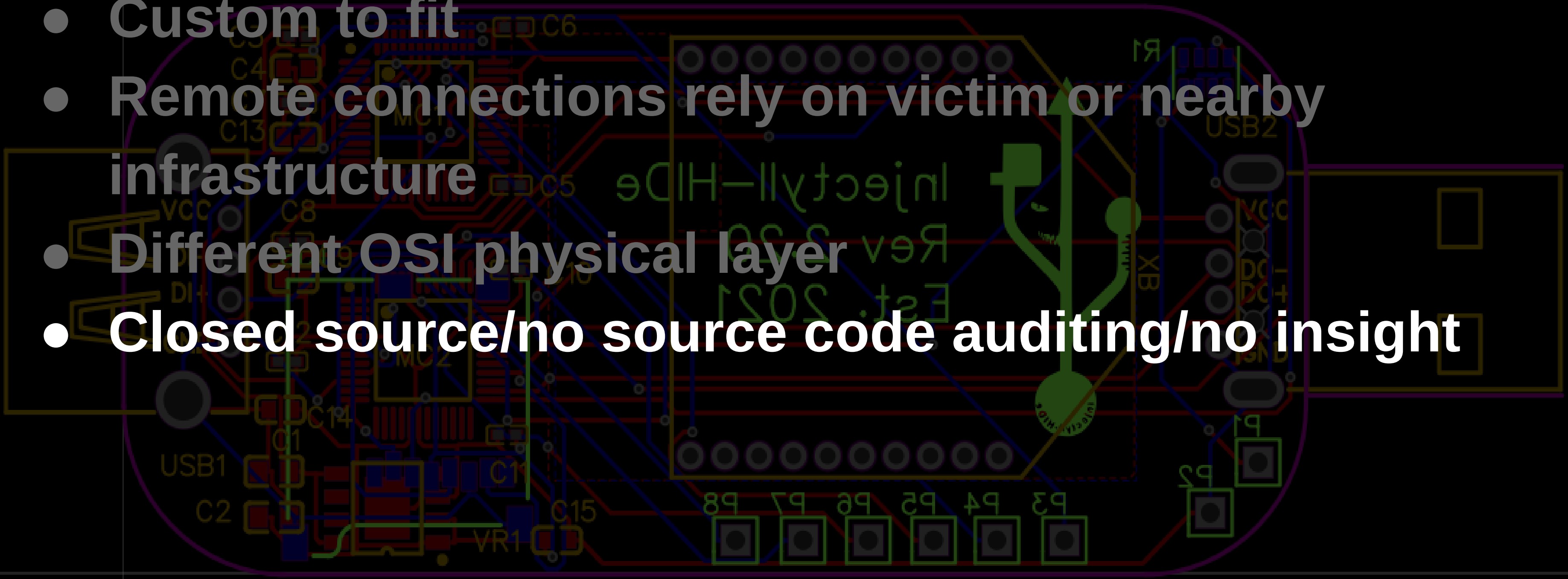


@c4m0ufl4g3

@Injectyll_HIDe

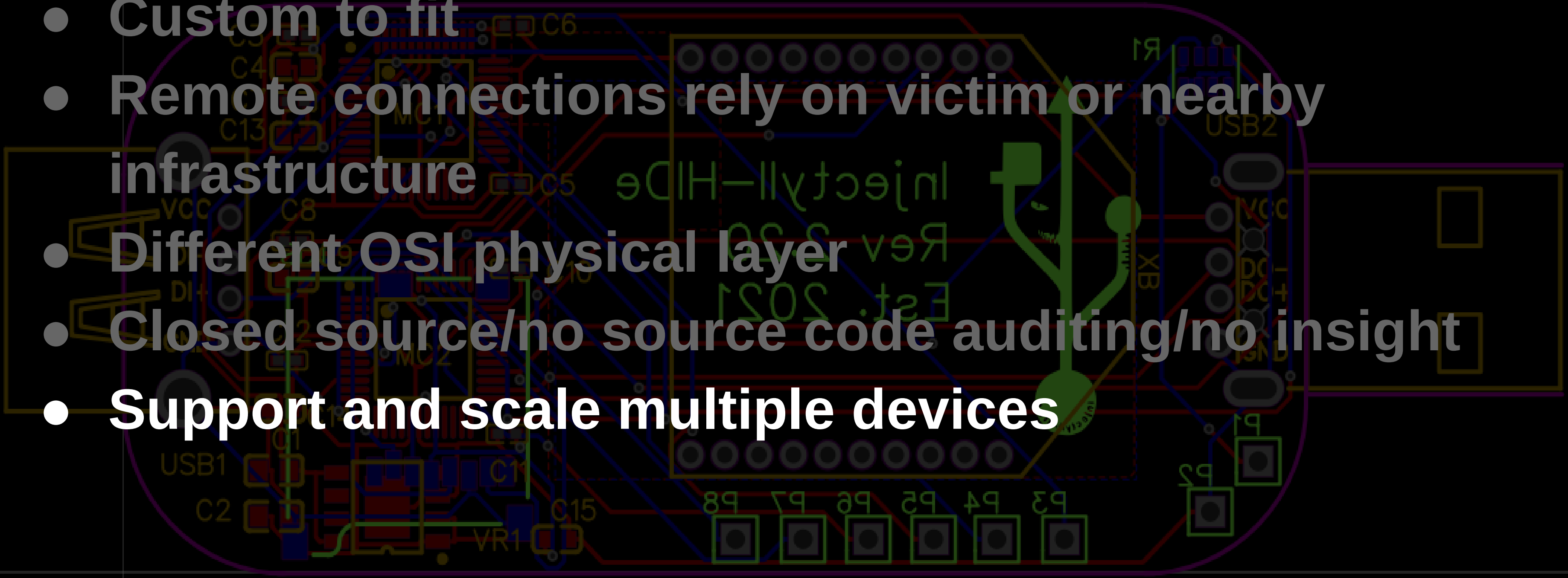
@allTheJurm

Why create our own?



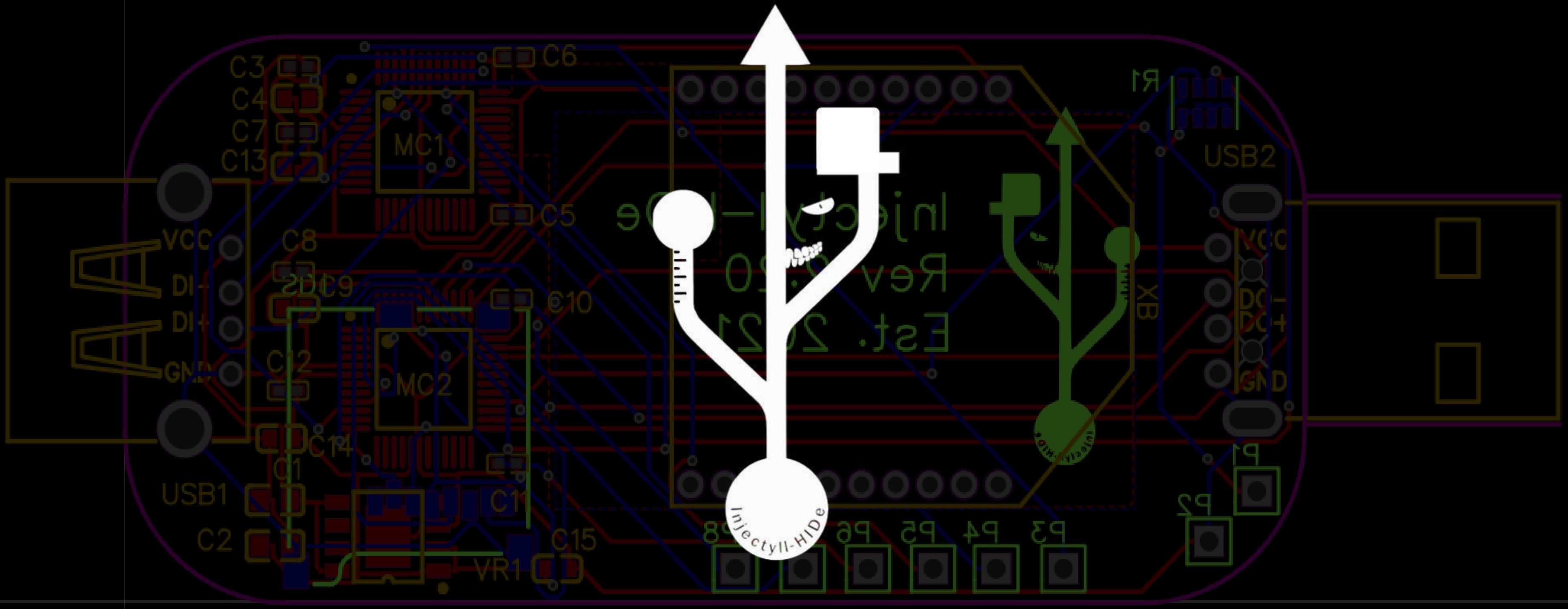
- Custom to fit
- Remote connections rely on victim or nearby infrastructure
- Different OSI physical layer
- **Closed source/no source code auditing/no insight**

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

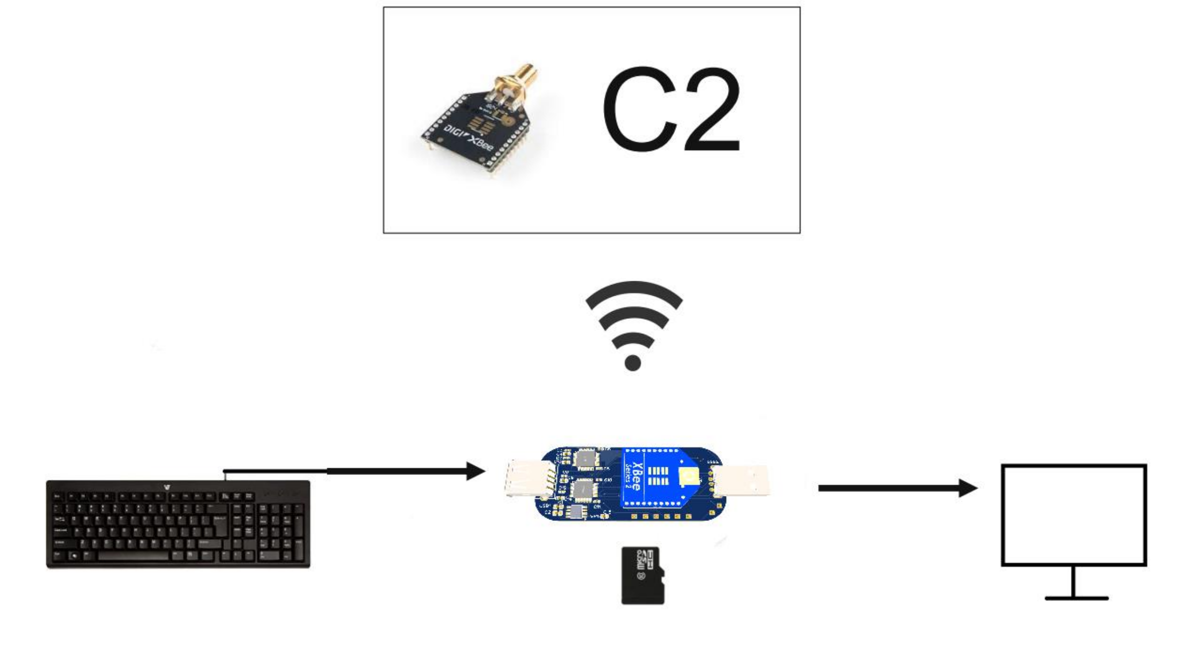


@c4m0ufl4g3

@allTheJurm

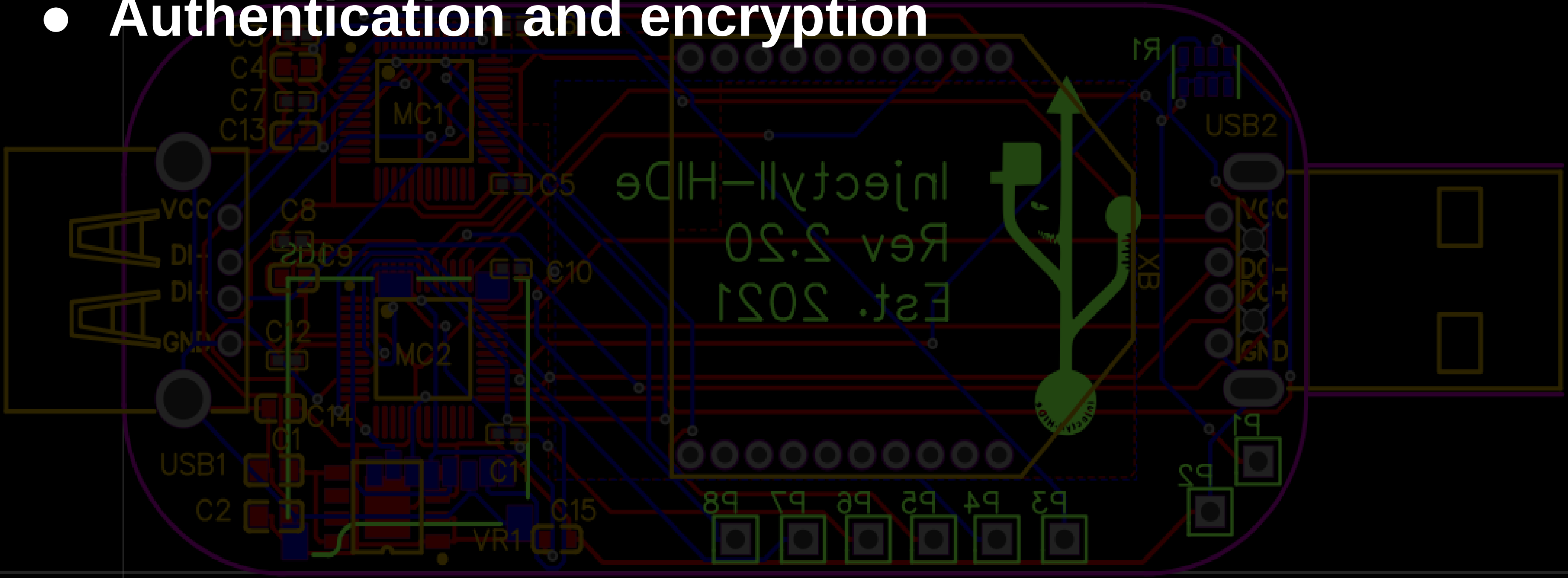
@Injectyll_HIDe

PCB Layout



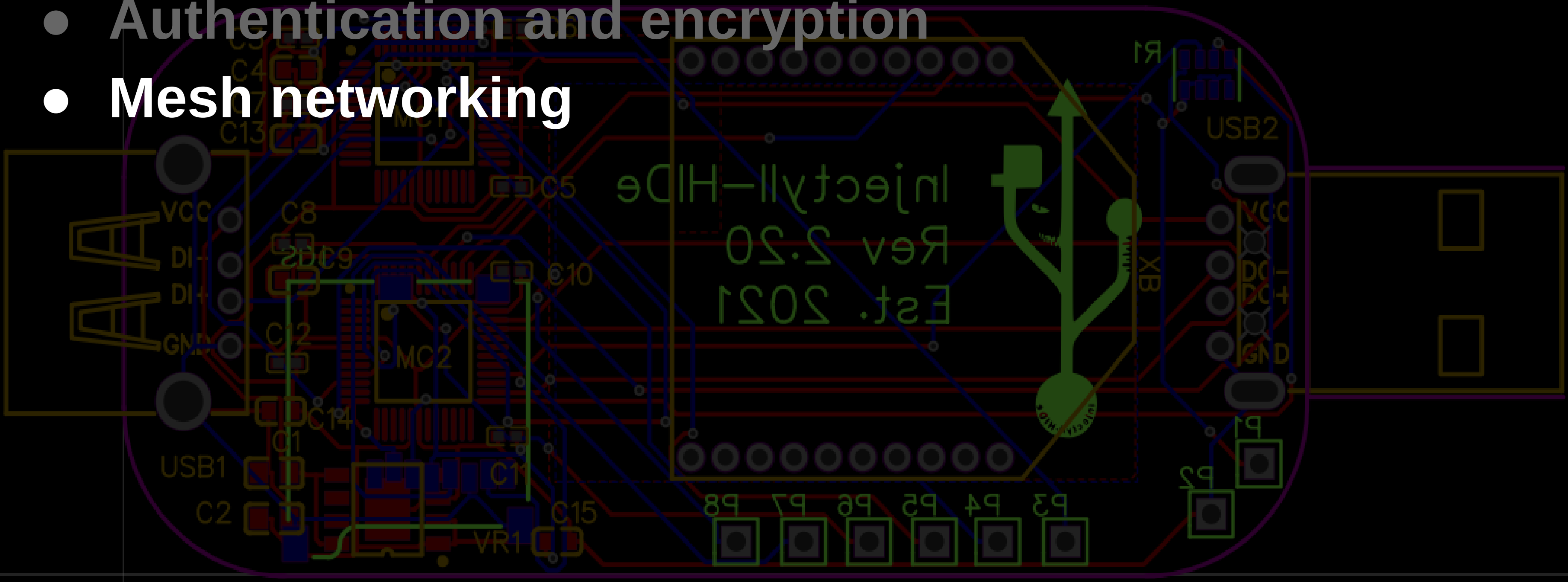
Covert, scalable network

- **Authentication and encryption**



Covert, scalable network

- Authentication and encryption
- **Mesh networking**



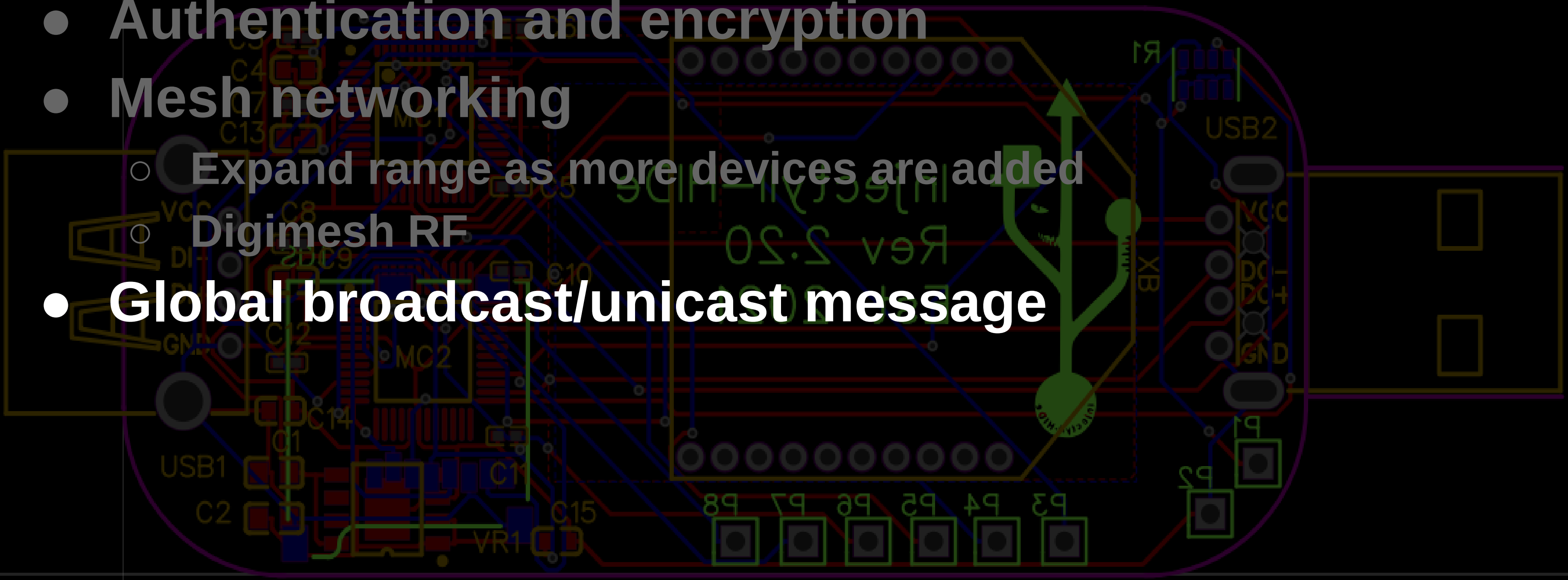
Covert, scalable network

- 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



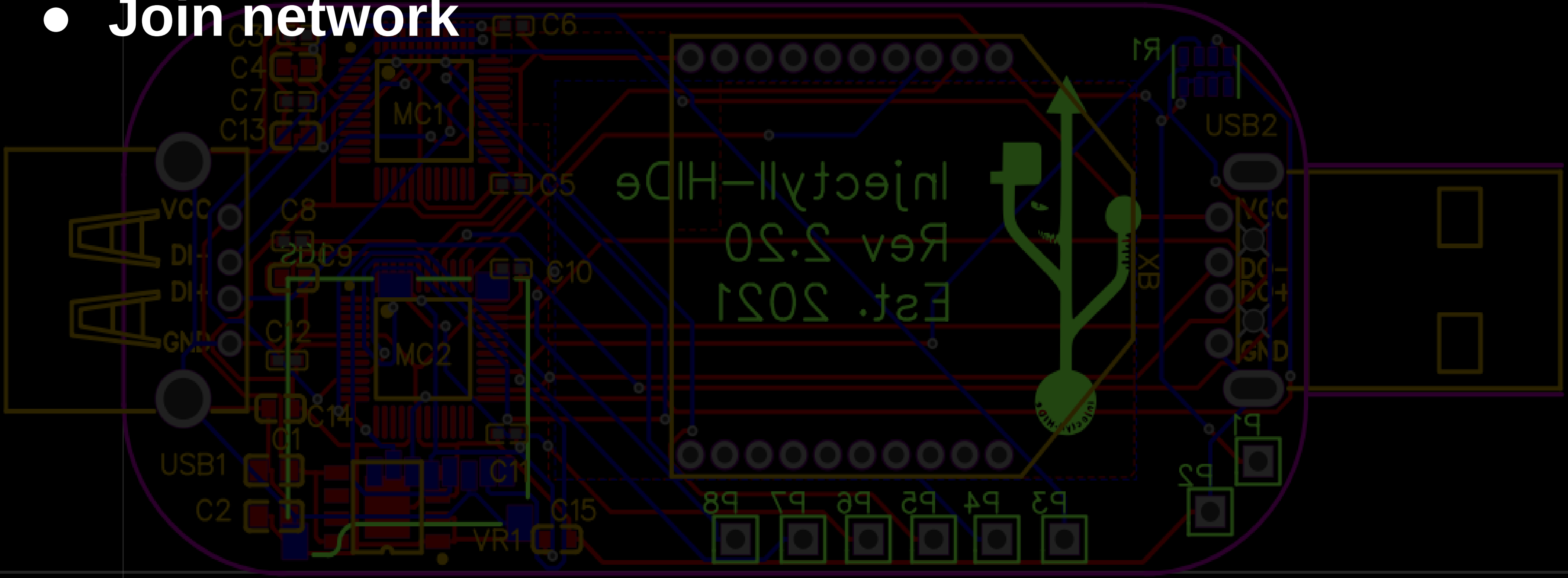
- Authentication and encryption
- Mesh networking
  - Expand range as more devices are added
  - Digimesh RF
- **Global broadcast/unicast message**

Covert, scalable network

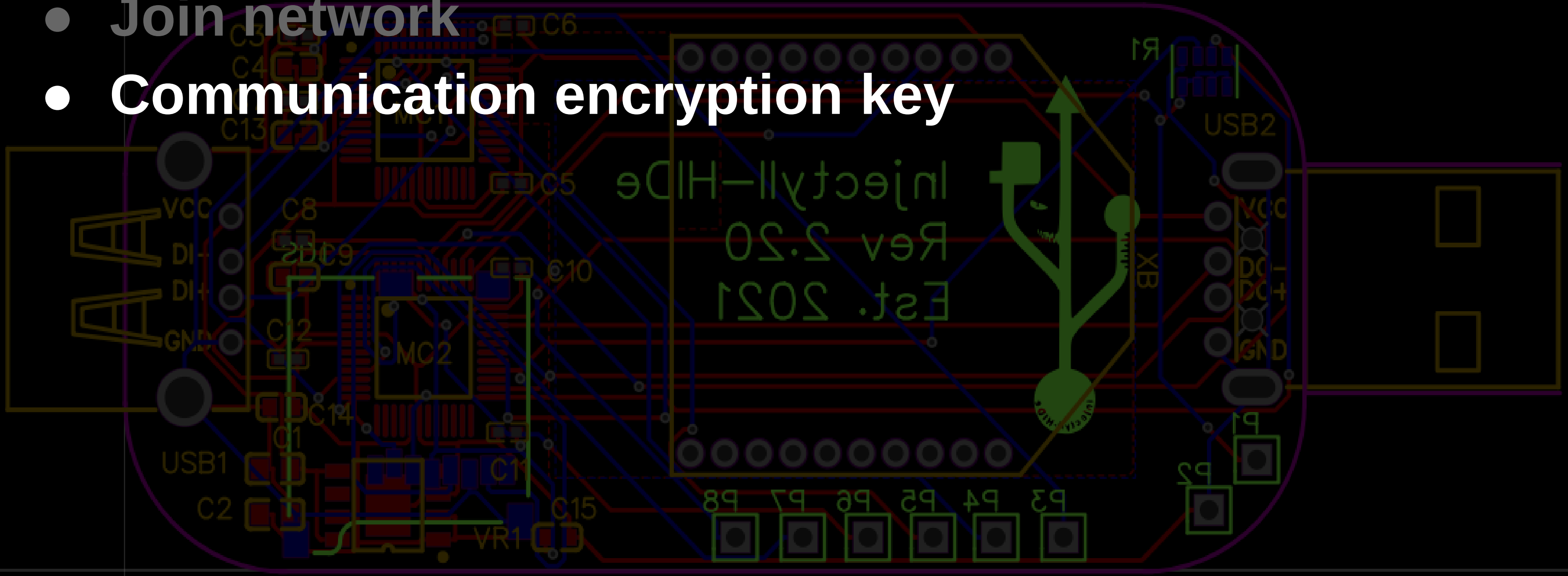
- Authentication and encryption
- Mesh networking
  - Expand range as more devices are added
  - Digimesh RF
- Global broadcast/unicast message
- Range up to:
  - 200 - 4,000 ft. (Std version)
  - 300 ft - 2 mi (Pro version)

Communication interlocks

- **Join network**



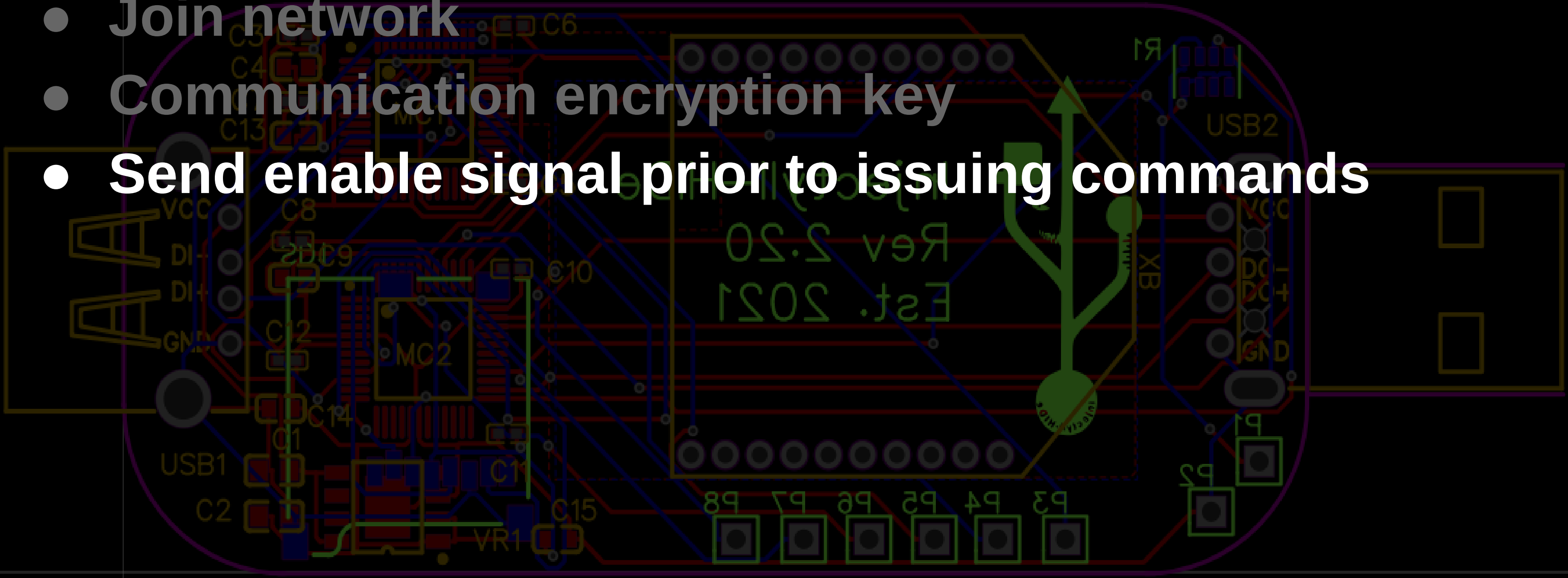
Communication interlocks



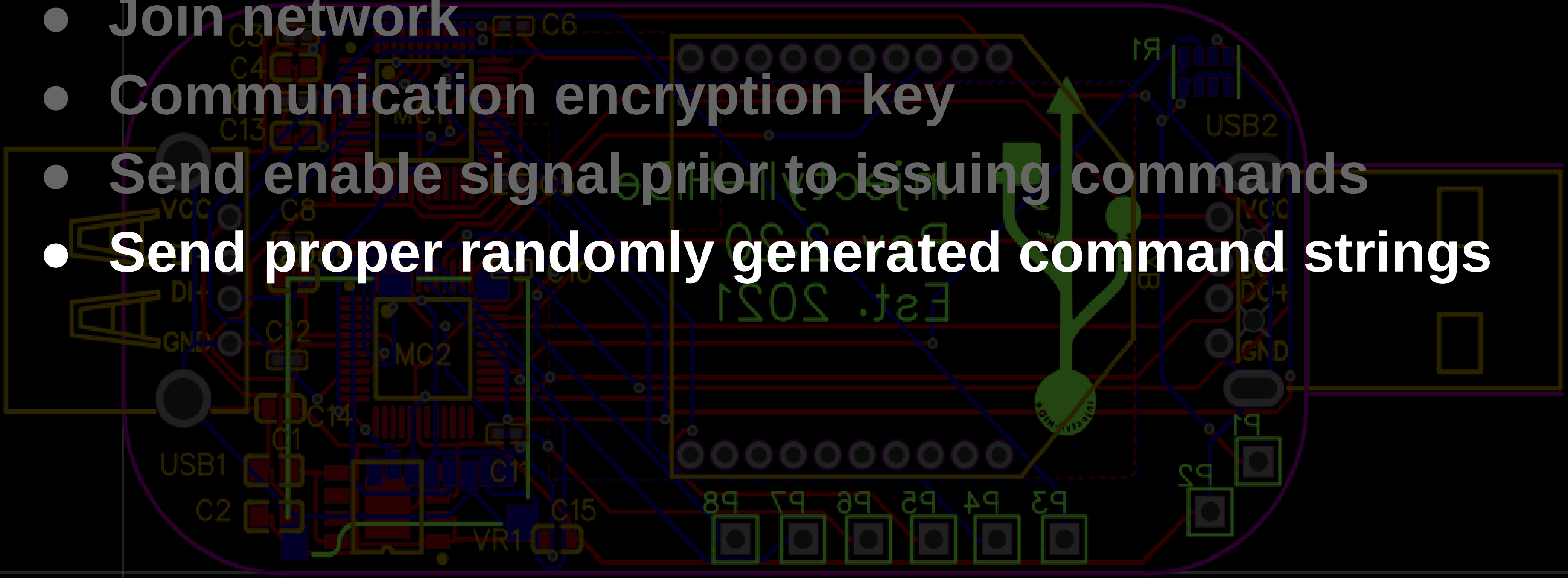
- Join network
- **Communication encryption key**

Communication interlocks

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



Communication interlocks

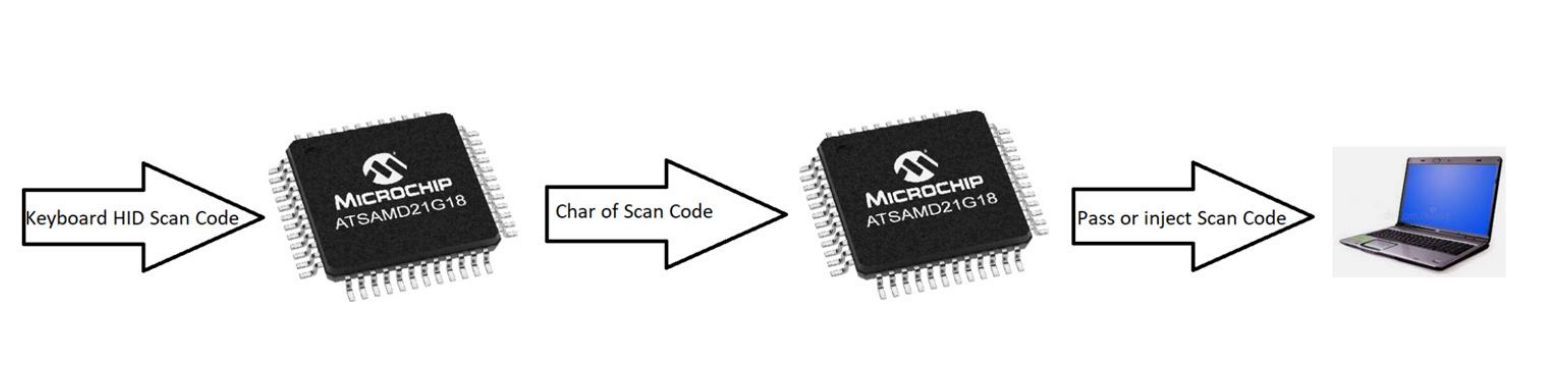


- Join network
- Communication encryption key
- Send enable signal prior to issuing commands
- **Send proper randomly generated command strings**

Keystroke injection/sniffing/recording

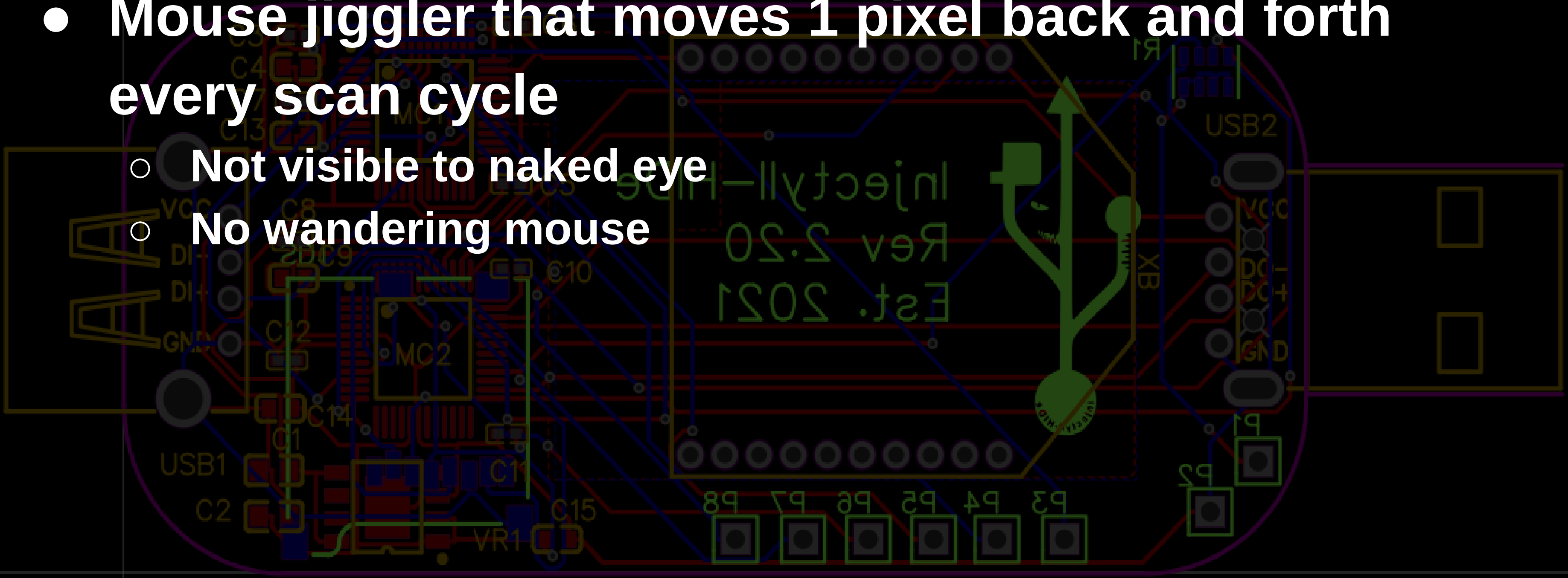
Started from USB Metamorph

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

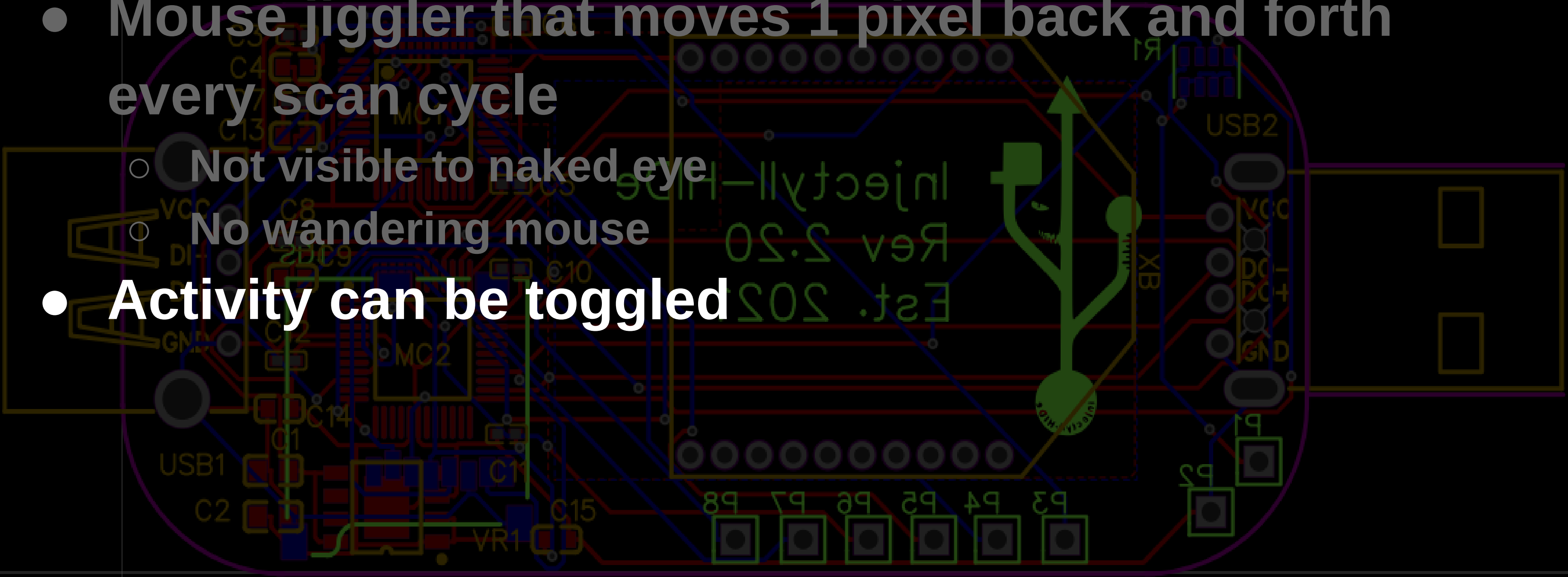


Insomnia Mode

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



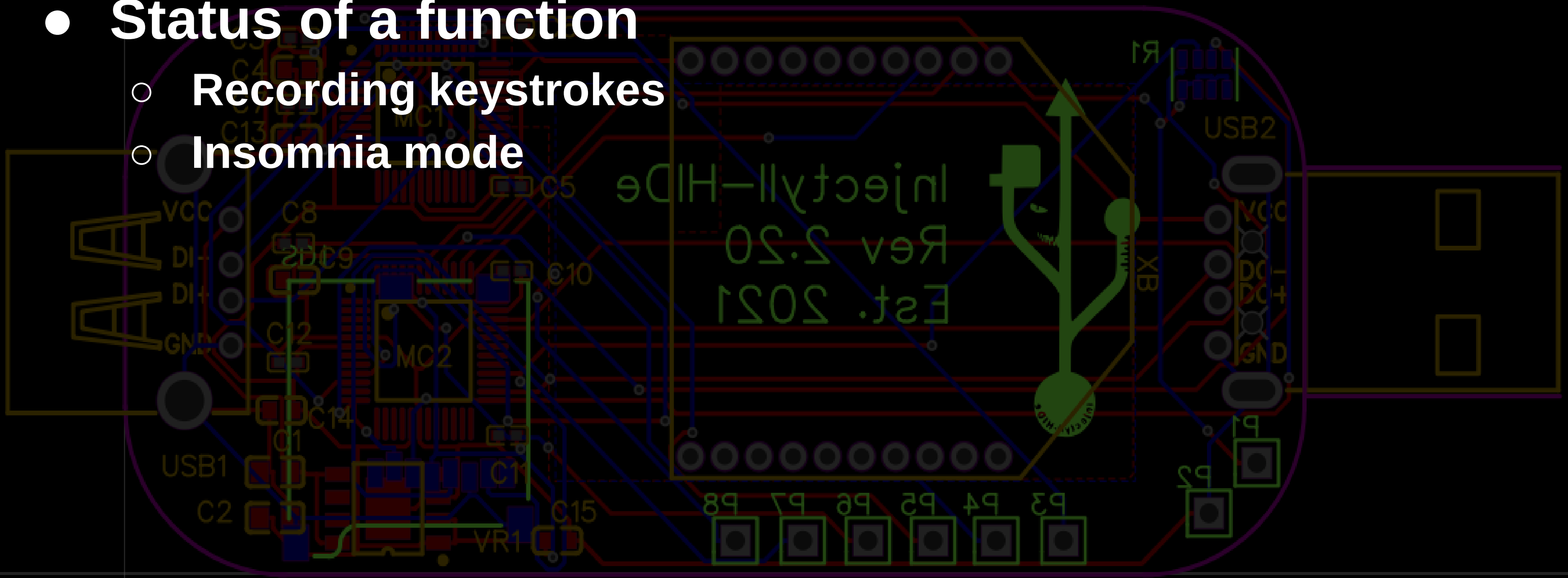
Insomnia Mode



- 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**

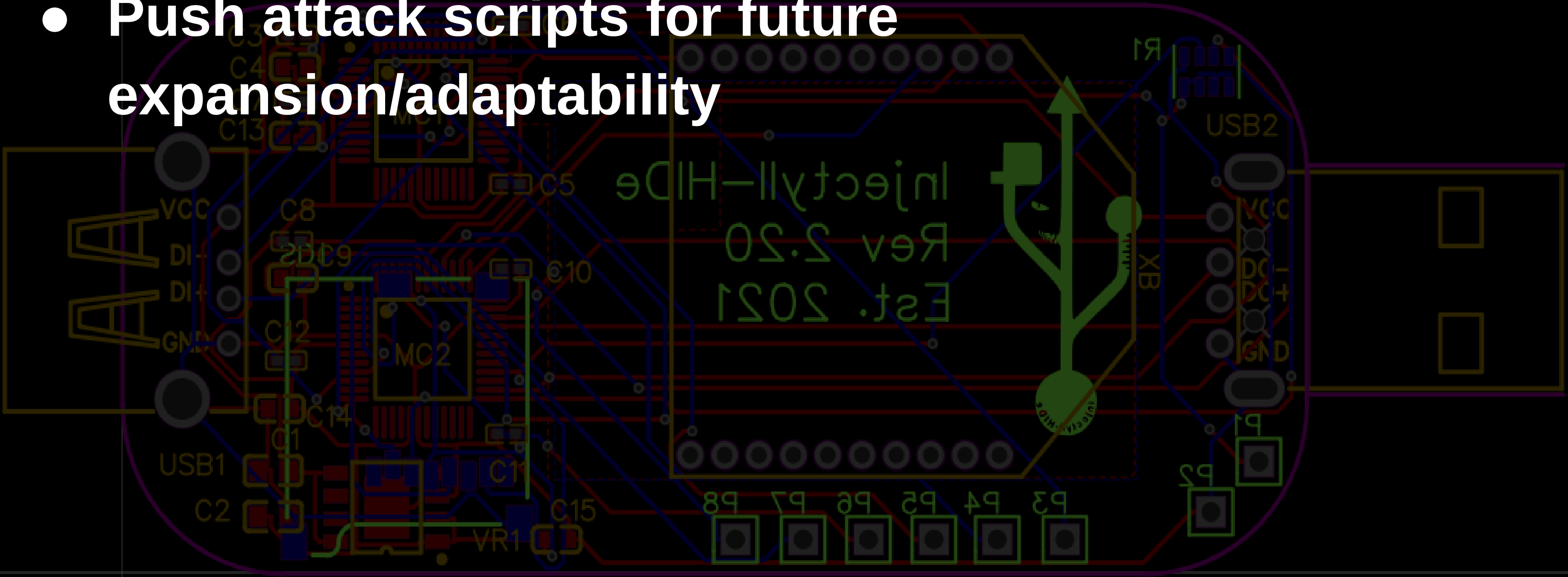


Status Update

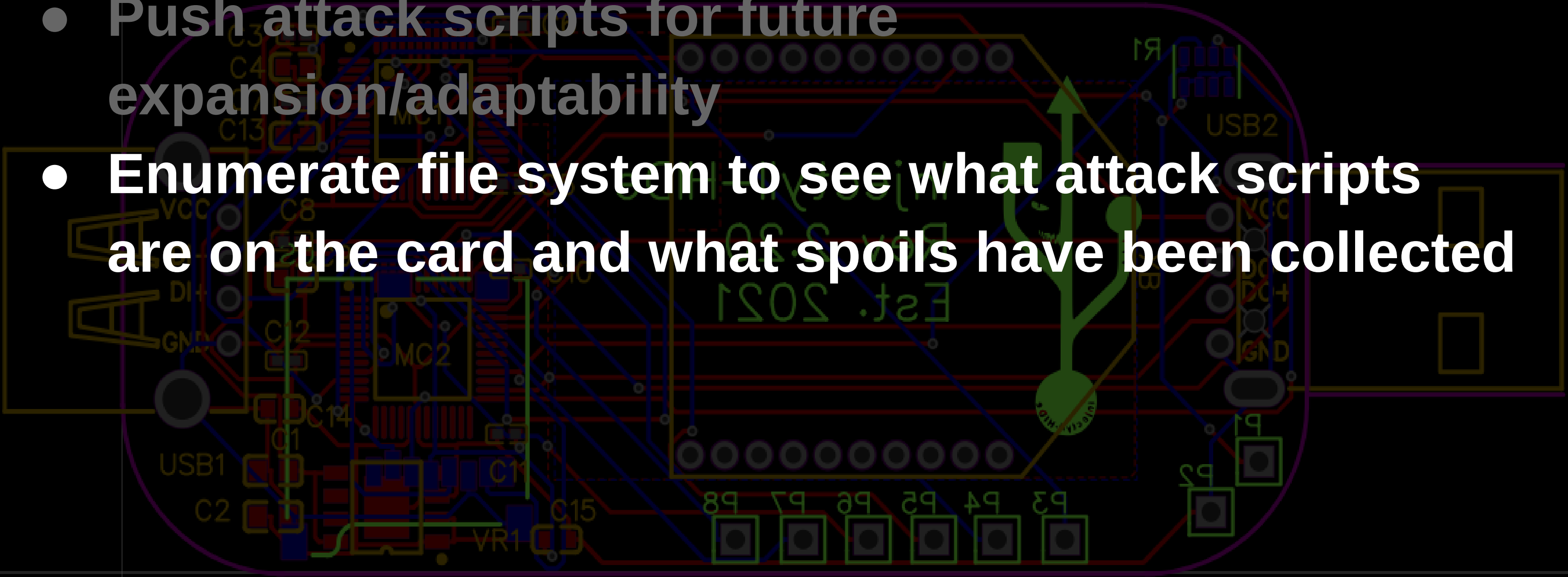
- Status of a function
  - Recording keystrokes
  - Insomnia mode
- Time elapsed since last key press detected

Storage and memory management

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

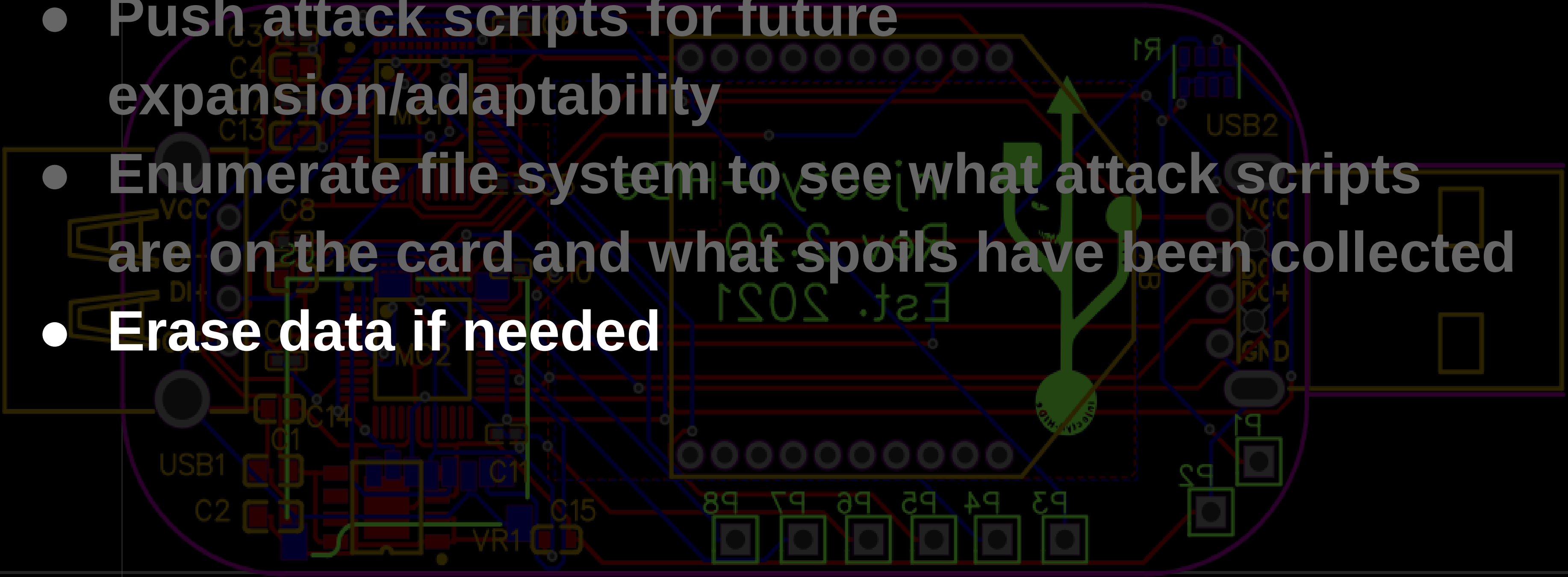


Storage and memory management



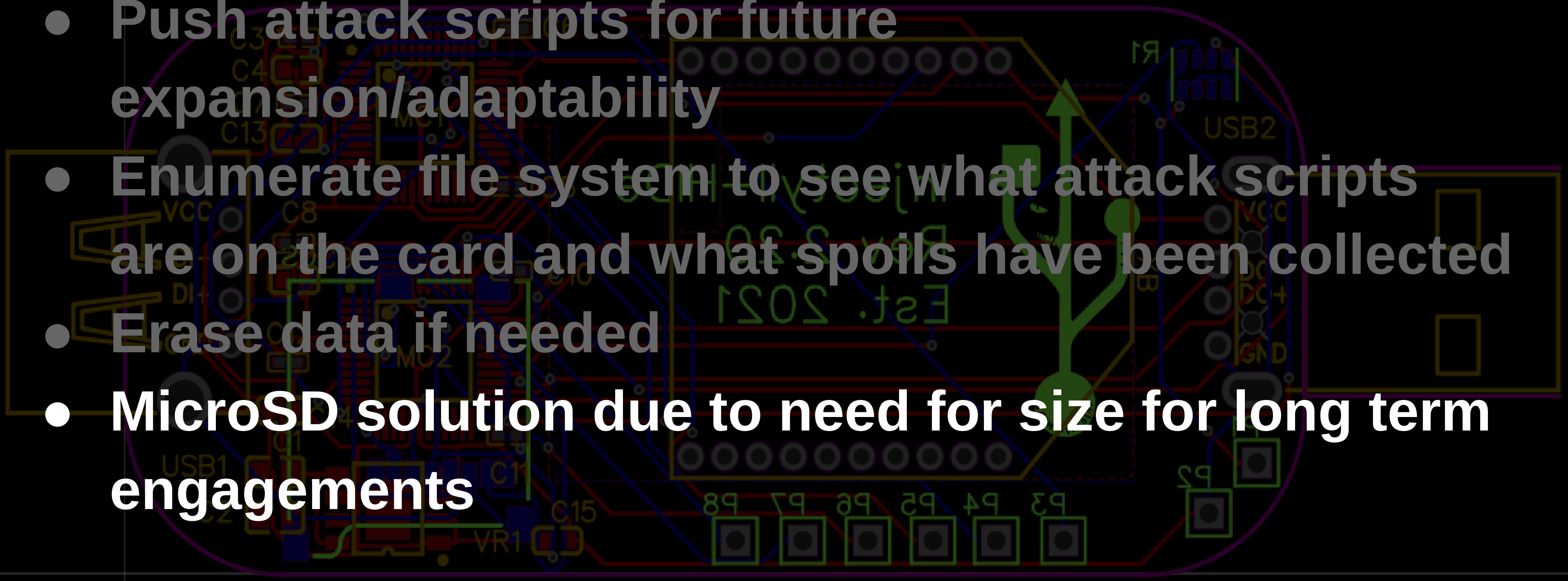
- Push attack scripts for future expansion/adaptability
- Enumerate file system to see what attack scripts are on the card and what spoils have been collected

Storage and memory management



- Push attack scripts for future expansion/adaptability
- Enumerate file system to see what attack scripts are on the card and what spoils have been collected
- **Erase data if needed**

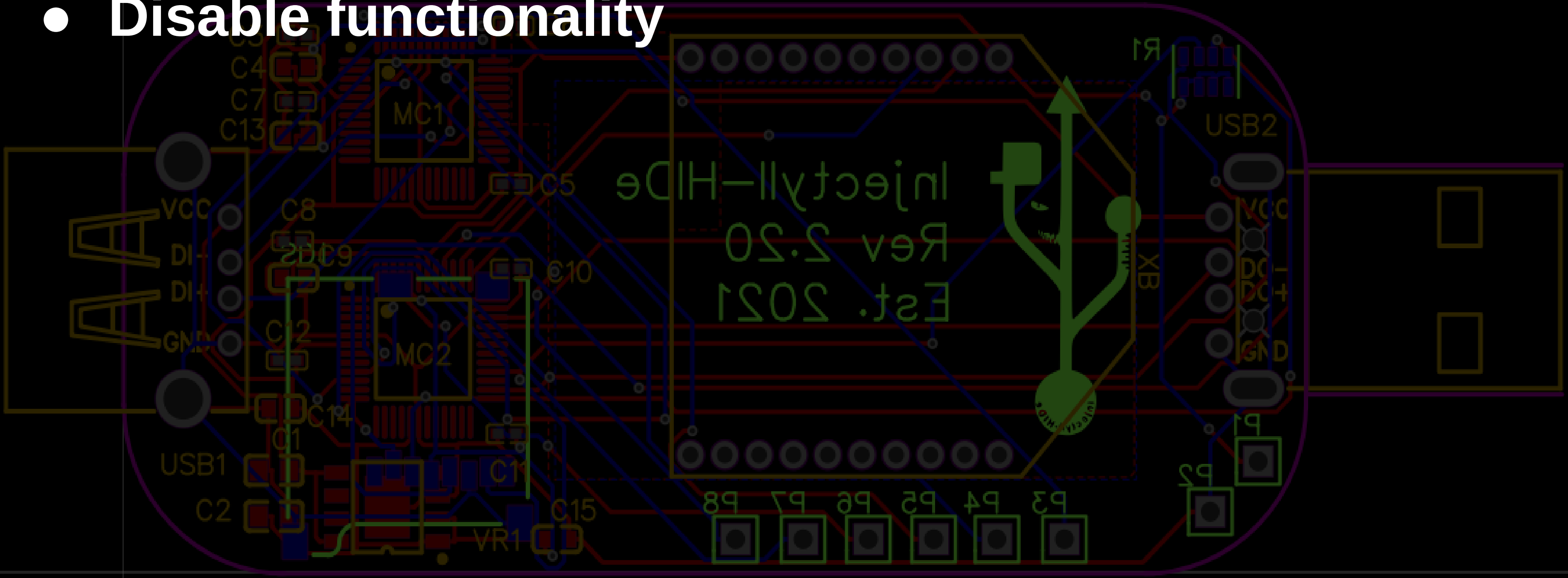
Storage and memory management



- Push attack scripts for future expansion/adaptability
- Enumerate file system to see what attack scripts are on the card and what spoils have been collected
- Erase data if needed
- **MicroSD solution due to need for size for long term engagements**

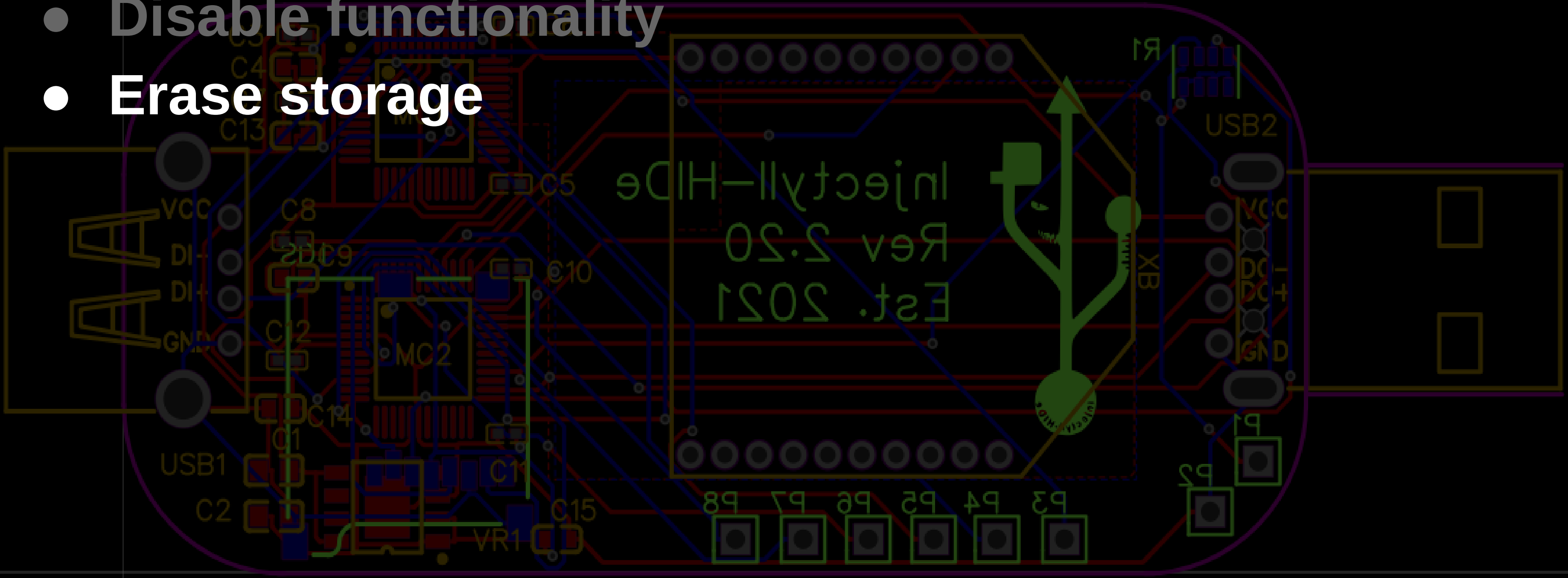
Go Dark mode

- **Disable functionality**



Go Dark mode

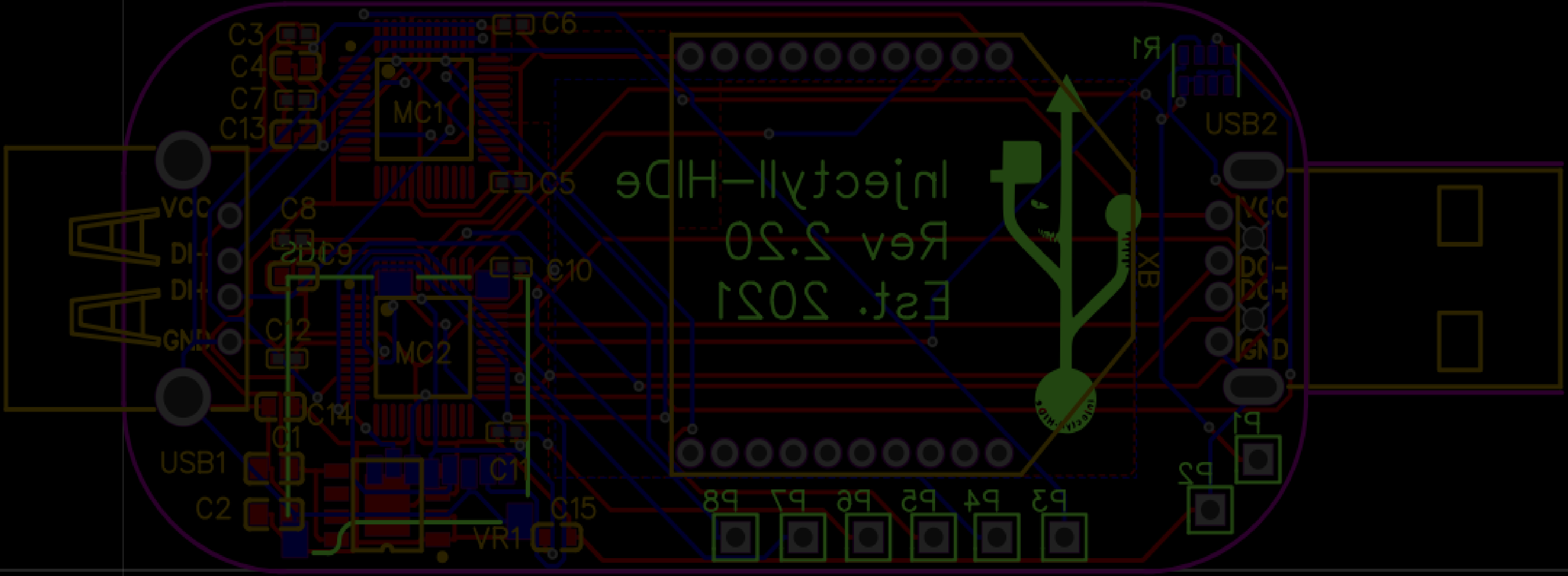
- Disable functionality
- **Erase storage**



Go Dark mode

- Disable functionality
- Erase storage
- Wait for enable message

Custom reverse shell script (Windows)



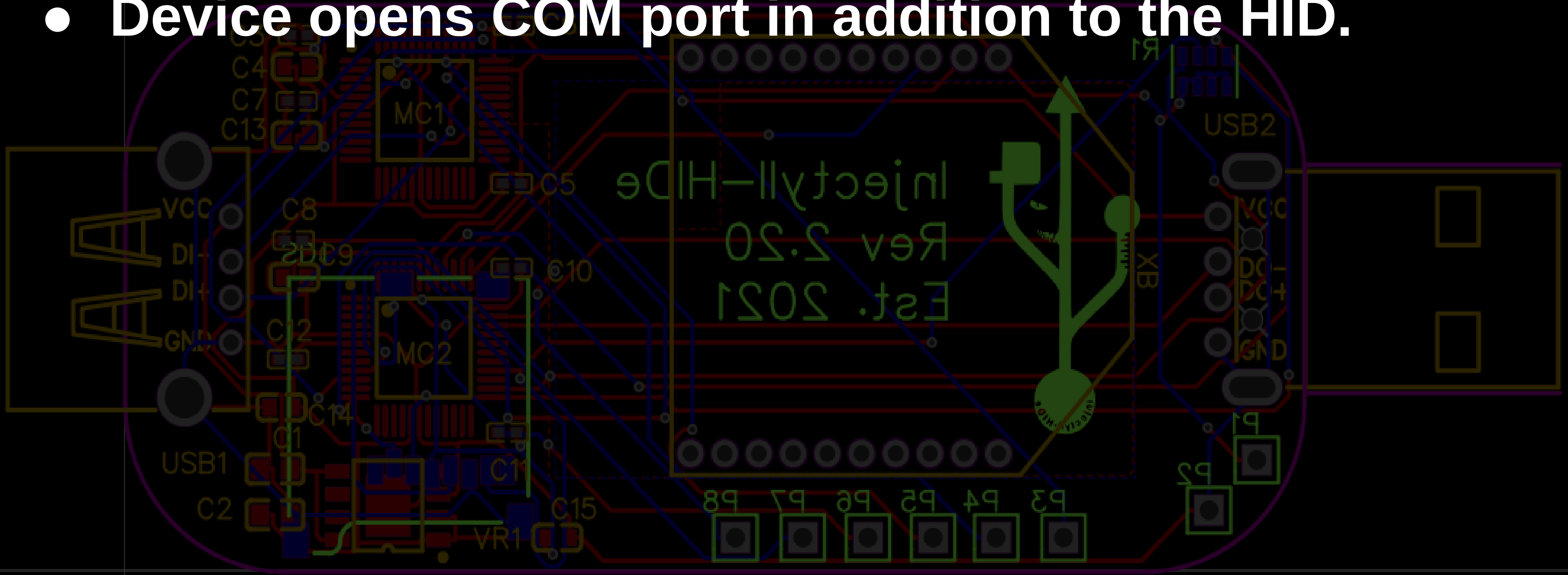
@c4m0ufl4g3

@Injectyll_HIDe

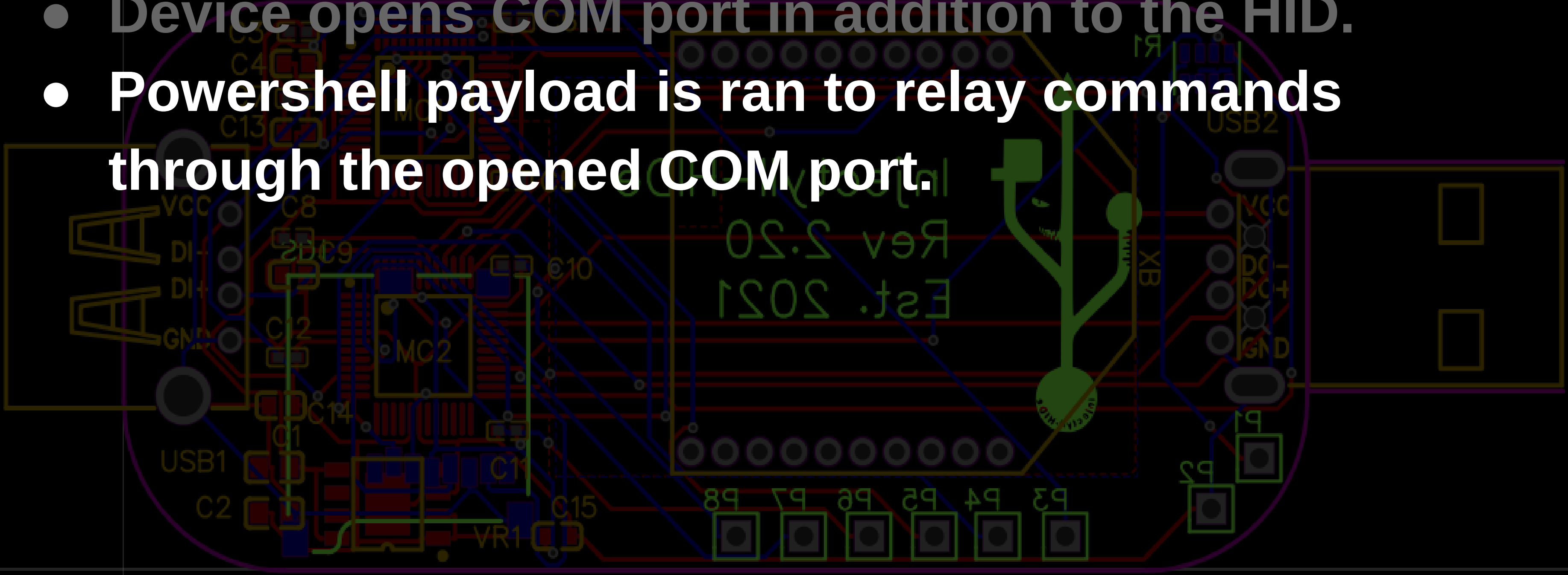
@allTheJurm

Custom reverse shell script (Windows)

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

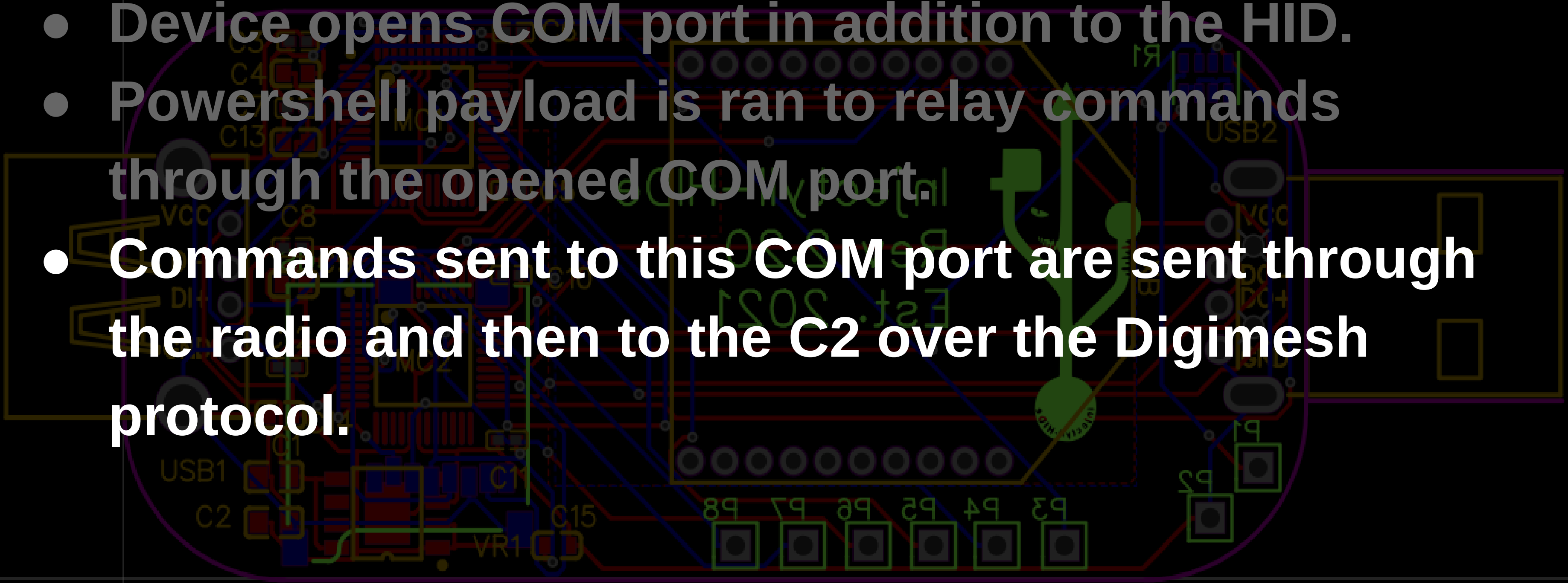


Custom reverse shell script (Windows)



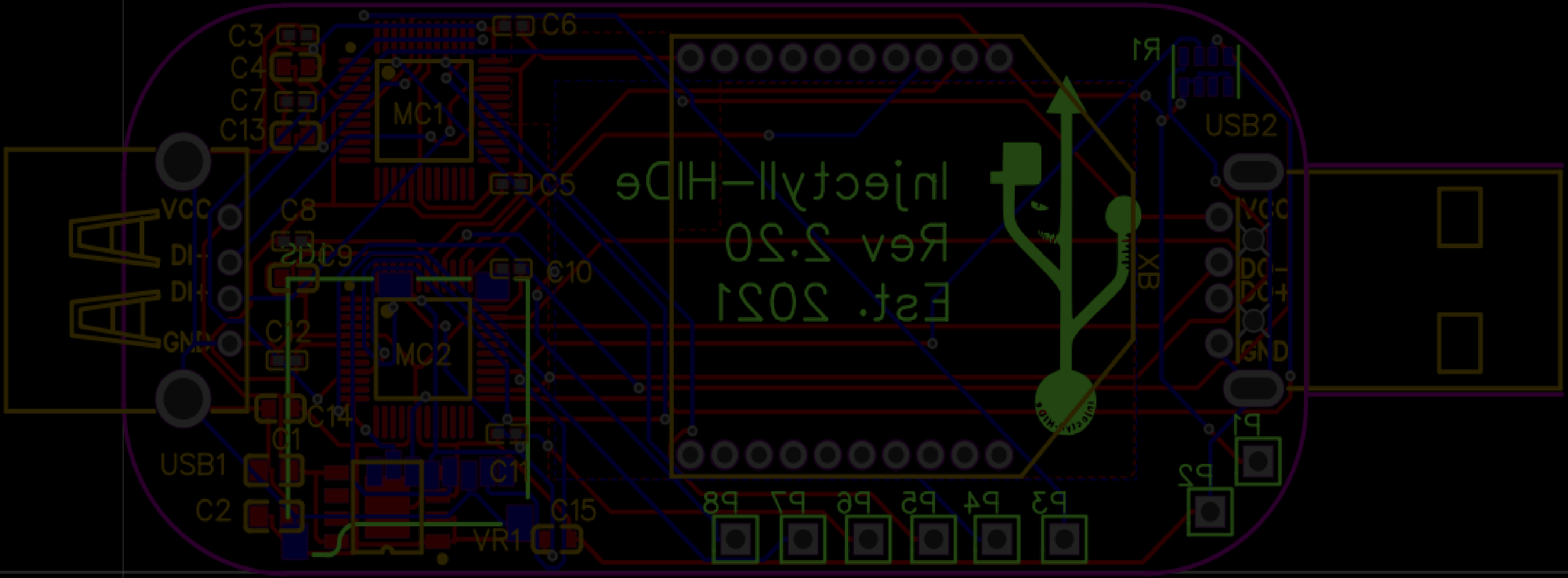
- Device opens COM port in addition to the HID.
- Powershell payload is ran to relay commands through the opened COM port.

Custom 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.**

Custom data exfil script



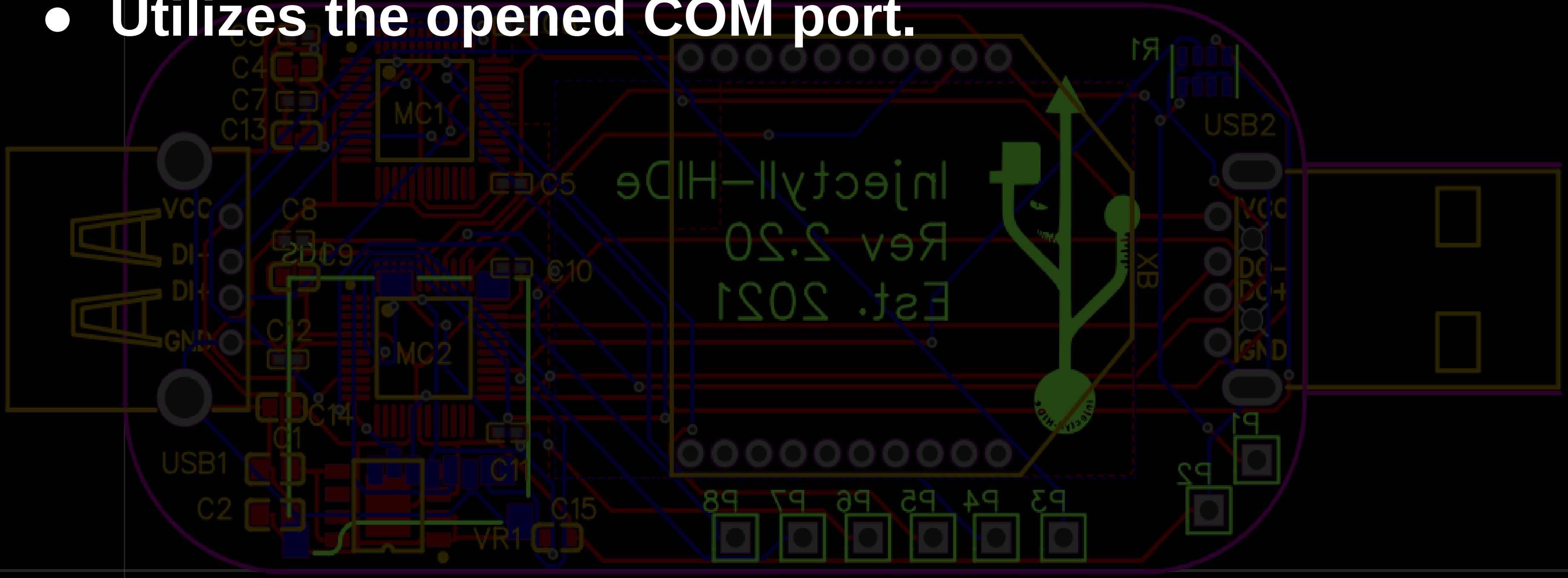
@c4m0ufl4g3

@Injectyll_HIDe

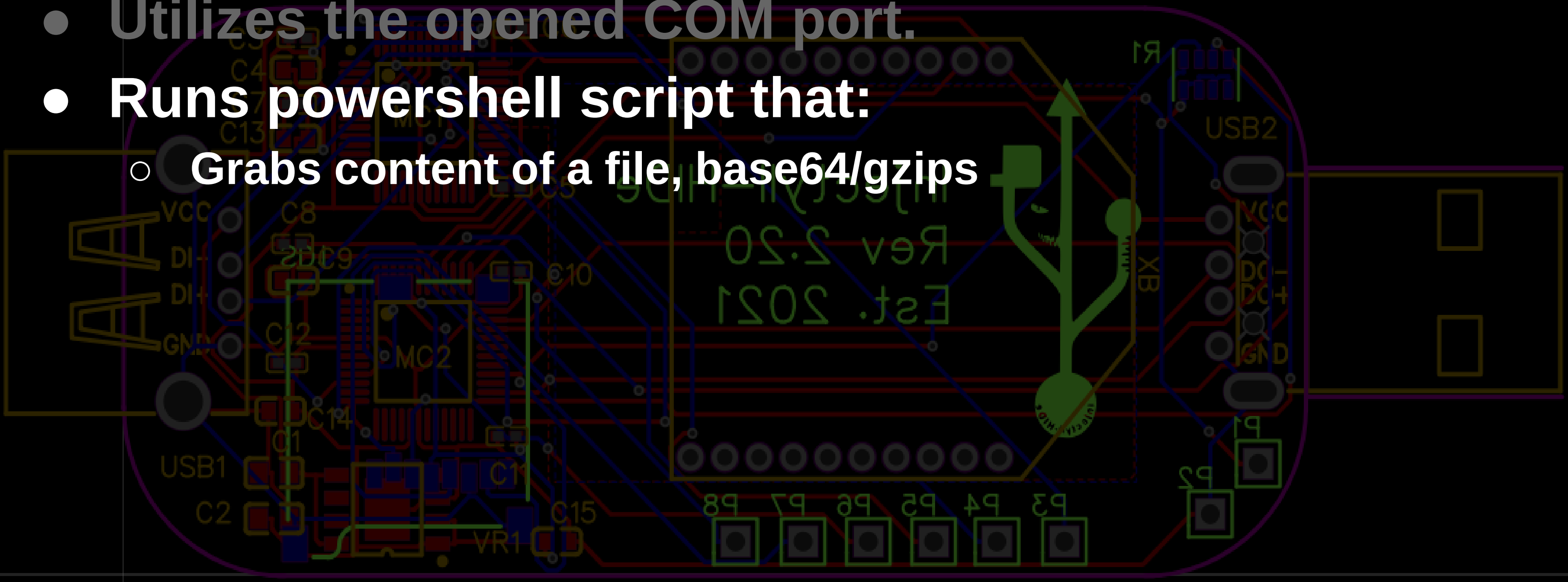
@allTheJurm

Custom data exfil script

- **Utilizes the opened COM port.**

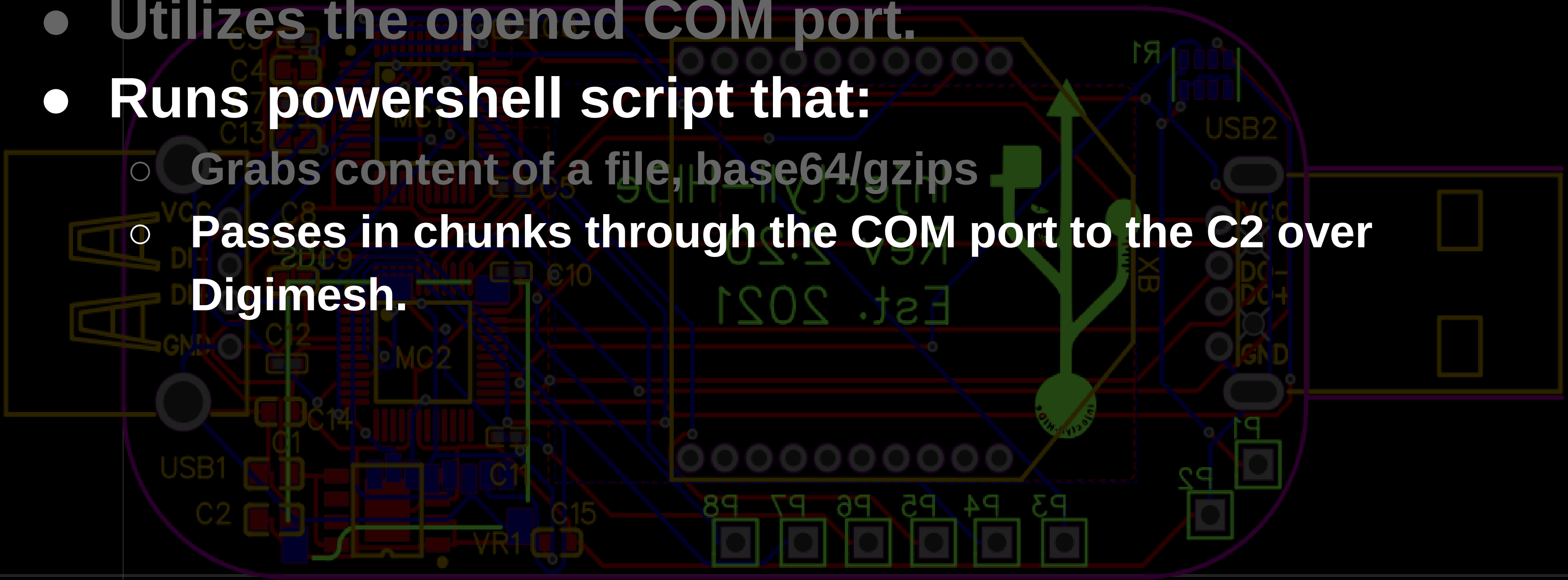


Custom data exfil script



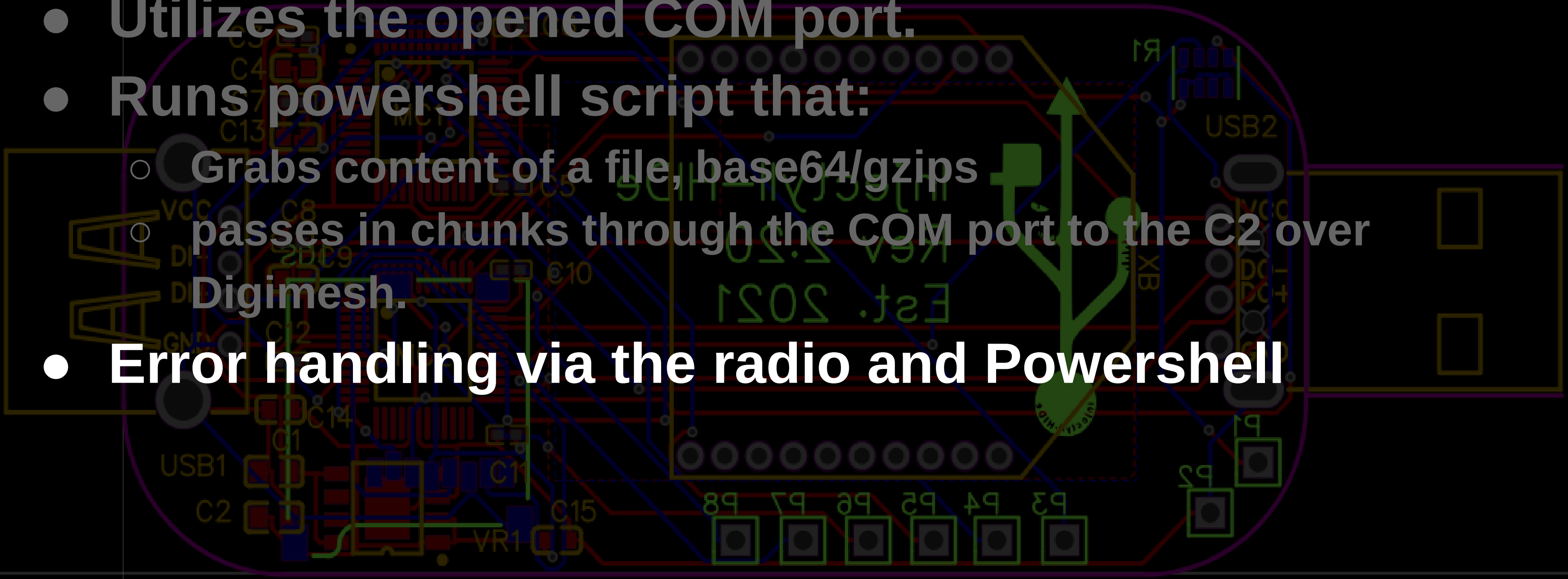
- Utilizes the opened COM port.
- Runs powershell script that:
  - Grabs content of a file, base64/gzips

Custom data exfil script



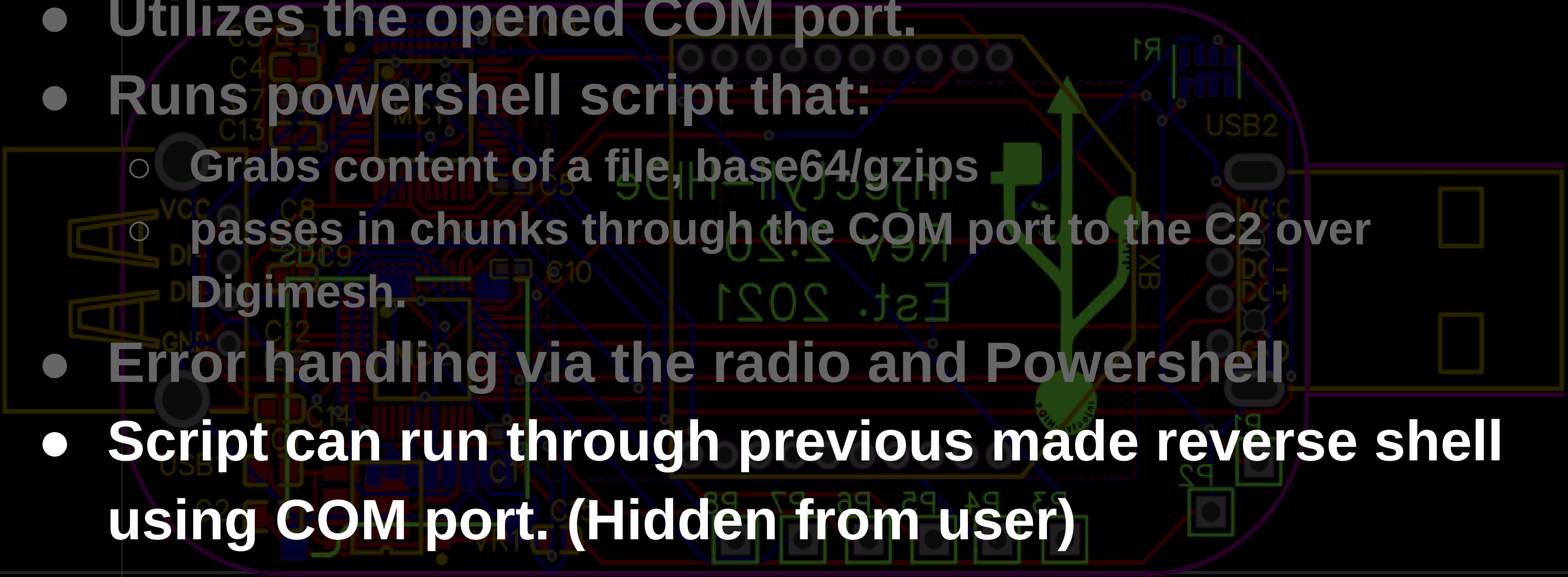
- Utilizes the opened COM port.
- Runs powershell script that:
  - Grabs content of a file, base64/gzips
  - Passes in chunks through the COM port to the C2 over Digimesh.

Custom data exfil script



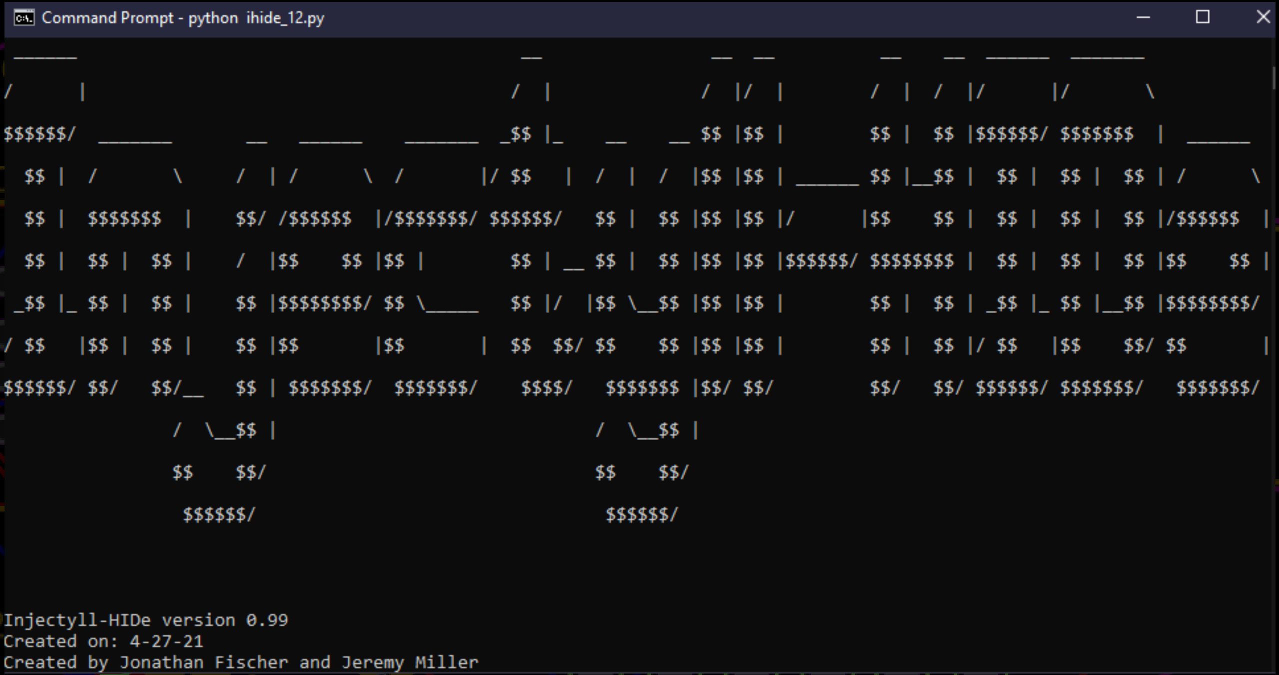
- Utilizes the opened COM port.
- Runs powershell script that:
  - Grabs content of a file, base64/gzips
  - passes in chunks through the COM port to the C2 over Digimesh.
- **Error handling via the radio and Powershell**

Custom 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)**

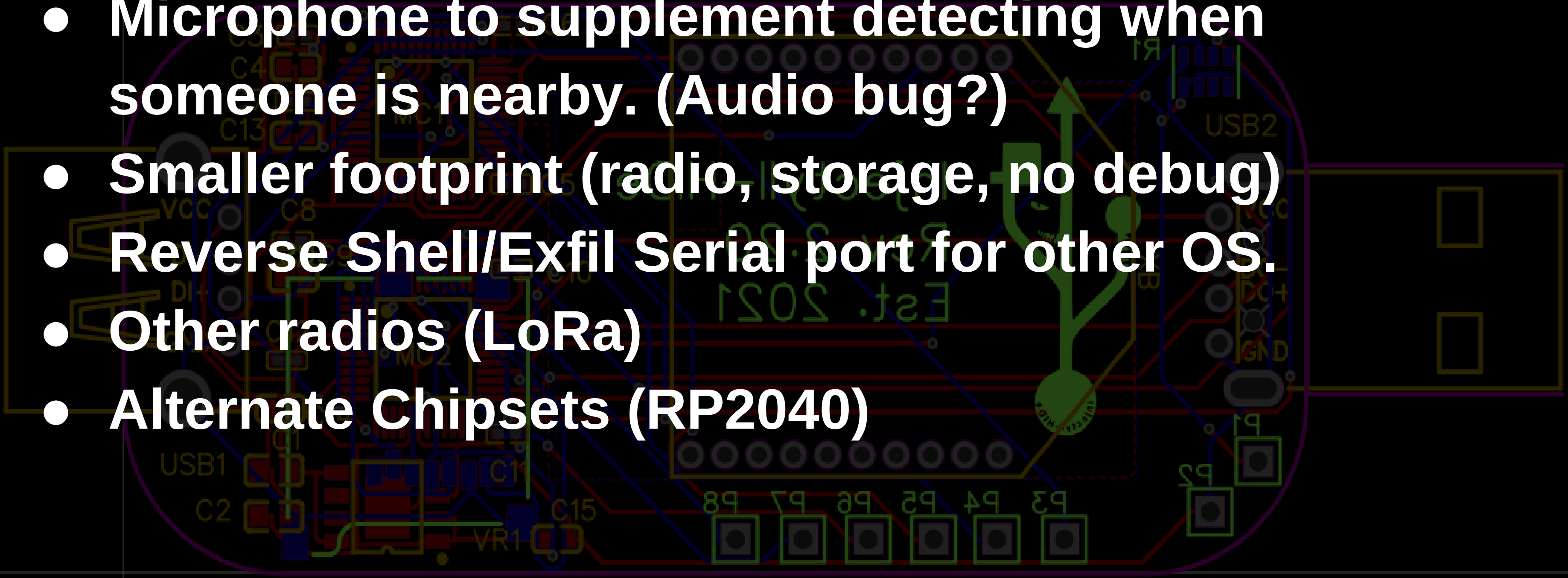
Custom C2



Command Prompt - python ihide_12.py

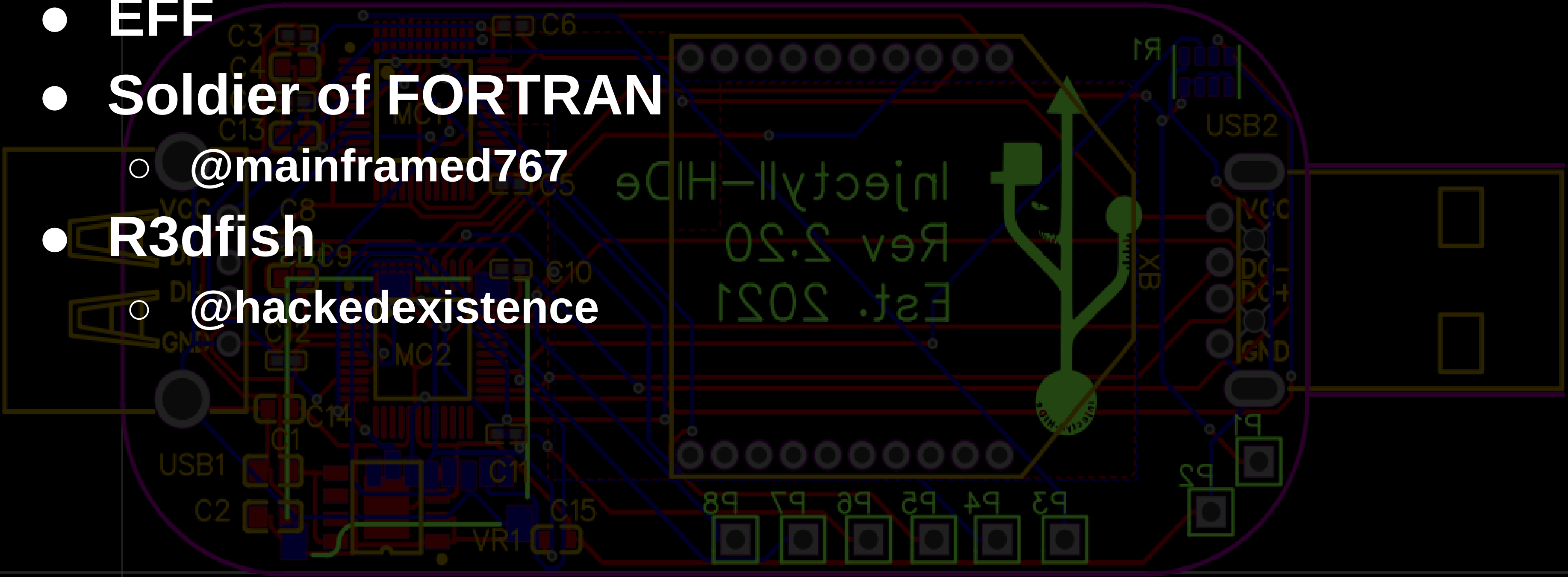
```
 ______                                          __                __  __          __    __  ______  _______
/      |                                        /  |              /  |/  |        /  |  /  |/      |/       \

$$$$$$/  _______       __    ______    _______  _$$ |_    __    __ $$ |$$ |        $$ |  $$ |$$$$$$/ $$$$$$$  |  ______

  $$ |  /       \     /  | /      \  /       |/ $$   |  /  |  /  |$$ |$$ | ______ $$ |__$$ |  $$ |  $$ |  $$ | /      \

  $$ |  $$$$$$$  |    $$/ /$$$$$$  |/$$$$$$$/ $$$$$$/   $$ |  $$ |$$ |$$ |/      |$$    $$ |  $$ |  $$ |  $$ |/$$$$$$  |

  $$ |  $$ |  $$ |    /  |$$    $$ |$$ |        $$ | __ $$ |  $$ |$$ |$$ |$$$$$$/ $$$$$$$$ |  $$ |  $$ |  $$ |$$    $$ |

 _$$ |_ $$ |  $$ |    $$ |$$$$$$$$/ $$ \_____   $$ |/  |$$ \__$$ |$$ |$$ |        $$ |  $$ | _$$ |_ $$ |__$$ |$$$$$$$$/

/ $$   |$$ |  $$ |    $$ |$$       |$$       |  $$  $$/ $$    $$ |$$ |$$ |        $$ |  $$ |/ $$   |$$    $$/ $$       |

$$$$$$/ $$/   $$/__   $$ | $$$$$$$/  $$$$$$$/    $$$$/   $$$$$$$ |$$/ $$/         $$/   $$/ $$$$$$/ $$$$$$$/   $$$$$$$/

                /  \__$$ |                              /  \__$$ |

                $$    $$/                               $$    $$/

                 $$$$$$/                                 $$$$$$/



Injectyll-HIDe version 0.99
Created on: 4-27-21
Created by Jonathan Fischer and Jeremy Miller
```

Roadmap



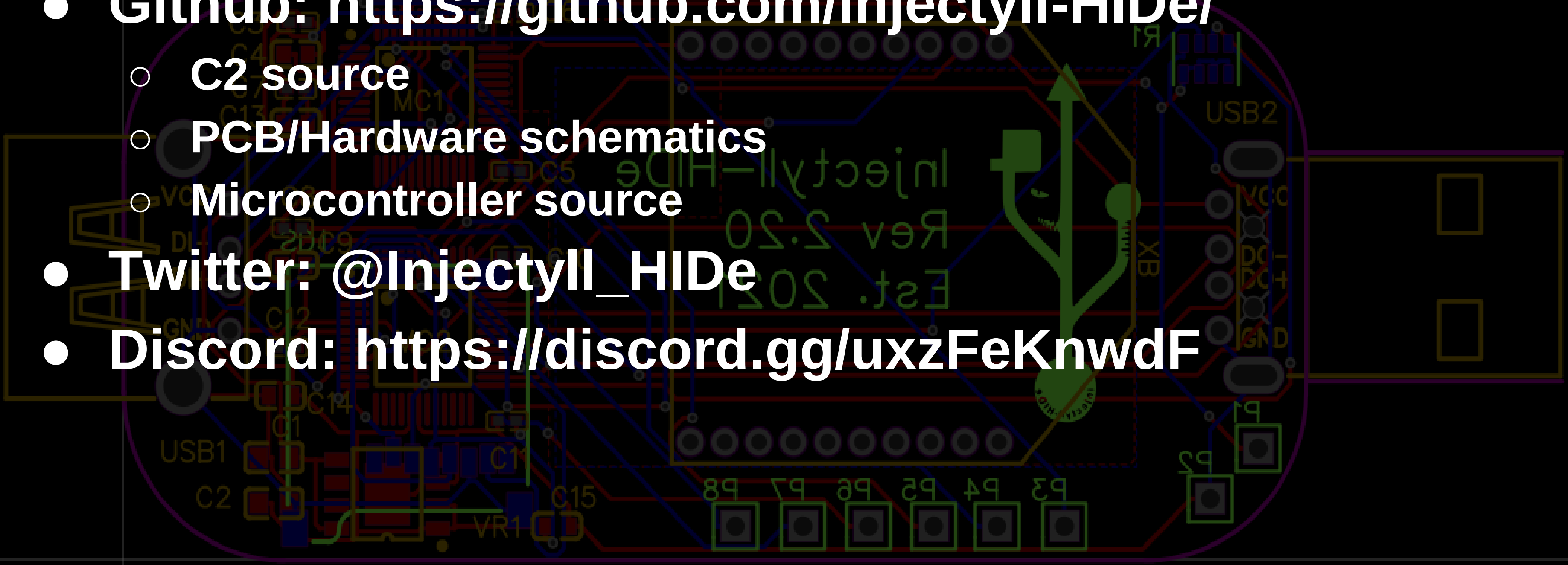
- Microphone to supplement detecting when someone is nearby. (Audio bug?)
- Smaller footprint (radio, storage, no debug)
- Reverse Shell/Exfil Serial port for other OS.
- Other radios (LoRa)
- Alternate Chipsets (RP2040)

Special Thank You!



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

Contribute/Contact/Q&A



- Github: https://github.com/Injectyll-HIDe/
  - C2 source
  - PCB/Hardware schematics
  - Microcontroller source
- Twitter: @Injectyll_HIDe
- Discord: https://discord.gg/uxzFeKnwdF