

Keeping Your Distance

Pwning RFID Physical Access Controls From 6FT and Beyond



Meet Your Speakers



Langston C.

Principal Penetration Tester

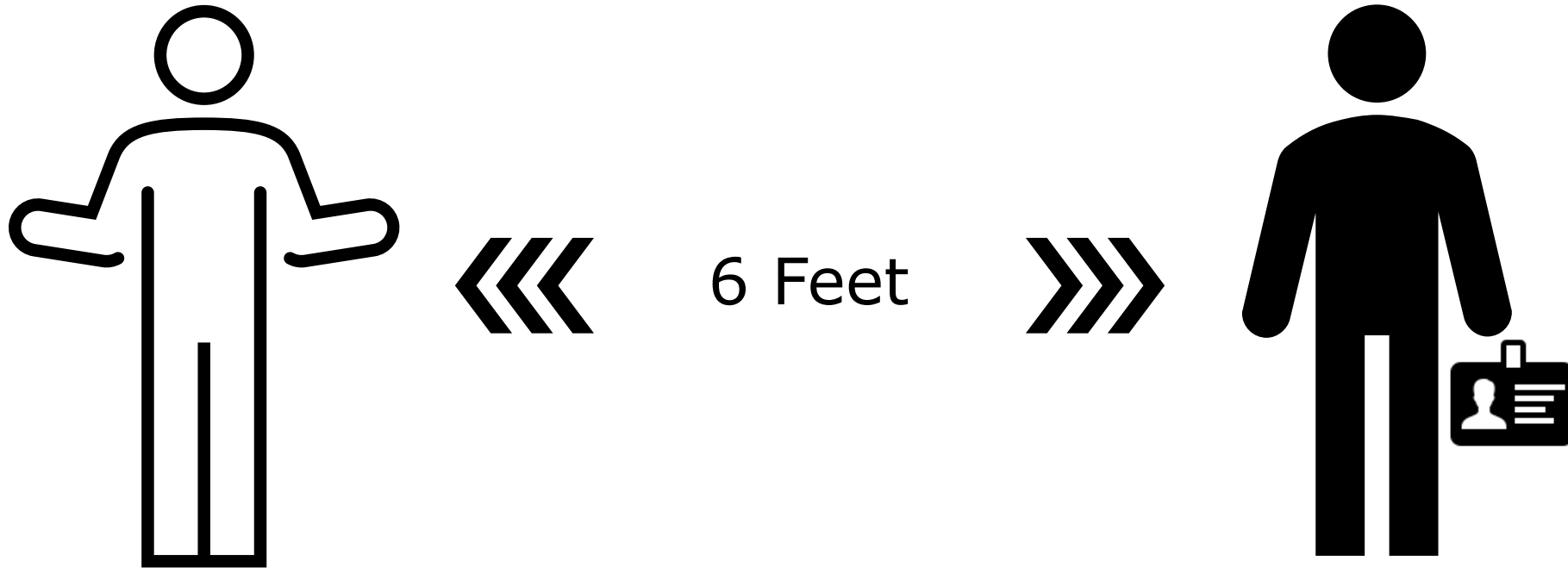


Dan G.

Penetration Tester

How Do You Conduct Physical Red Team Engagements During A Pandemic?

The Problem



What is RFID Cloning?

- Radio Frequency Identification (RFID) technology supports many physical access control systems
- RFID access control technology provides convenient and cost-effective benefits
- These benefits come with many weaknesses
- Numerous implementations of RFID are susceptible to RFID cloning
- Threat actors can surreptitiously clone or copy RFID credentials under certain circumstances

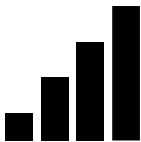
Low Frequency VS High Frequency RFID



125 kHz



Less Secure



Long range



13.56 MHz



Secure



Short range

Traditional Cloning Methods

Traditional Close-Range Techniques

- **The Brush Pass RFID Method**
~ 2'-3'
 - Pros: Very stealthy and fast
 - Cons: Weak Signal Strength and not always socially distanced!
- **Clipboard Cloner Method**
~5"-7"
 - Pros: Portable and high signal strength
 - Cons: Less stealthy and not socially distanced!



Social Distanced Badge Cloning (6ft and Beyond!)

The Stand-Alone Wall Reader Implant

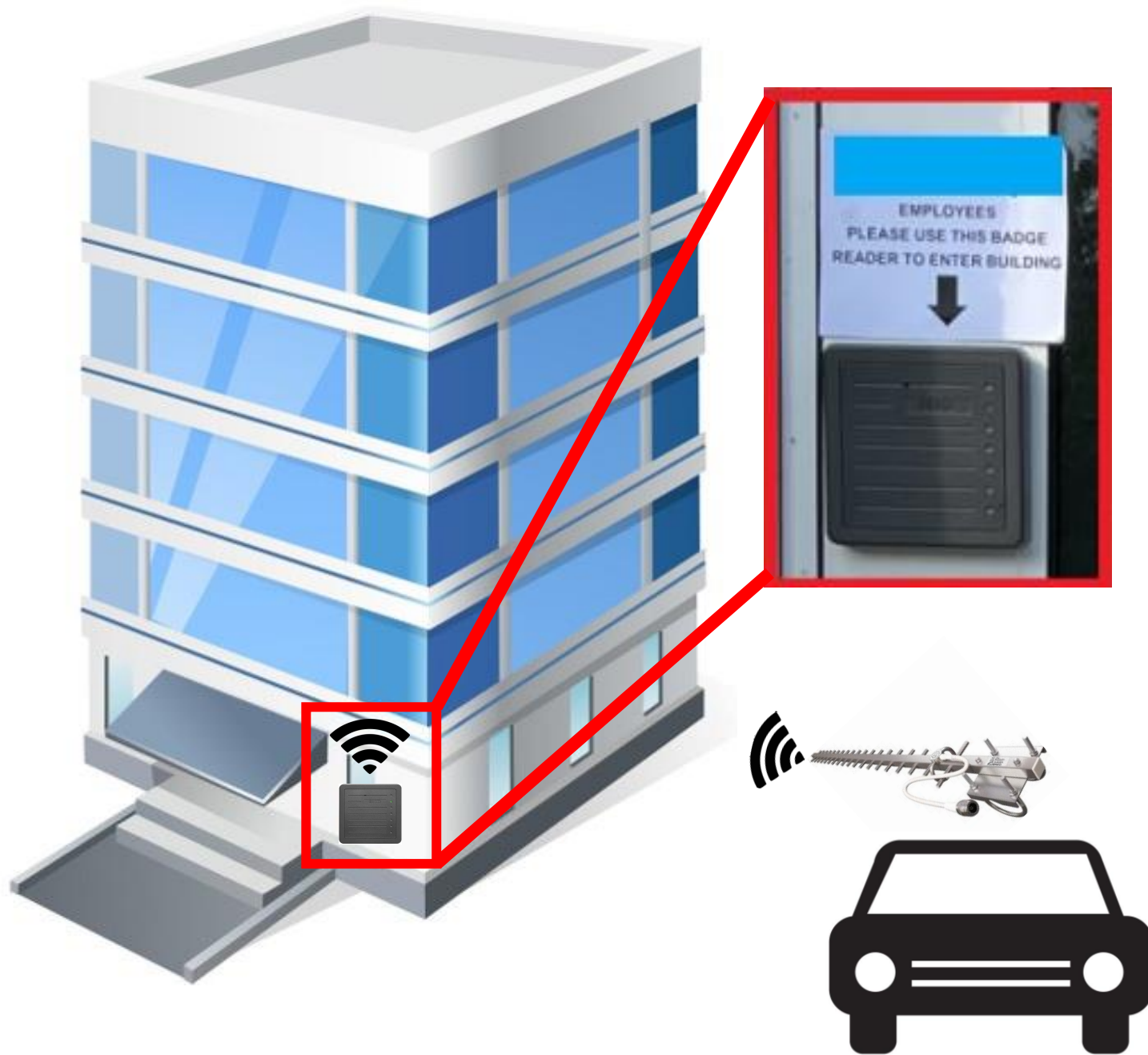
- Allows credential collection with little to no human interaction.
- Very stealthy, testers maintain anonymity.
- Remotely collect badge credentials through secured wireless.



Grab the Loot!

Remotely Collect
Card/FOB Key Loot from
the ESP RFID Tool WiFi!

Grab your favorite long-
range antenna and wait!



Rogue Reader Wireless Interface

- RFID ESP Key WiFi Access
 - SSID: "ESP-RFID-Tool"
 - URL: <http://192.168.1.1>
- Default credentials to access the configuration page:
 - Username: "admin"
 - Password: "rfidtool"
- Change SSID to blend in with target organization
- Access HEX Code Data in the "List Exfiltrated Data" Page

ESP-RFID-Tool v1.0.3



by Corey Harding

www.LegacySecurityGroup.com / www.Exploit.Agency

File System Info Calculated in Bytes

Total: 2949250 **Free:** 2948497 **Used:** 753

[List Exfiltrated Data](#)

[Experimental TX Mode](#)

-

[Configure Settings](#)

-

[Format File System](#)

-

[Upgrade Firmware](#)




-



[Help](#)



<https://github.com/rfidtool/ESP-RFID-Tool>

Rogue Reader Wireless Interface

  192.168.1.1/viewlog?payload=/ClippyPayload.txt

[<- BACK TO INDEX](#)



[List Exfiltrated Data](#)

[Download File](#) - [Delete File](#)

Note: Preambles shown are only a guess based on card length and may not be accurate for every card format.

/ClippyPayload.txt

26 bit card,18 bit preamble,Binary:000000100000000001 00001111000000101001110011, **HEX:20043C0A73**

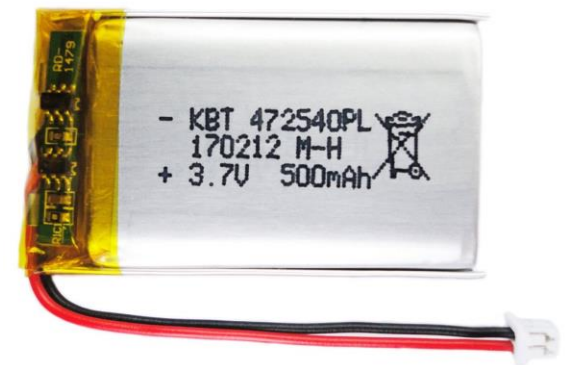


- Copy the HEX Code Payload for later!

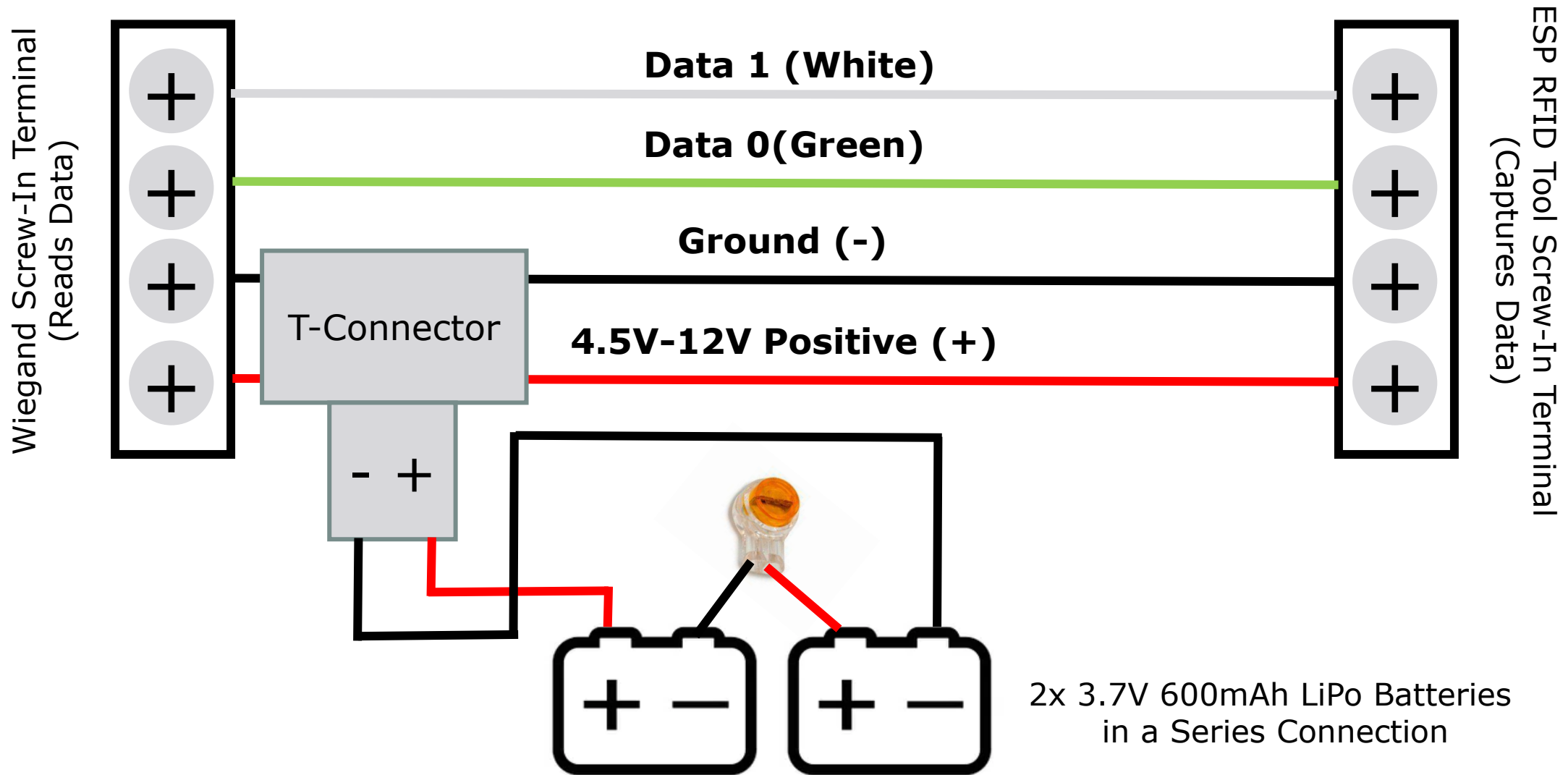
Wall Reader Build – No Soldering Needed!

Low Frequency BOM (Build of Materials):

- HID Prox Pro 5355AGN00 Reader
- ESP RFID Tool OR ESPKey
- 3M Wall Hanging Strips
- 2x 3.7V 500mAh LiPo Batteries w/ JST connector
- 1x T Tap Connector
- 2x UY Wire to Wire Connector
- Bread Board Jumper Wires
- 22AWG electrical wire



Wall Reader Connection Guide



Misdirection with Low-Frequency

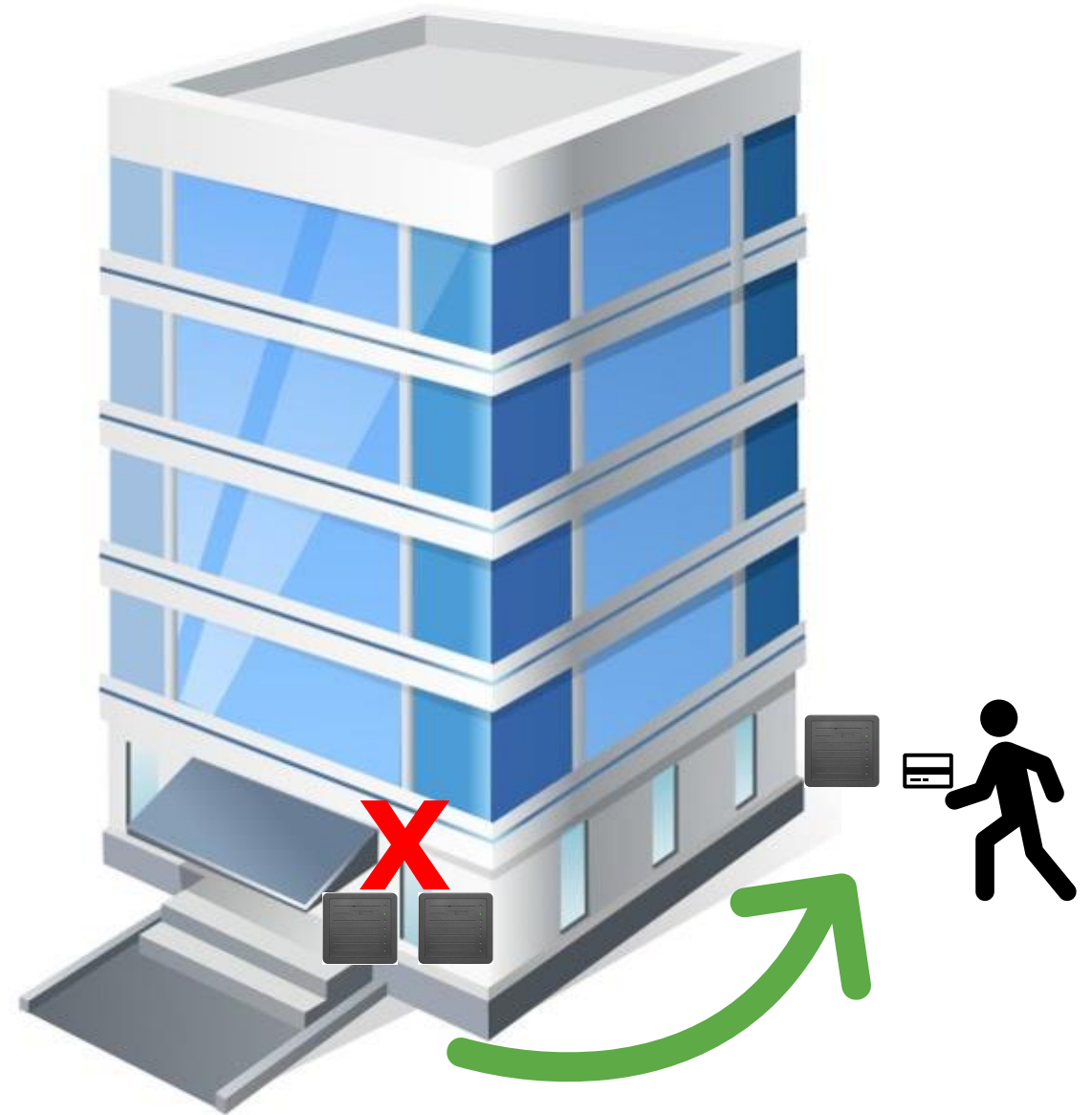
Misdirection – DOSing Readers

- Create a Social Engineering opportunity with a Badge Reader Denial of Service (DoS) attack!
- Placing two Low-Frequency RFID readers within 6" of each other causes interference and will jam the signal from reading card data.

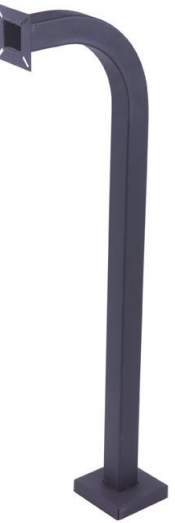
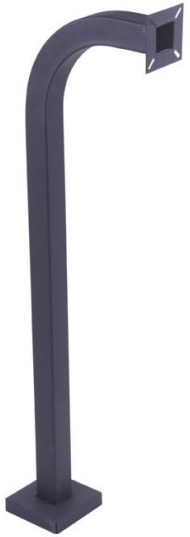


Misdirection – DOSing Readers

- Create a Social Engineering opportunity with a Badge Reader DOS!
- Redirect employees to increase tailgating opportunities!



Introducing the Gooseneck Reader



The Gooseneck Reader

- **Simple, yet effective!**
 - Gooseneck Pedestal
 - Long Range Reader
 - Plywood
 - Rubber Feet
 - Spray Paint



The Gooseneck Reader

- Mobile Long-Range Reader for both Low or High Frequency
- Reads up to ~3.3' (1M) Away
- 12 Hour Battery



The Gooseneck Reader

- Mobile Long-Range Reader for both Low or High Frequency
- Reads up to ~3.3' (1M) Away
- 12 Hour Battery



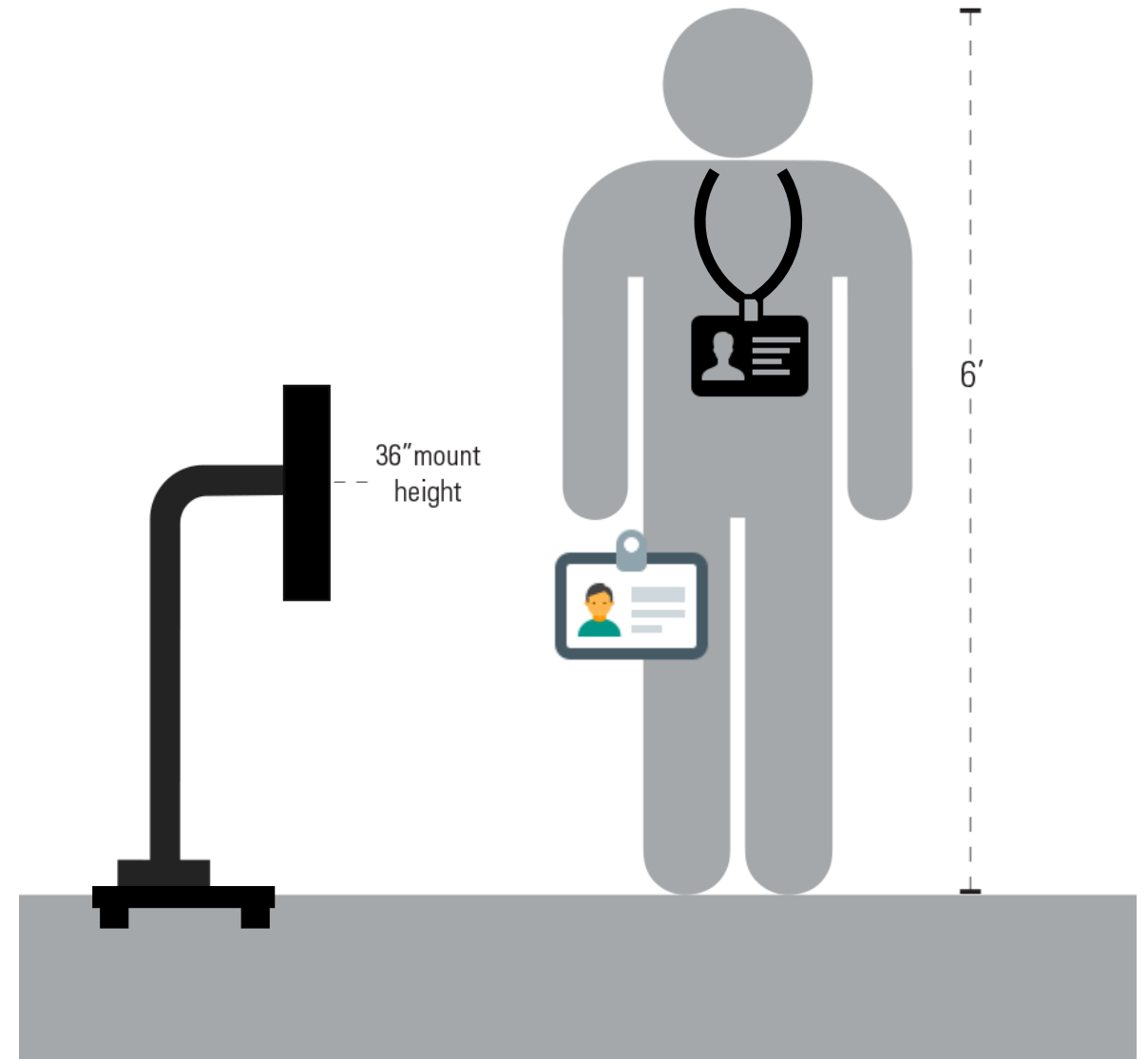
The Gooseneck Reader

- Mobile Long-Range Reader for both Low or High Frequency
- Reads up to ~3.3' (1M) Away
- 12 Hour Battery



The Gooseneck Reader

- Mobile Long-Range Reader for both Low or High Frequency
- Reads up to ~3.3' (1M) Away
- 12 Hour Battery



Gooseneck Build – No Soldering Needed!

Gooseneck BOM (Build of Materials):

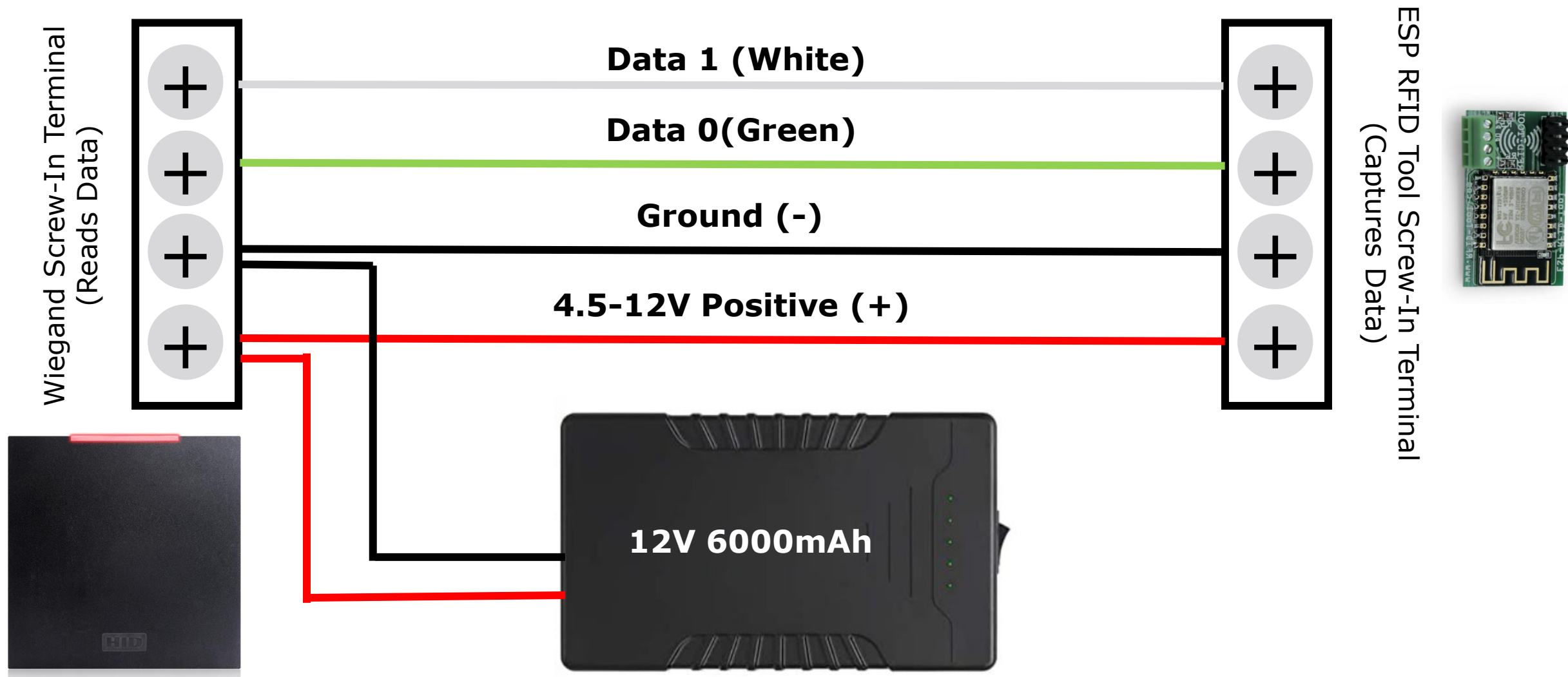
- Low Frequency Long Range Reader (e.g. HID MaxiProx 5375)
- High Frequency Long Range Reader (e.g. HI iCLASS SE R90)
- MDF or Plywood Wood
- ESP RFID Tool
- 12V 6000mAh/5V 12000mAh DC Battery
- 3/8"x1.25" Nuts and Bolts
- Black Spray Paint
- Bread Board Jumper Wires
- 22AWG electrical wire
- DC Power Pigtail
- Rubber Feet
- Pedestal Pro Gooseneck

Full build tutorial guide:

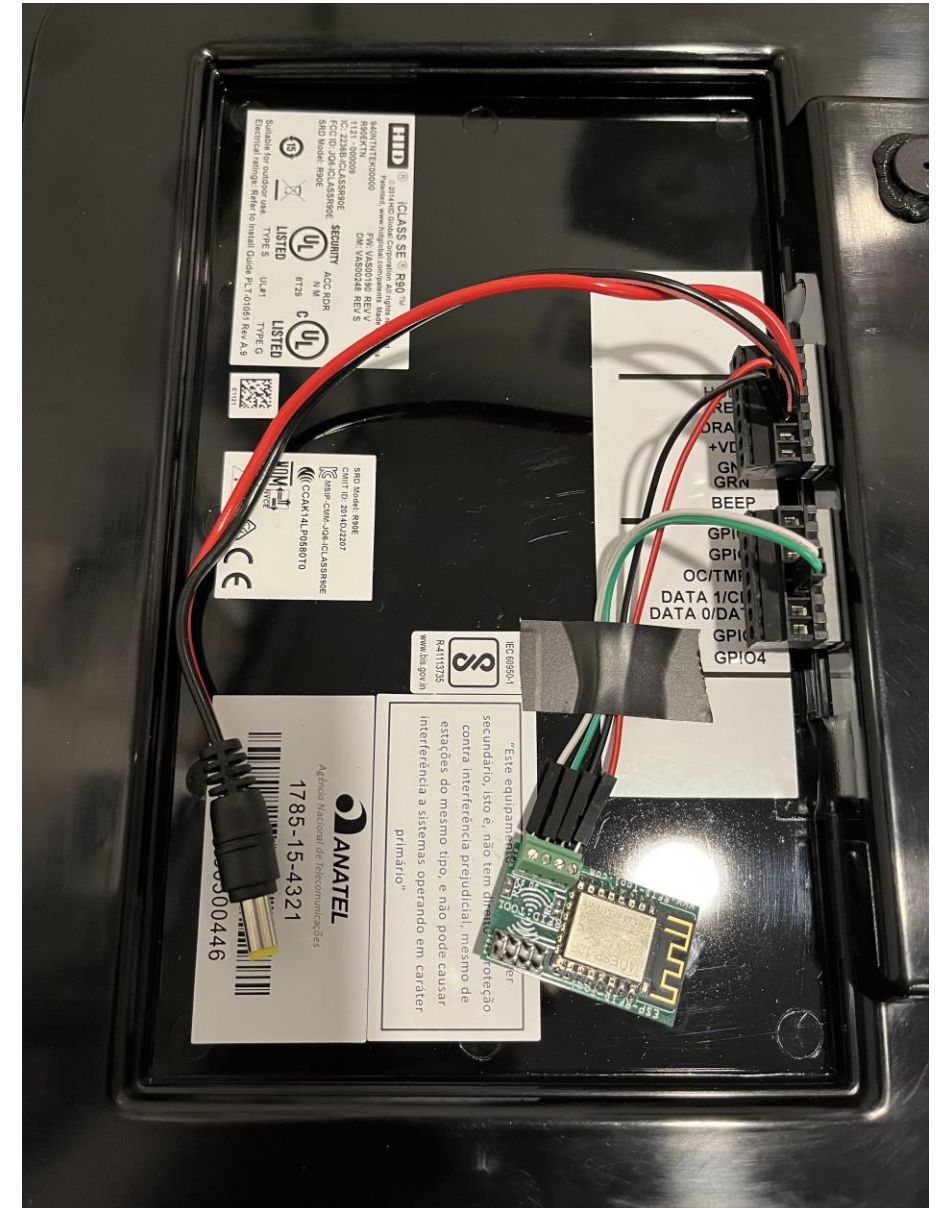
www.github.com/sh0ckSec



Long Range Reader Connection Guide



Long Range Reader Wiring



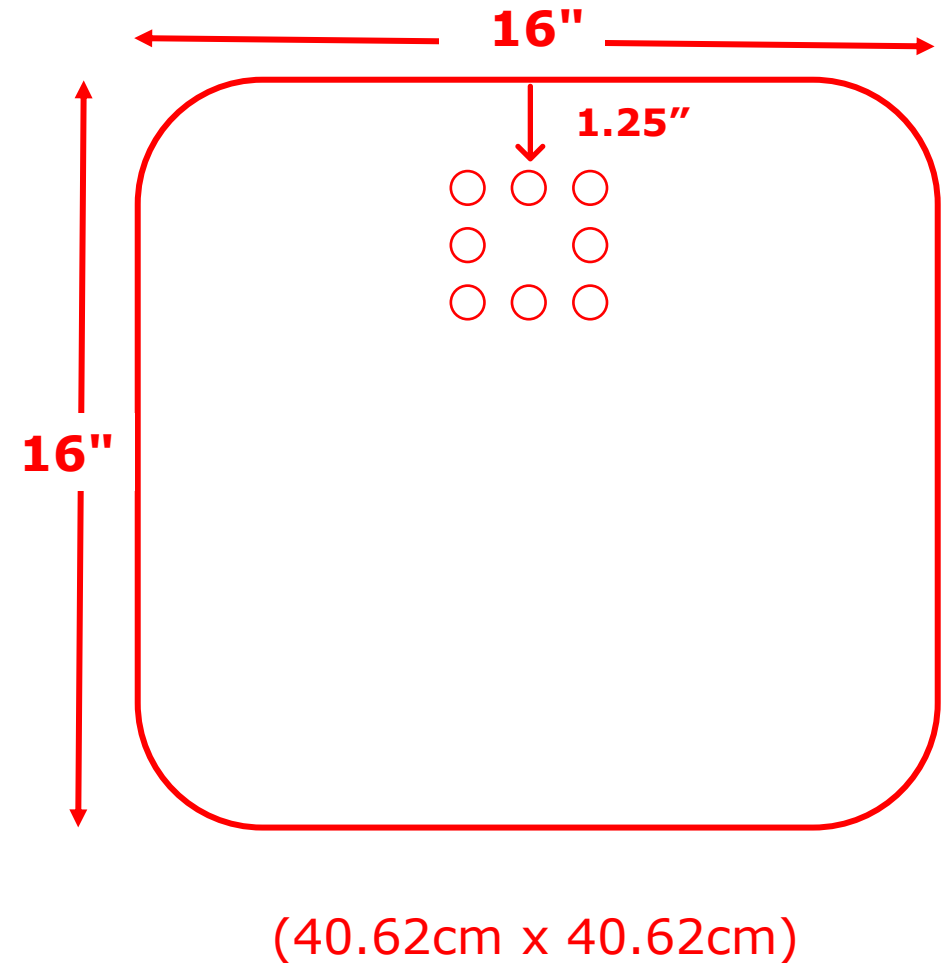
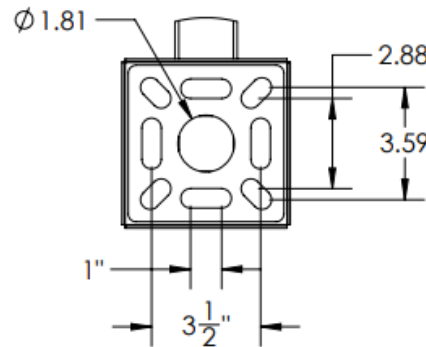
Gooseneck Base

Download the Gooseneck Base MK2 template here for laser cutting, CNC or print, along a full build tutorial guide:

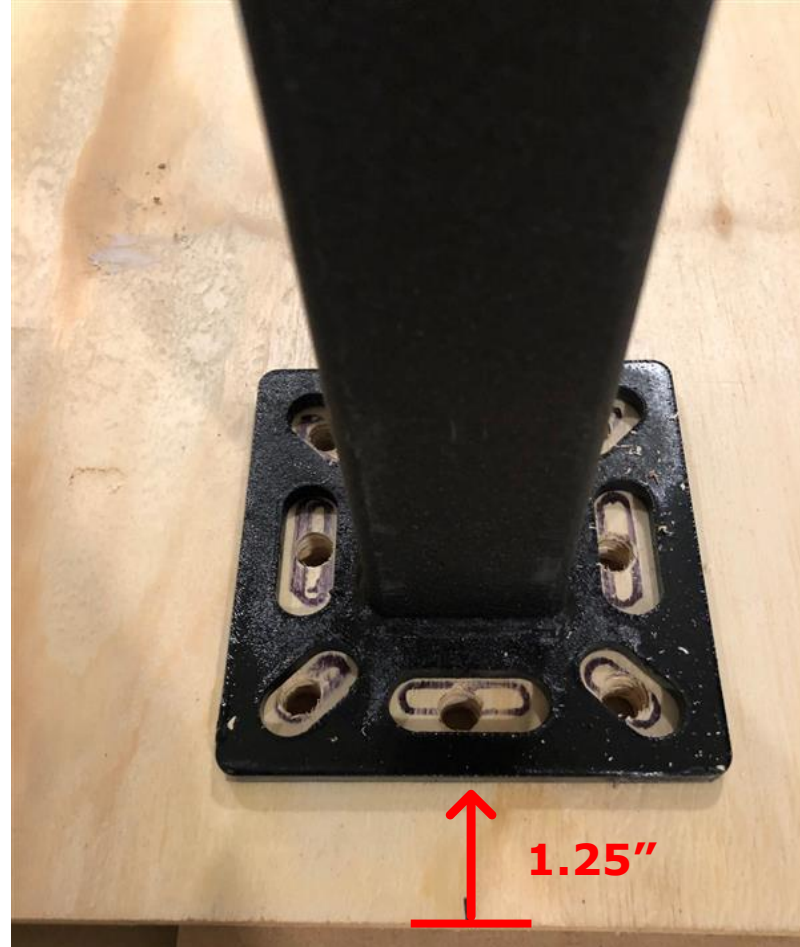
www.github.com/sh0ckSec

Materials:

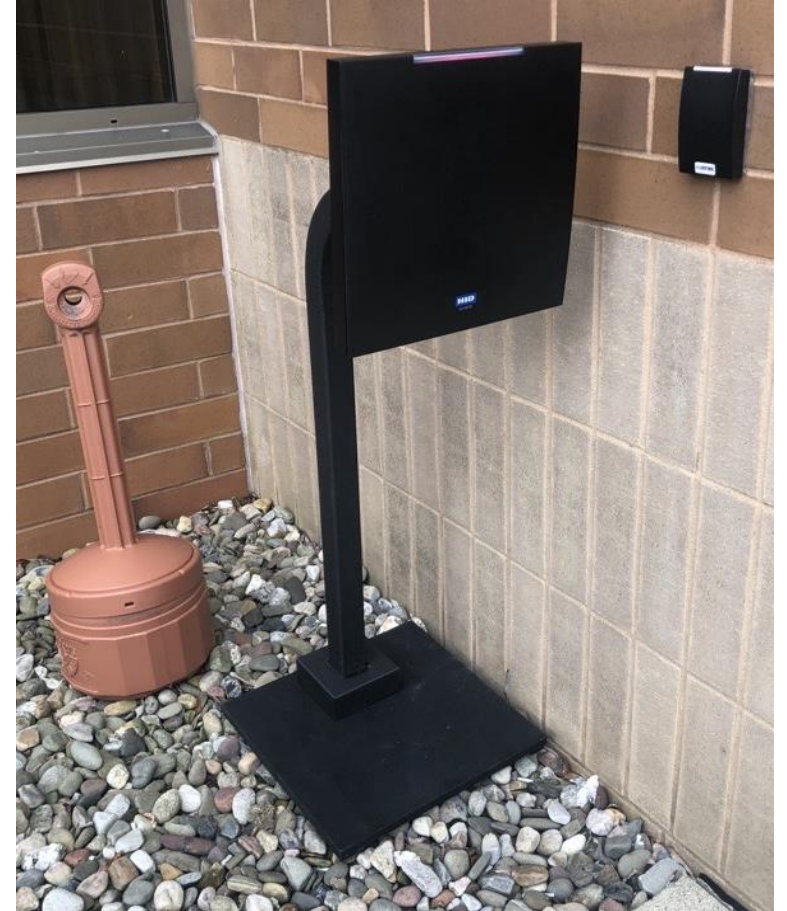
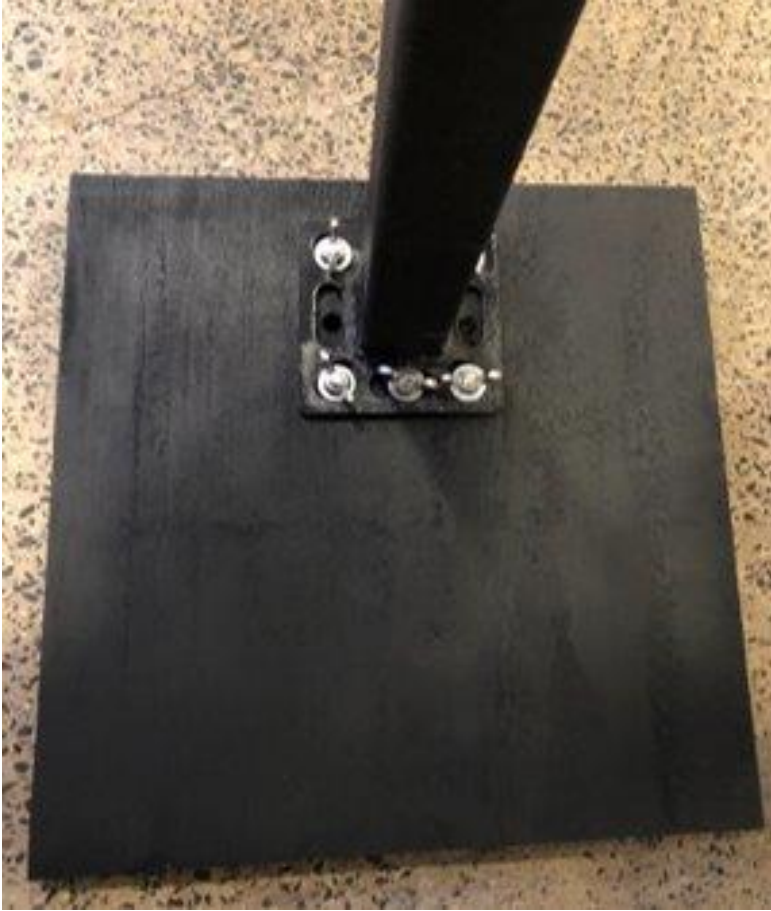
- 30mm Heavy Duty Rubber Furniture Pads
- 3/8" x 1 1/4" Carriage Bolts and Wing Nuts
- 1/2" thick MDF or Plywood



Gooseneck Base – Installation



Gooseneck Base – Installation



Grab the Loot!

Remotely Collect
Card/FOB Key Data Loot
from the ESP RFID Tool
WiFi!

Grab your favorite long-
range antenna and wait!



Cloning Badge Data with a Mobile Phone

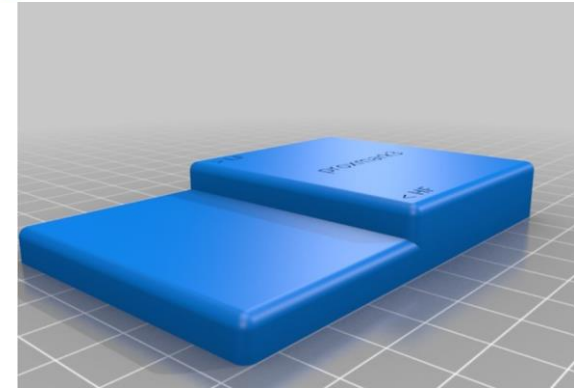
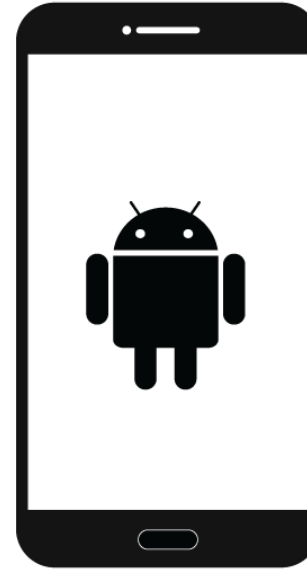
Quick, Cheap and Easy!






Mobile Phone RFID Copy Method



Materials Needed:

- Android Phone or Tablet
- Proxmark3 Easy or Proxmark3 RDV4
- USB-C to Micro USB OTG Cable
- Blank T5557 Rewriteable RFID Cards
- **AndProx** Mobile App (No Root required!)
 - <https://github.com/AndProx/AndProx>
- **Bonus!**
 - 3D Print a Proxmark3 Easy enclosure by vikwin
 - <https://www.thingiverse.com/thing:3123482>



Rogue Reader Wireless Interface

  192.168.1.1/viewlog?payload=/ClippyPayload.txt

[<- BACK TO INDEX](#)



[List Exfiltrated Data](#)


[Download File](#) - [Delete File](#)

Note: Preambles shown are only a guess based on card length and may not be accurate for every card format.

/ClippyPayload.txt

26 bit card,18 bit preamble,Binary:000000100000000001 00001111000000101001110011, **HEX:20043C0A73**

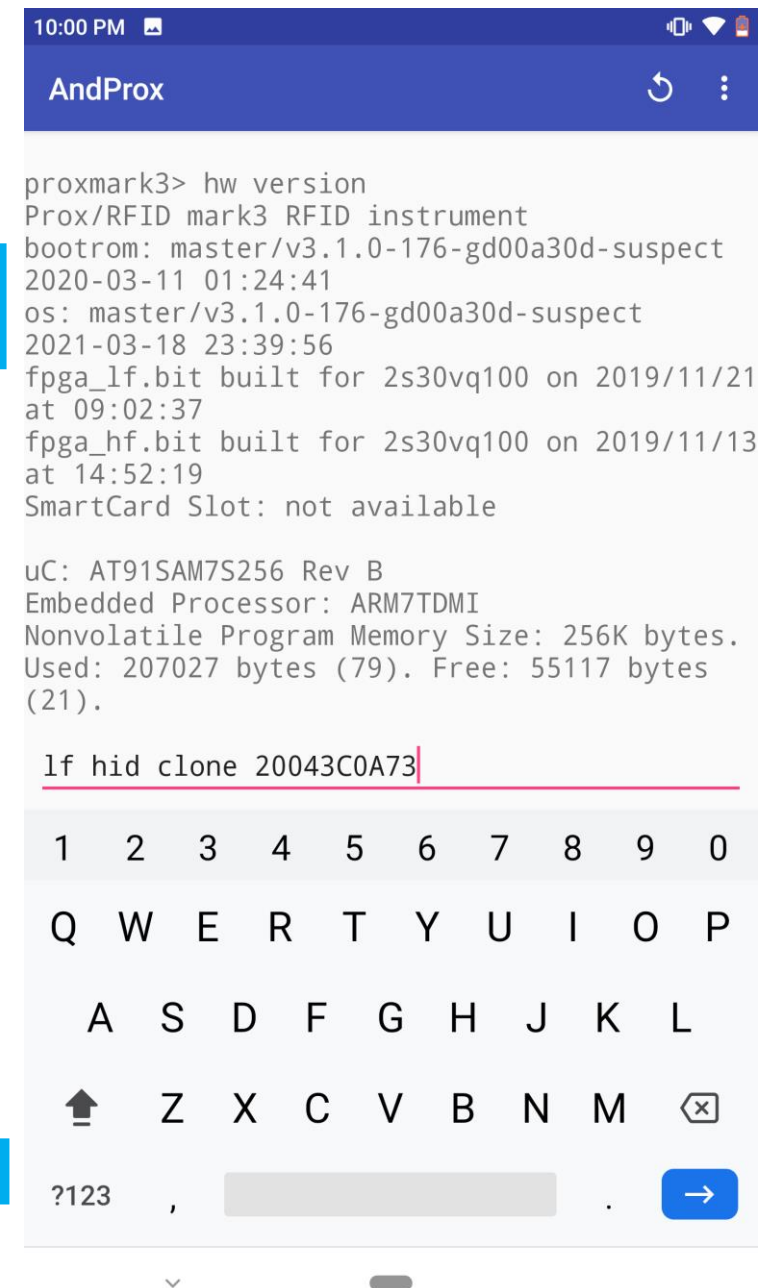
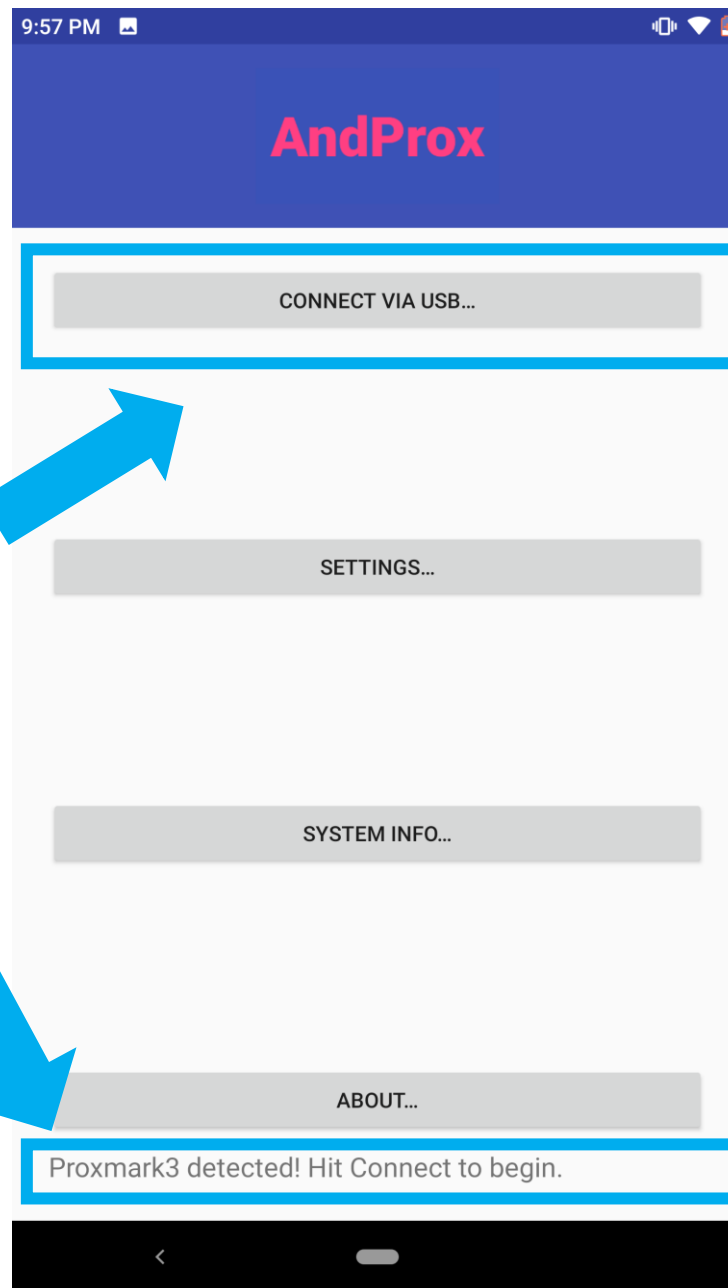


- Copy the HEX Code Payload!

AndProx Setup

After you download and install...

1. Plug in your Proxmark3 via OTG cable and Click Connect Via USB
2. Begin sending commands!



AndProx Commands

```
> lf hid clone <HEX CODE>
```

```
> lf hid clone 20043C0A73
```

#Example

```
> lf search
```

#Verify Your Card Data!



```
proxmark3> lf hid clone 20043C0A73
```

```
#db# DONE!
```

```
proxmark3> lf search
```

NOTE: some demods output possible binary
if it finds something that looks like a tag
False Positives ARE possible

Checking for known tags:

HID Prox TAG ID: 20043c0a73

Format: H10301 (HID H10301 26-bit)
Facility Code: 30
Card Number: 1337
Parity: Valid

Valid HID Prox ID Found!

Enter a command...

And you're in!



References

- Dib, Alex. "RFID Thief v2.0." July 2018, <https://scund00r.com/all/rfid/tutorial/2018/07/12/rfid-theif-v2.html>
- Farrell, Michael and Boris Hajduk. "AndProx." July 2021, GitHub, <https://github.com/AndProx/AndProx>
- Harding, Cory. "ESP-RFID-Tool." March 2018, GitHub, <https://github.com/rfidtool/ESP-RFID-Tool>
- Kelly, Mike. "Wiegotcha – RFID Thief." January 2017, <https://exfil.co/2017/01/17/wiegotcha-rfid-thief/>
- Rumble, Rich. "RFID Sniffing Under Your Nose and in Your Face." DerbyCon IX, September 2019, <https://www.youtube.com/watch?v=y37j6RDtybQ>
- W., Viktor. "Enclosure For Proxmark3 Easy." Thingiverse, September 2018, <https://www.thingiverse.com/thing:3123482>
- White, Brent and Tim Roberts. "Breaking Into Your Building: A Hacker's Guide to Unauthorized Access." NolaCon 2019, May 2019, <https://www.youtube.com/watch?v=eft8PEImQZM>

Thank You!



@sh0ckSec
[Github.com/sh0cksec](https://github.com/sh0cksec)



@_BadCharacters
[Badcharacters.io](https://badcharacters.io)

CORE  BTS