Project Walrus

Make the most of your card cloning devices

Whois Team Walrus

Daniel Underhay

@dunderhay

Security Consultant at Aura Information Security

Matthew Daley

bugfuzz.com

Senior Security Consultant at Aura Information Security

Backstory – More Red Teaming ☺

- Phishing and social engineering attacks targeted at staff
- **Bypassing lock and access control systems**
- Attempts to physically access the premises
- Attempts to remove sensitive data
- Assessment and attempted infiltration of any internet-connected services or devices
- And more...

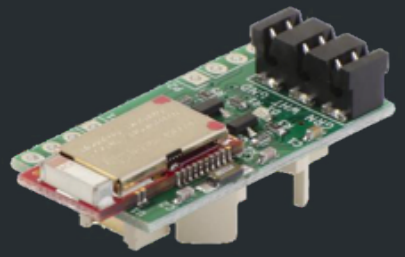
Access Control Systems

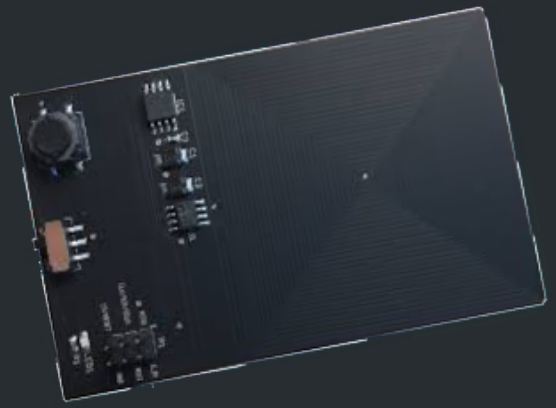
- Restrict entrance to a property, building or room to authorized persons
- Electronic locks
- Card or biometric access readers and software
- Some of these cards are easily cloned

Where Do We Find These

- Building entrance
- Elevators
- Office doors
- Areas that require additional privilege:
    - ❑ Server rooms
    - ❑ Secure rooms

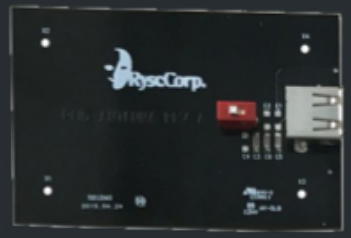
Card Cloning Devices

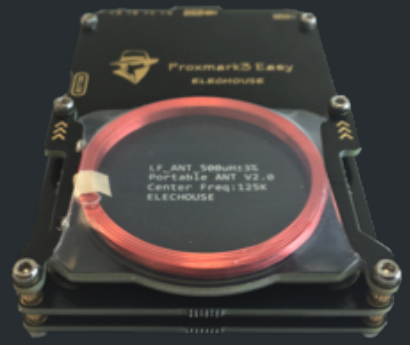




Proxmark3

- Created by Jonathan Westhues
- Industry standard card cloning device
- Low Frequency: 125kHz and 134kHz (HID Prox II, HITAG, and EM4100)
- High Frequency: 13.56Mhz (Mifare Classic/Ultralight, and iClass)





HTTPS://GITHUB.COM/PROXMARK/PROXMARK3

Chameleon Mini

- Created by Kasper & Oswald
- Portable tool for ISO14443/ISO15693/NFC security analysis
- Emulate and clone contactless cards
- High Frequency: 13.56Mhz
  (Mifare Classic 1K/4K 4B/7B/Ultralight)

HTTPS://GITHUB.COM/EMSEC/CHAMELEONMINI
HTTPS://KASPER-OSWALD.DE/GB/CHAMELEONMINI/

Tastic RFID Thief

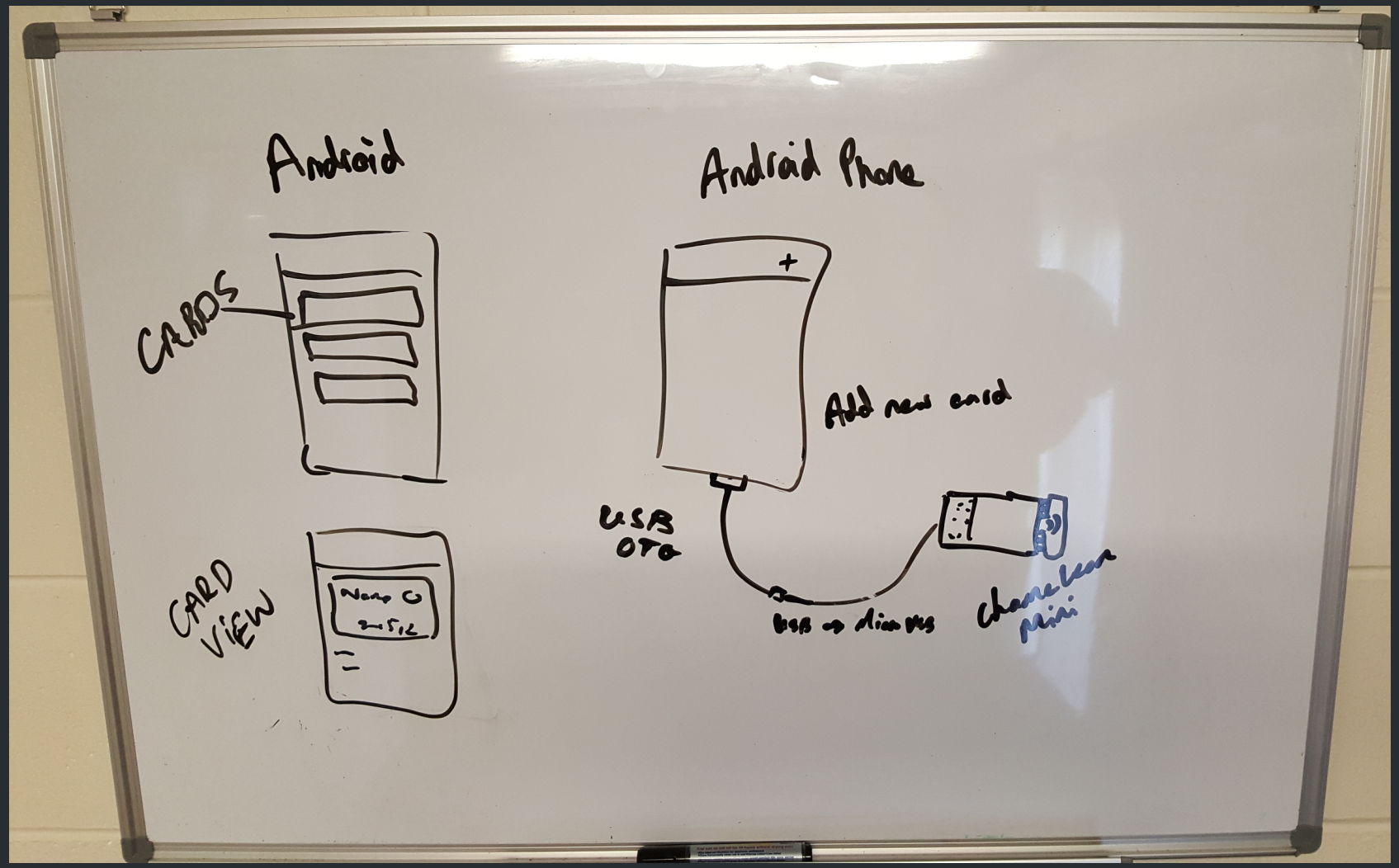
- HID Maxiprox 5375
- Long range RFID card reader
- Modified by Bishop Fox
- Low Frequency: 125kHz (HID Prox II)
- Range ~ 0.5 meters

HTTPS://WWW.BISHOPFOX.COM/RESOURCES/TOOLS/RFID-HACKING/ATTACK-TOOLS/

Difficulties with Card Cloning

- No common tool that controls all the devices
- No common database to store cloned cards
- Cloning cards surreptitiously can be tricky
- Existing standalone mode on Proxmark3 is sketchy (no feedback)
- Devices are often not very ‘user friendly’

An Idea

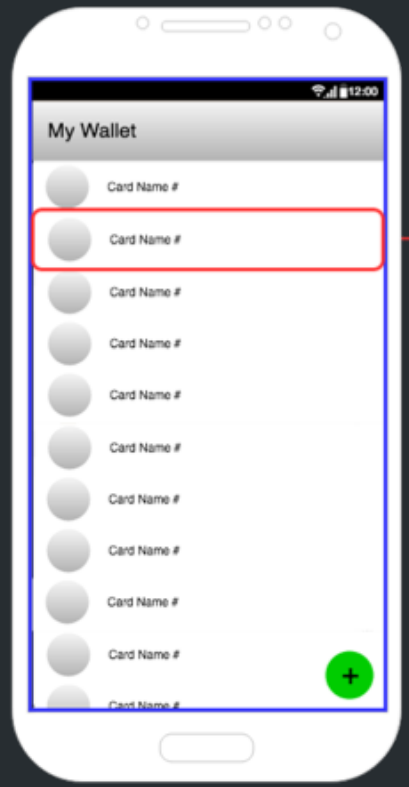


PoC || GTFO

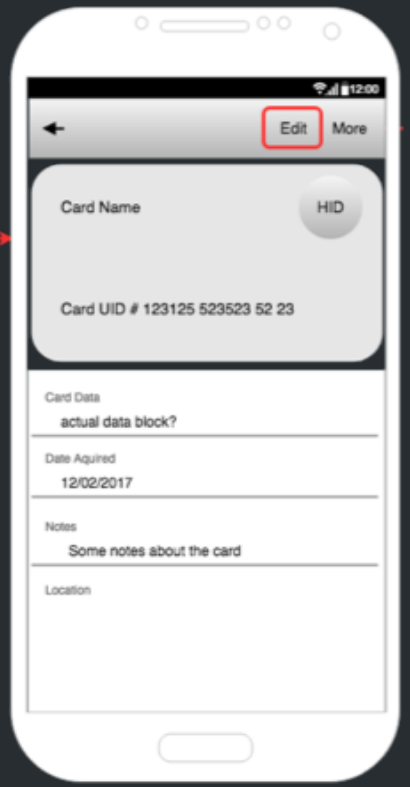
Card data:

```
MIFARE Classic 1k
ATQA: 0400
UID: 5D019376
SAK: 08
```

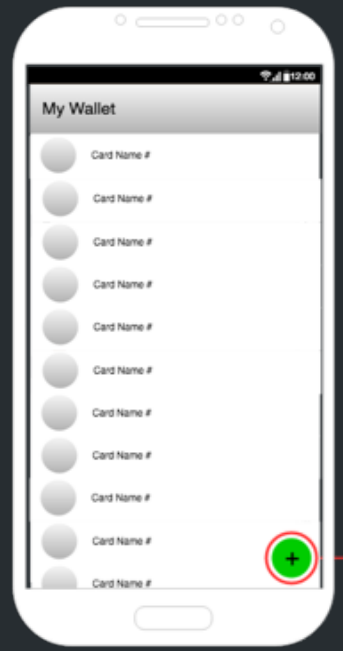
Wireframing



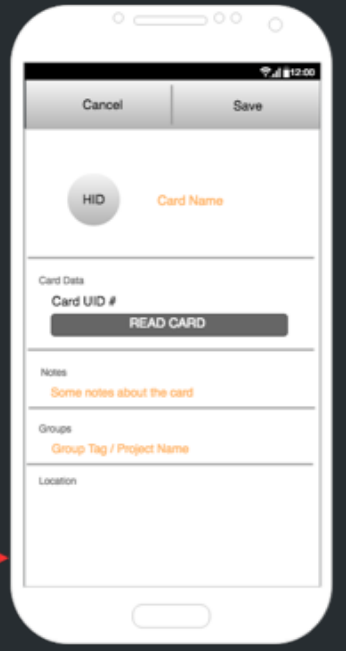
My Wallet Screen



Detailed Card Screen



My Wallet Screen

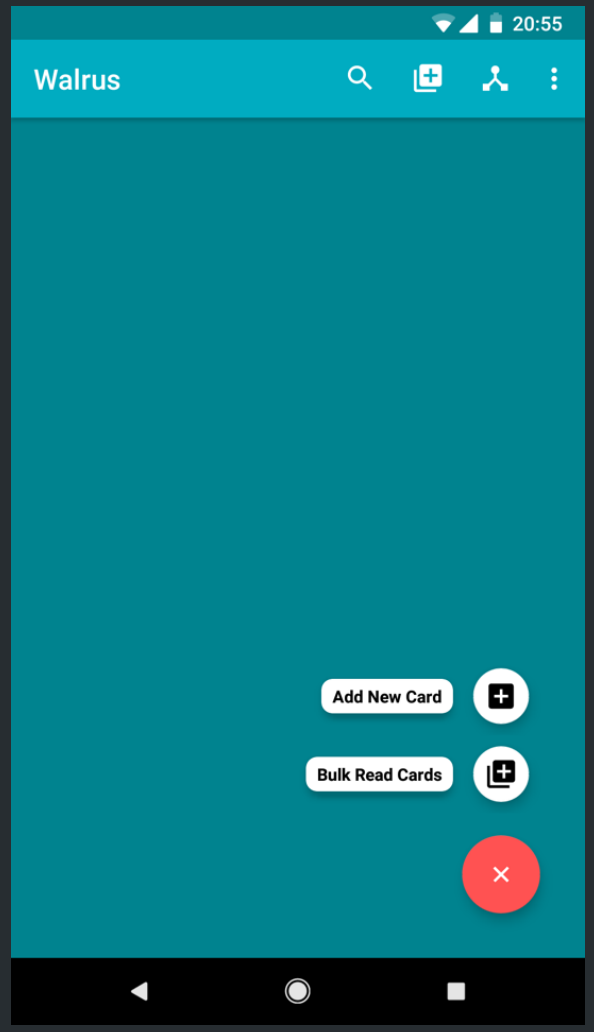


Add New Card View

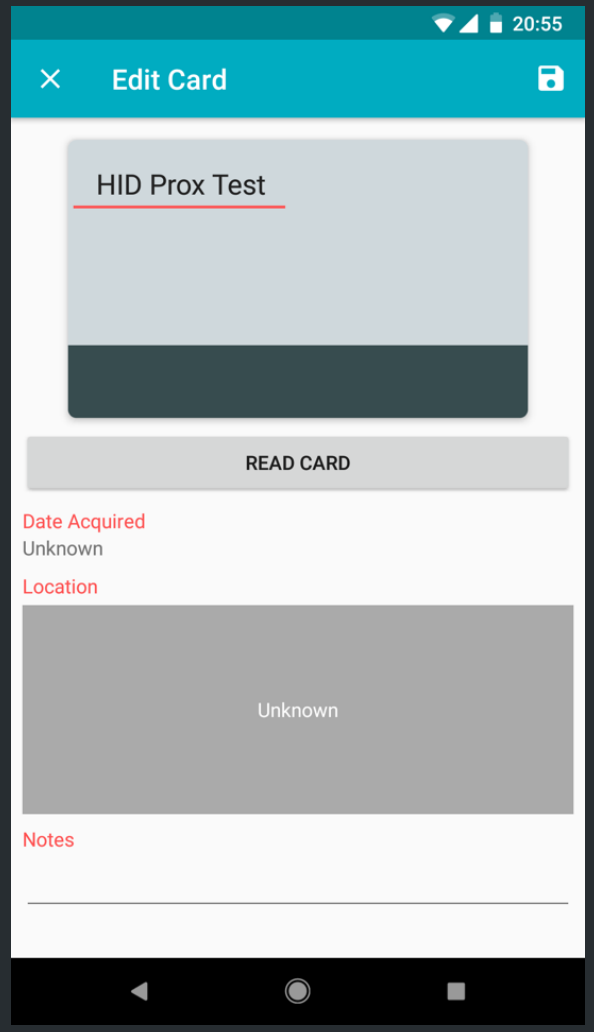
Introducing Walrus

- Walrus provides a common interface for your card cloning devices
- Cards are stored in a common wallet instead of in separate databases
- Reliable card cloning during red team engagements using your Android phone instead of your laptop – much less suspicious
- No need to use your device's limited physical interface or a cumbersome command prompt – use a simple, quick GUI instead
- Easy to use, rated for users aged years 3+ on Play Store

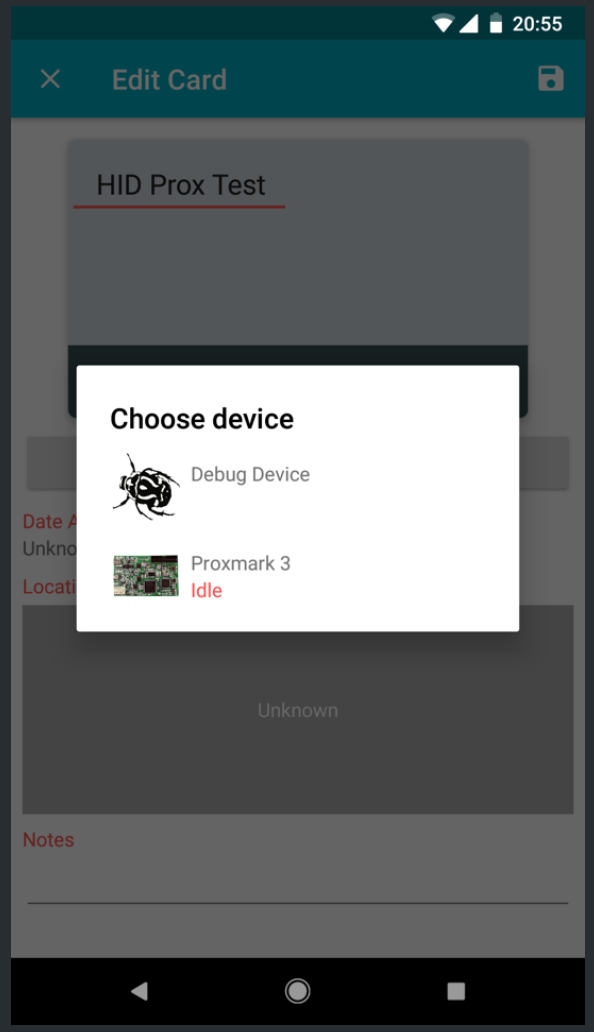
Cloning Cards with Walrus - Proxmark3



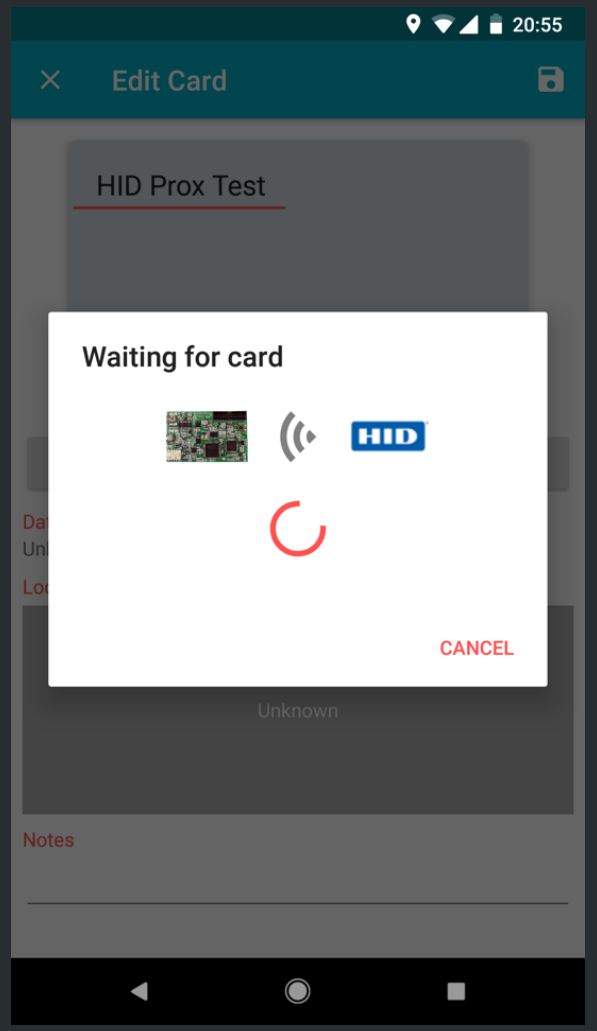
Walrus - Proxmark3



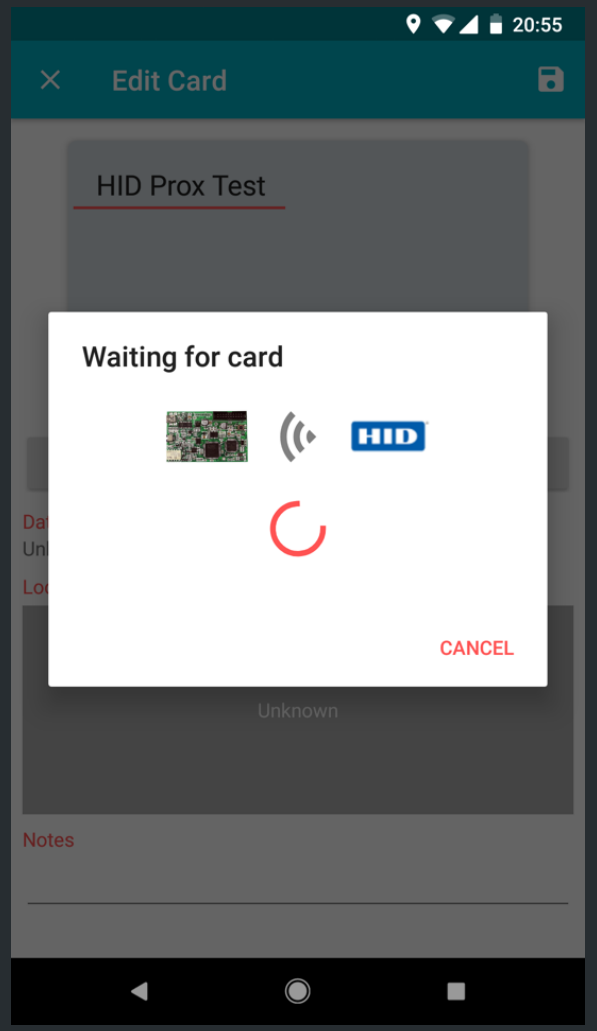
Walrus - Proxmark3



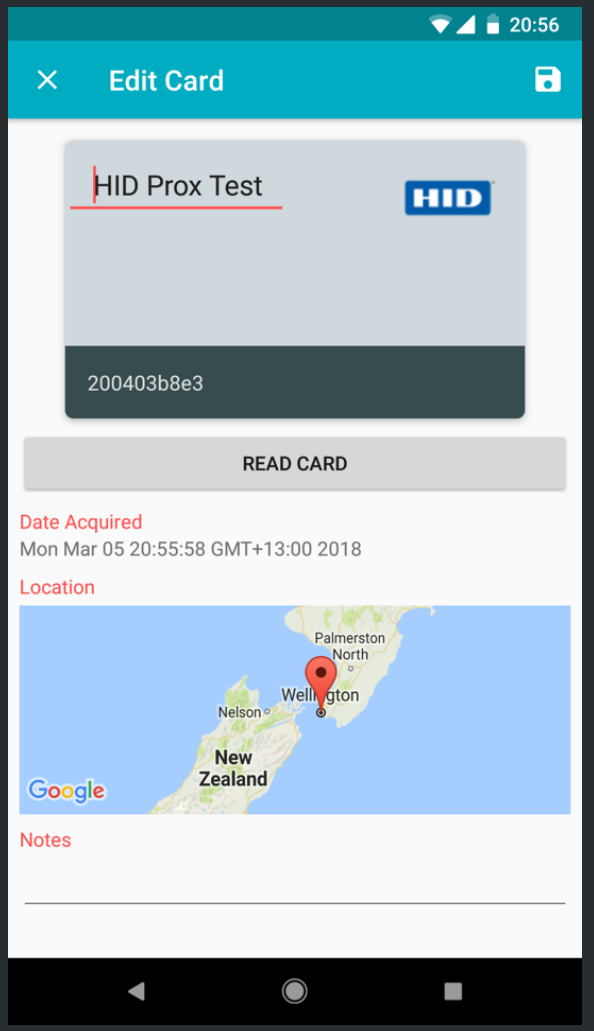
Walrus - Proxmark3



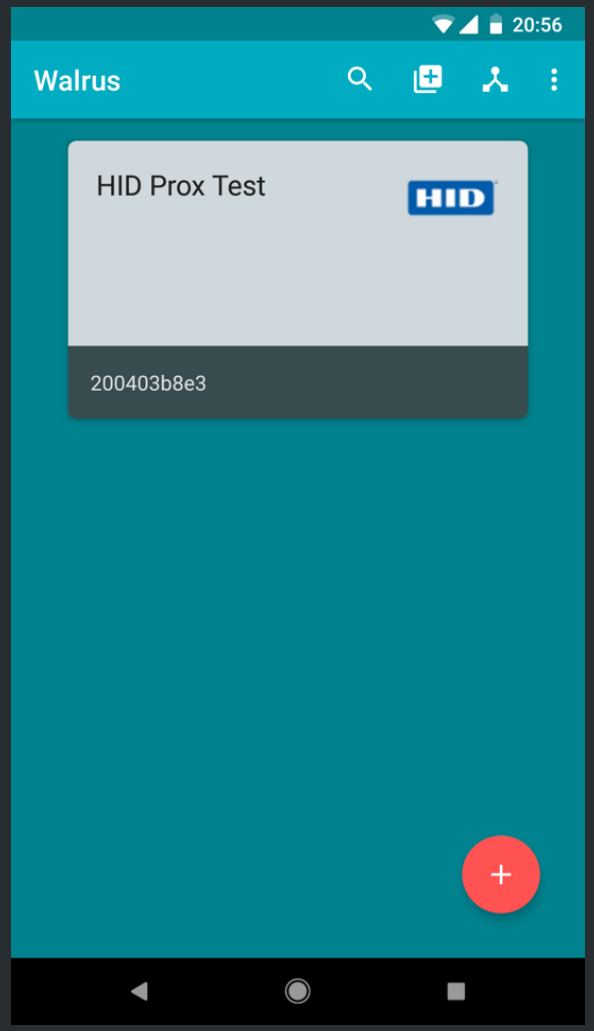
Walrus - Proxmark3



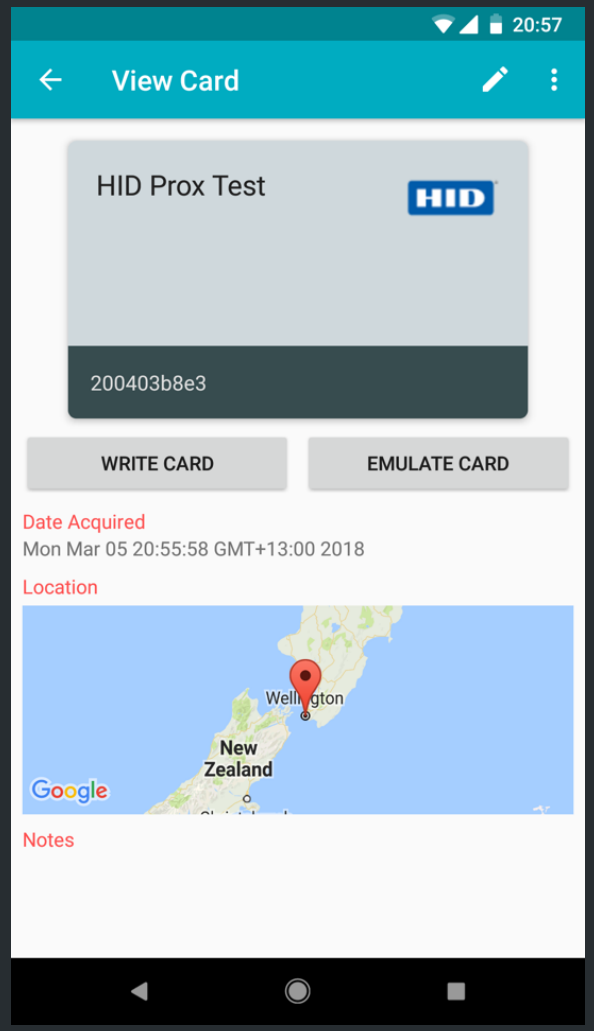
Walrus - Proxmark3



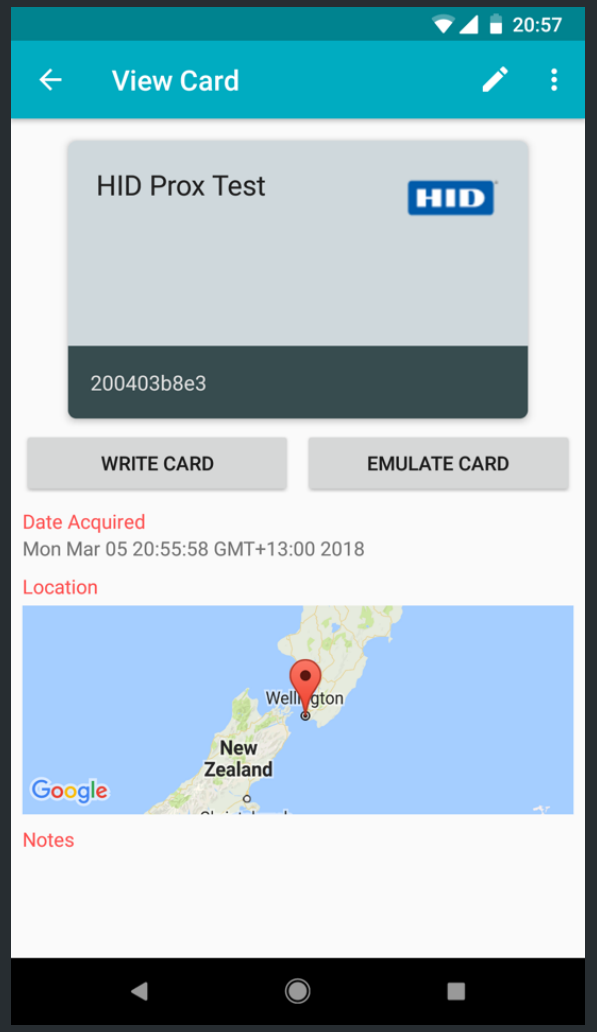
Walrus - Proxmark3



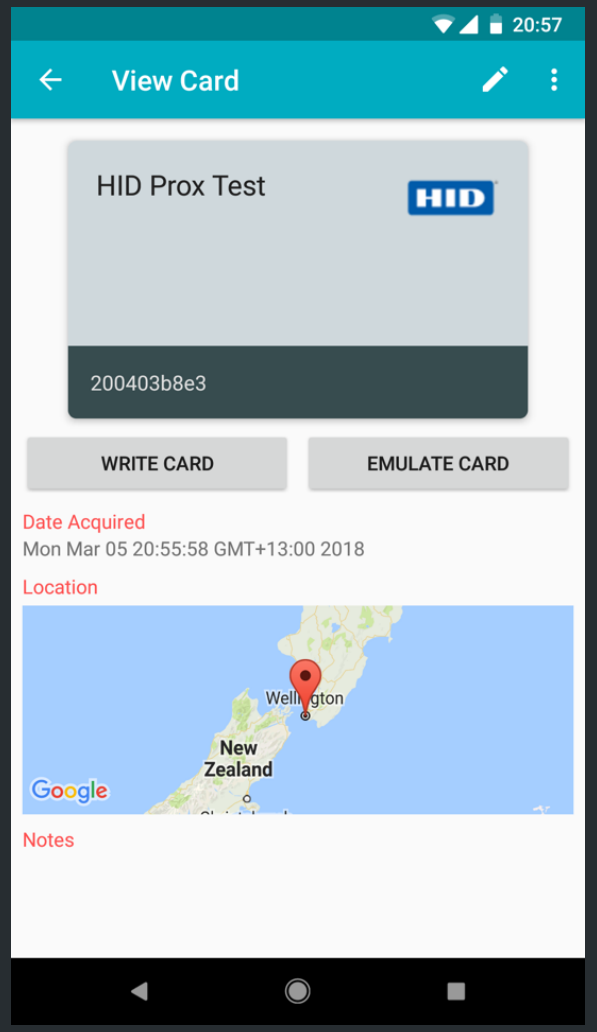
Walrus - Proxmark3



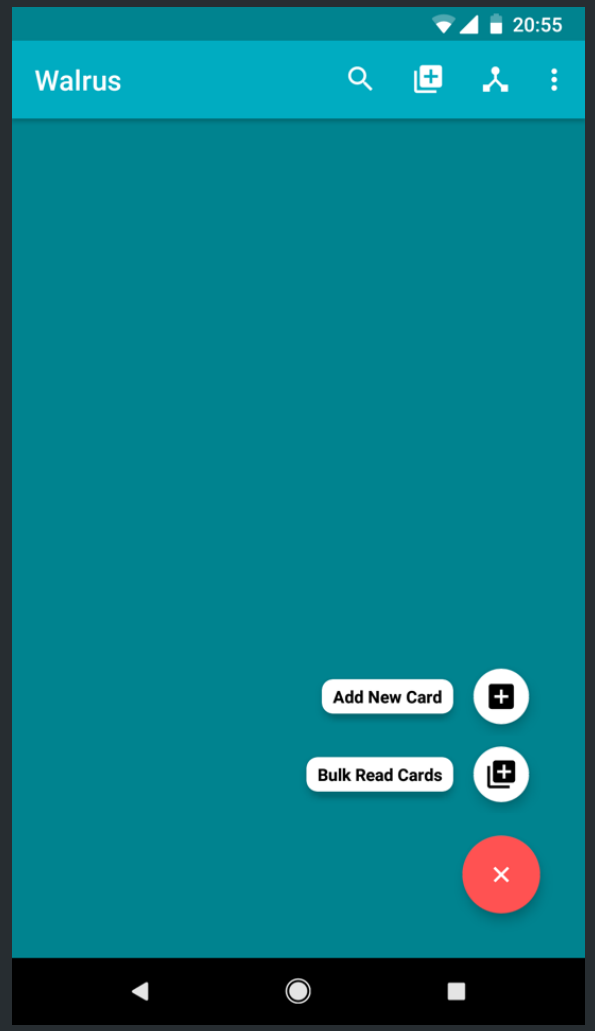
Walrus - Proxmark3

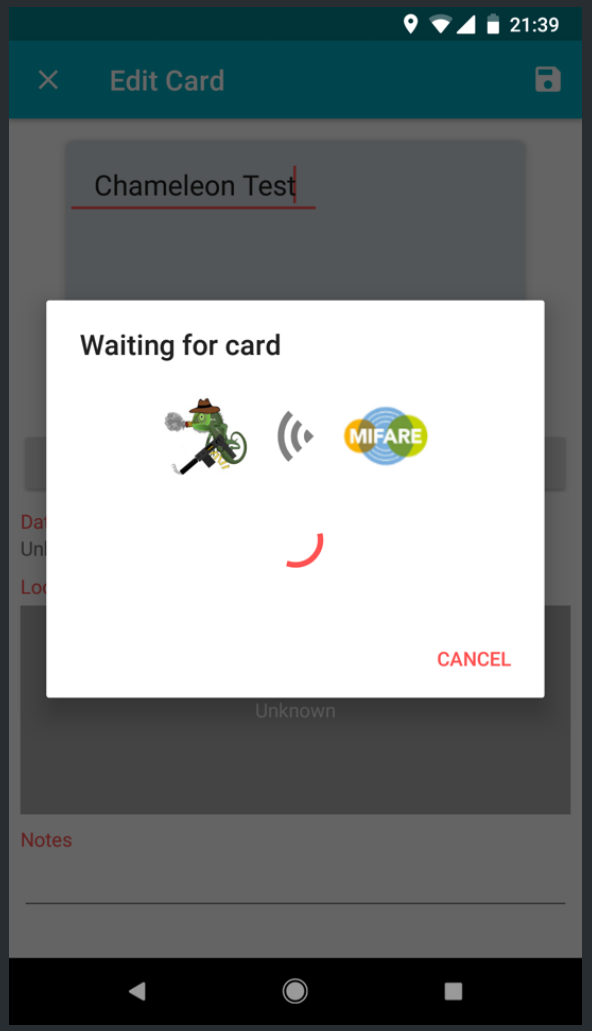


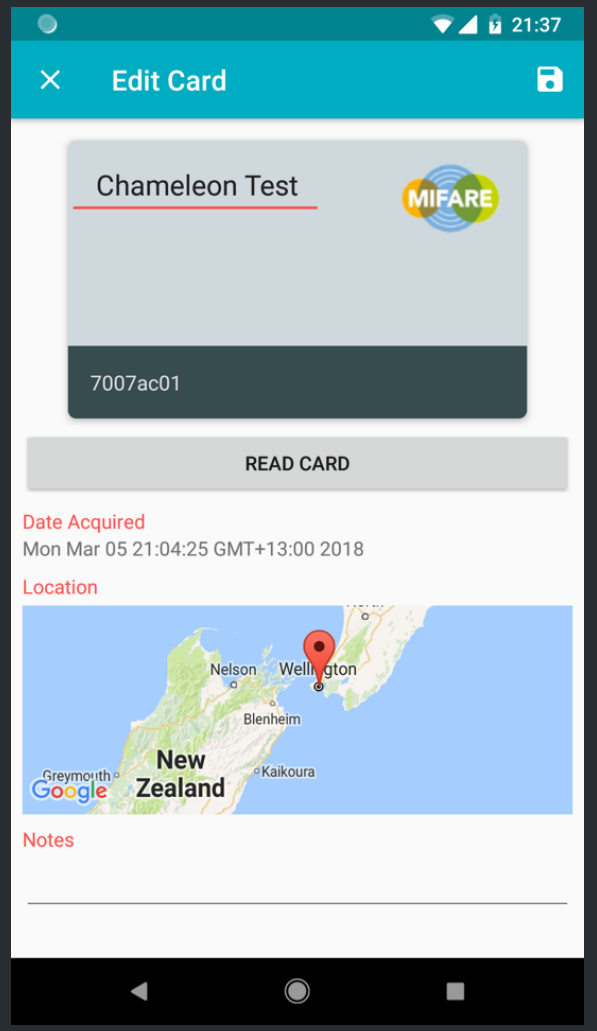
Walrus - Proxmark3



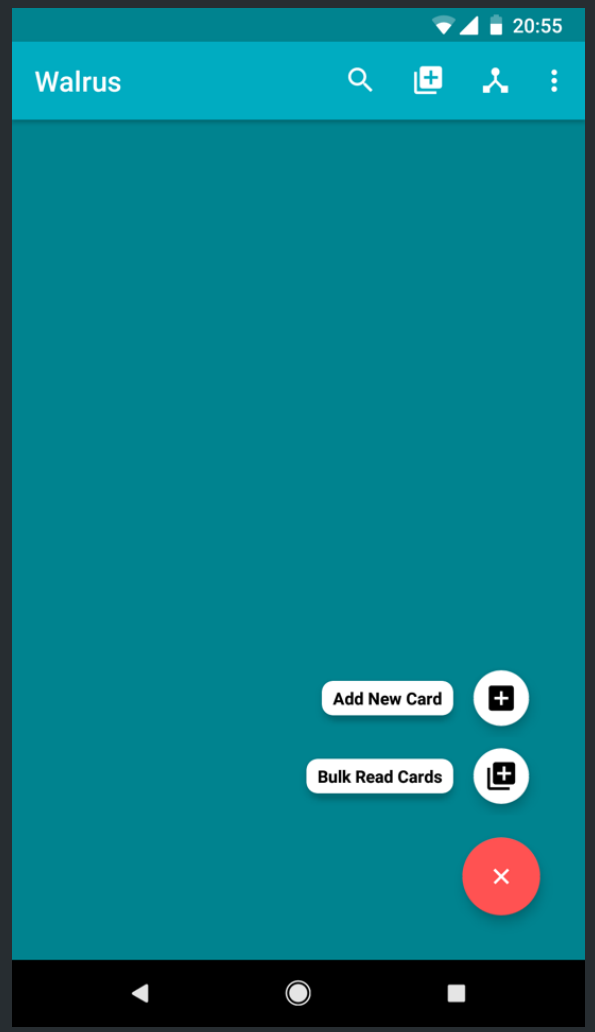
Walrus - Chameleon Mini

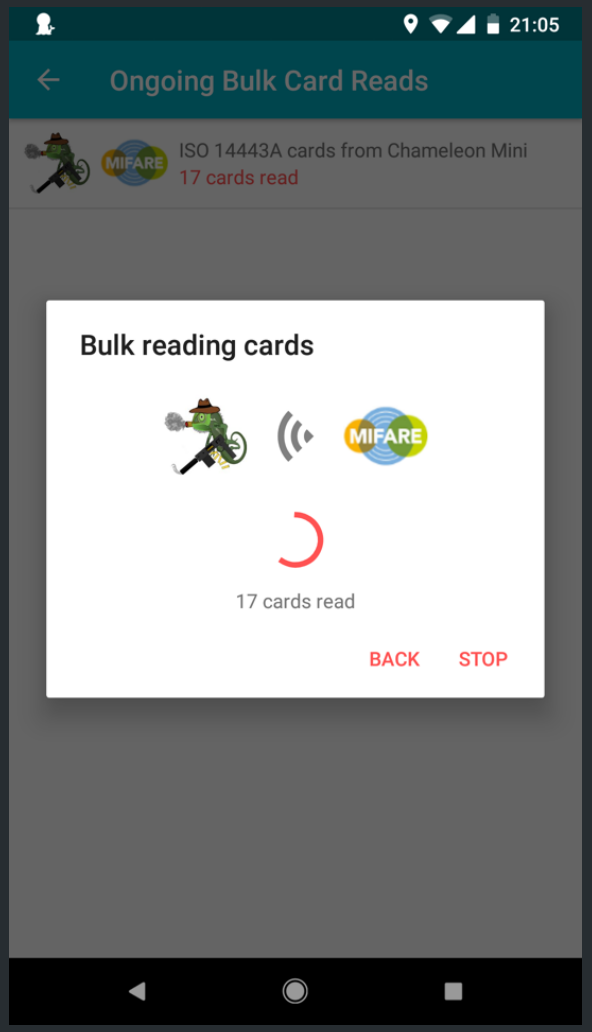


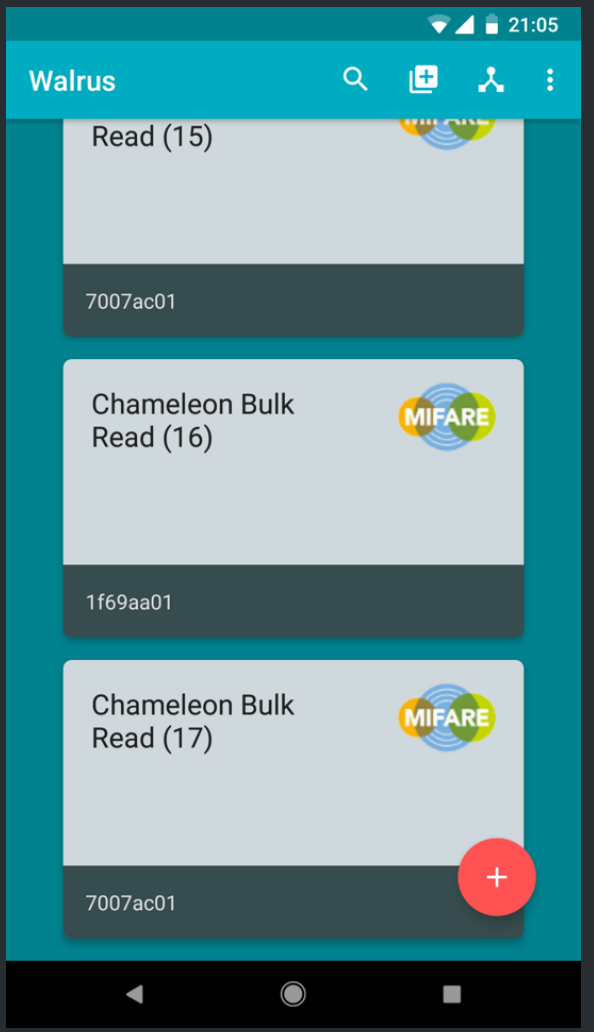




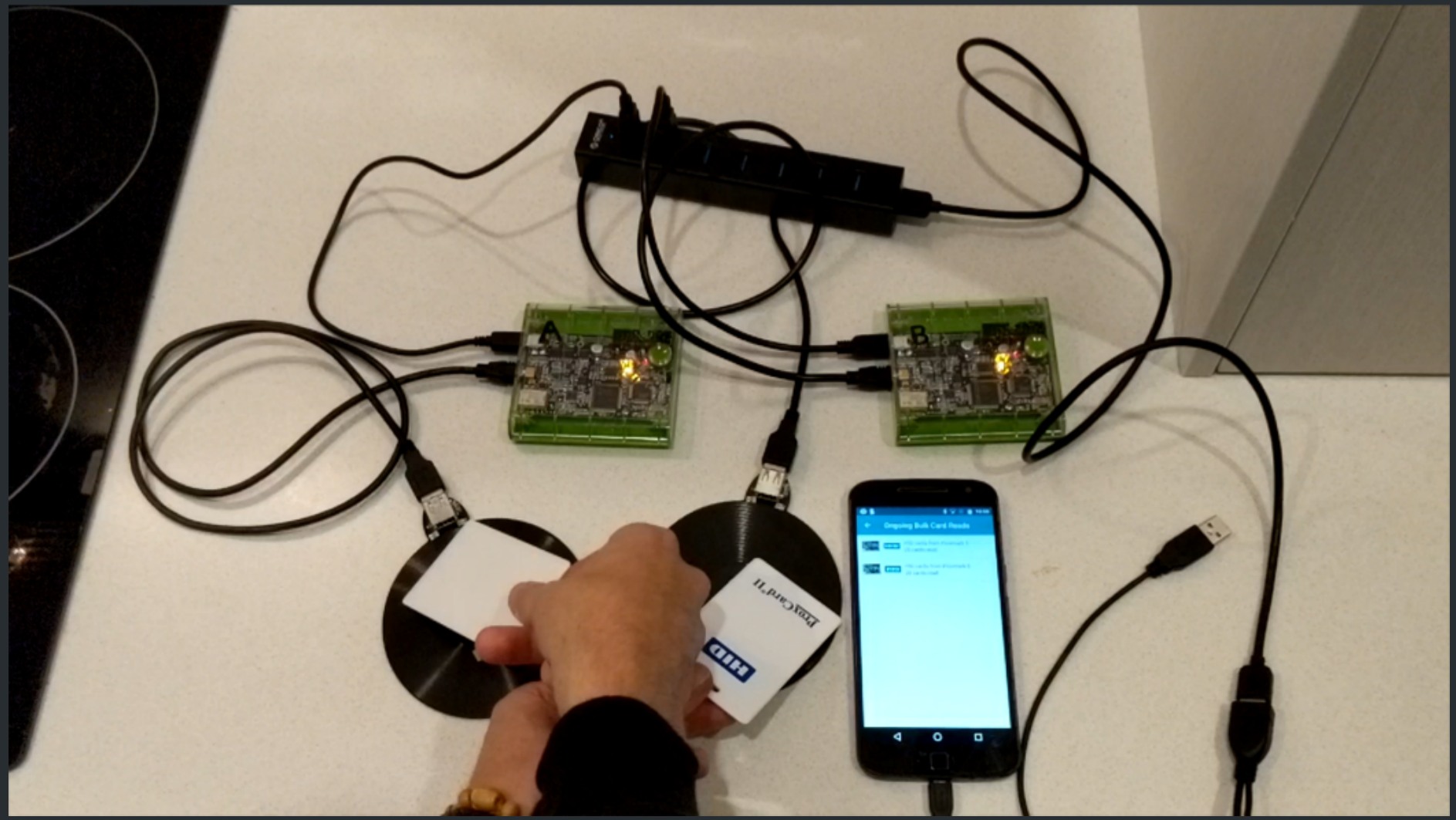
Walrus Bulk Read Mode (Walrus-Driving)



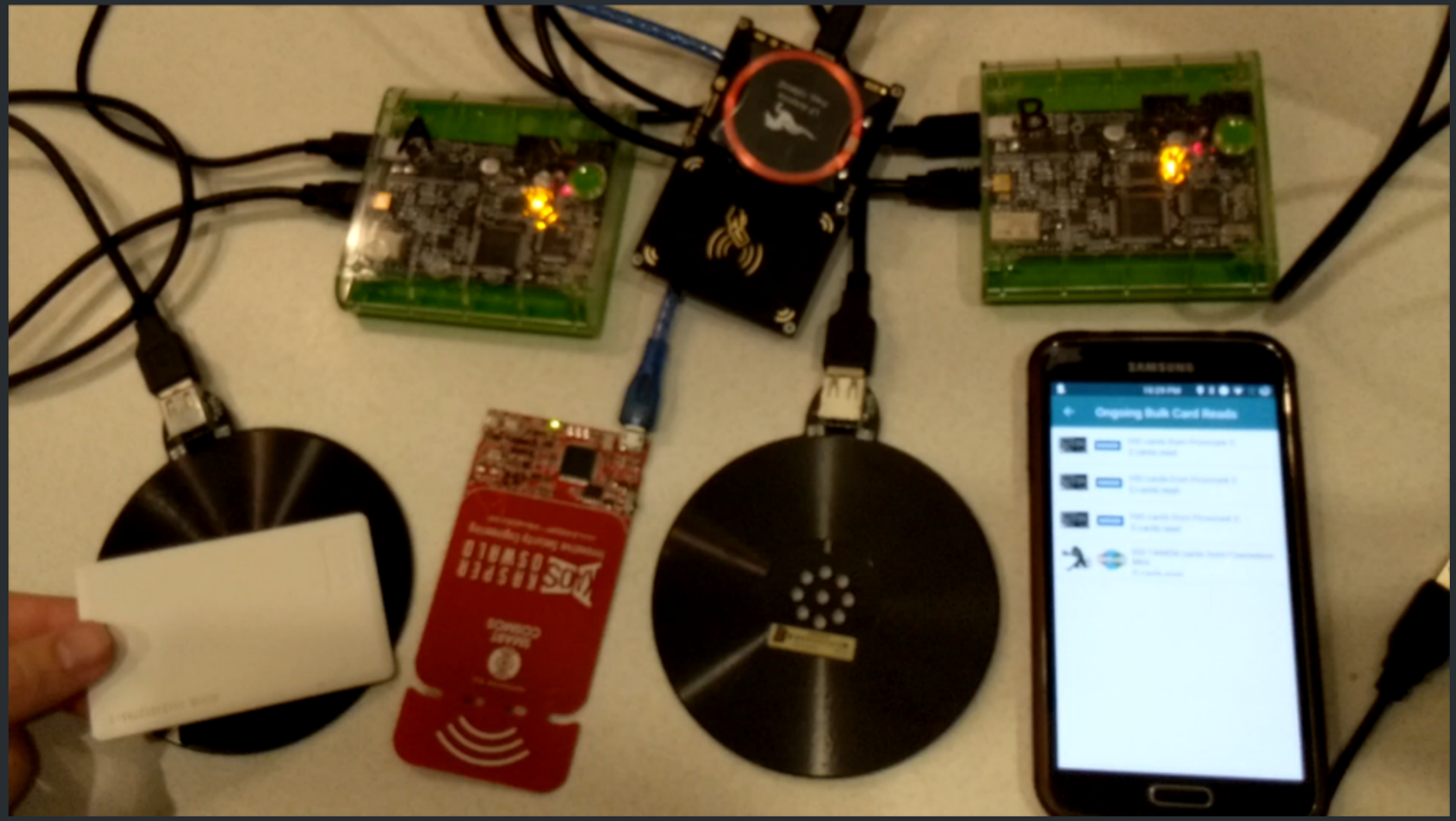




How Many Devices Can It Take?



How Many Devices Can It Take?!



Tastic RFID Thief to Walrus?

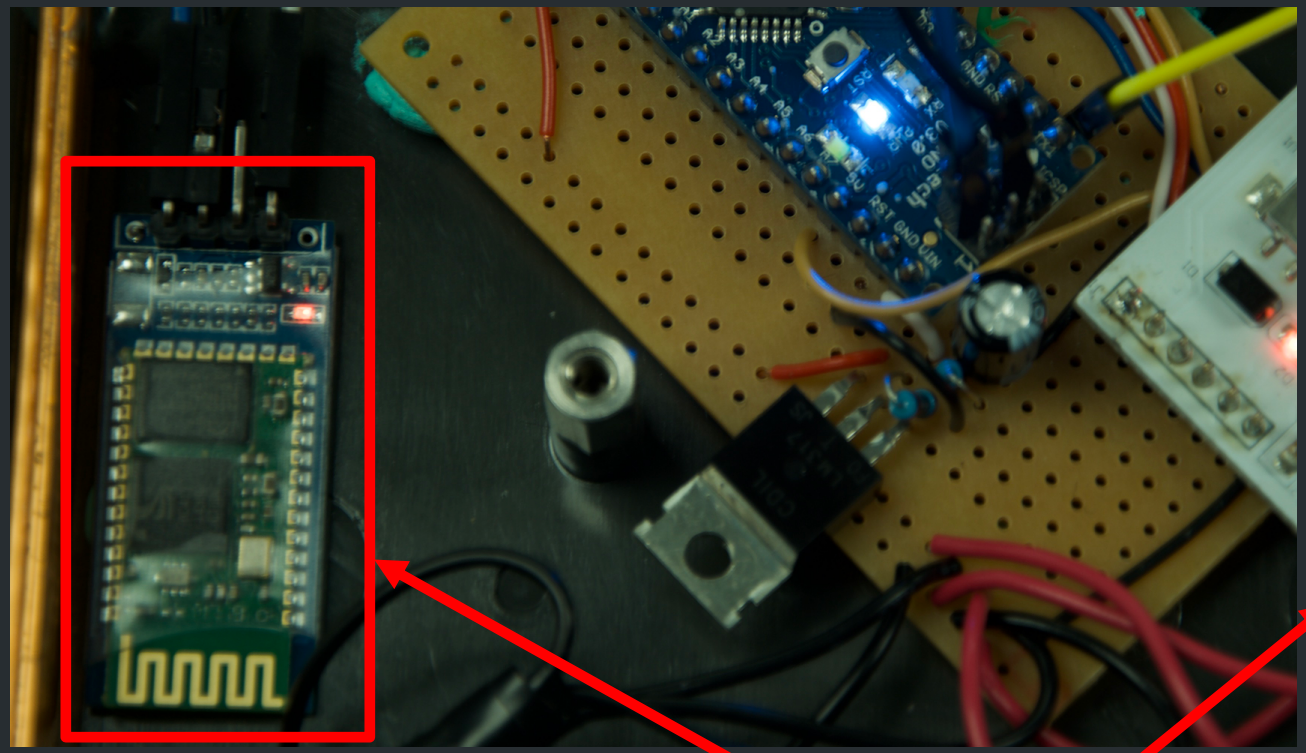
?

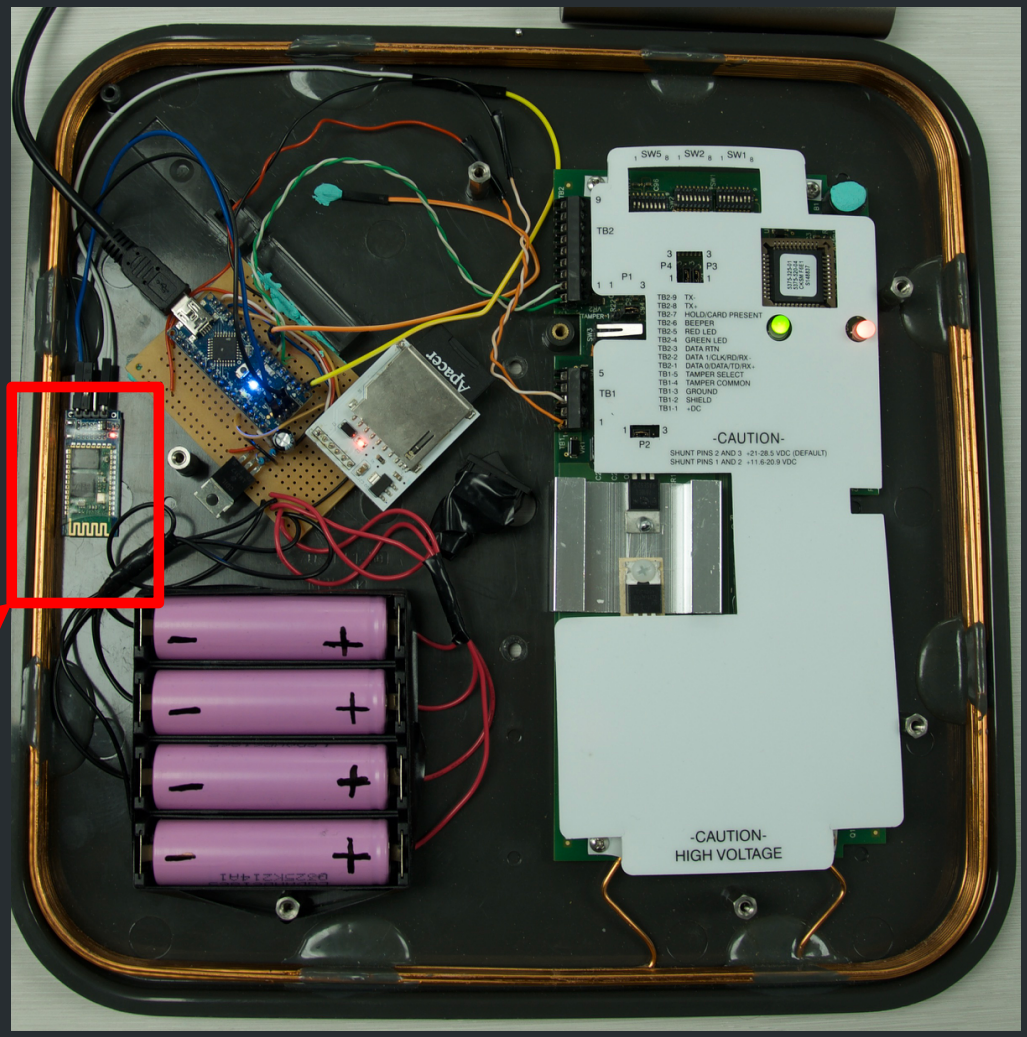
Tastic RFID Thief + Bluetooth

+

HC-06

Tastic RFID Thief BLE Edition





Disclaimer

- Bad actors ahead
- Only clone cards if you have been given permission to do so
- UI is out of date and has been upgraded

Help us Test!

Open alpha release on Play Store now!

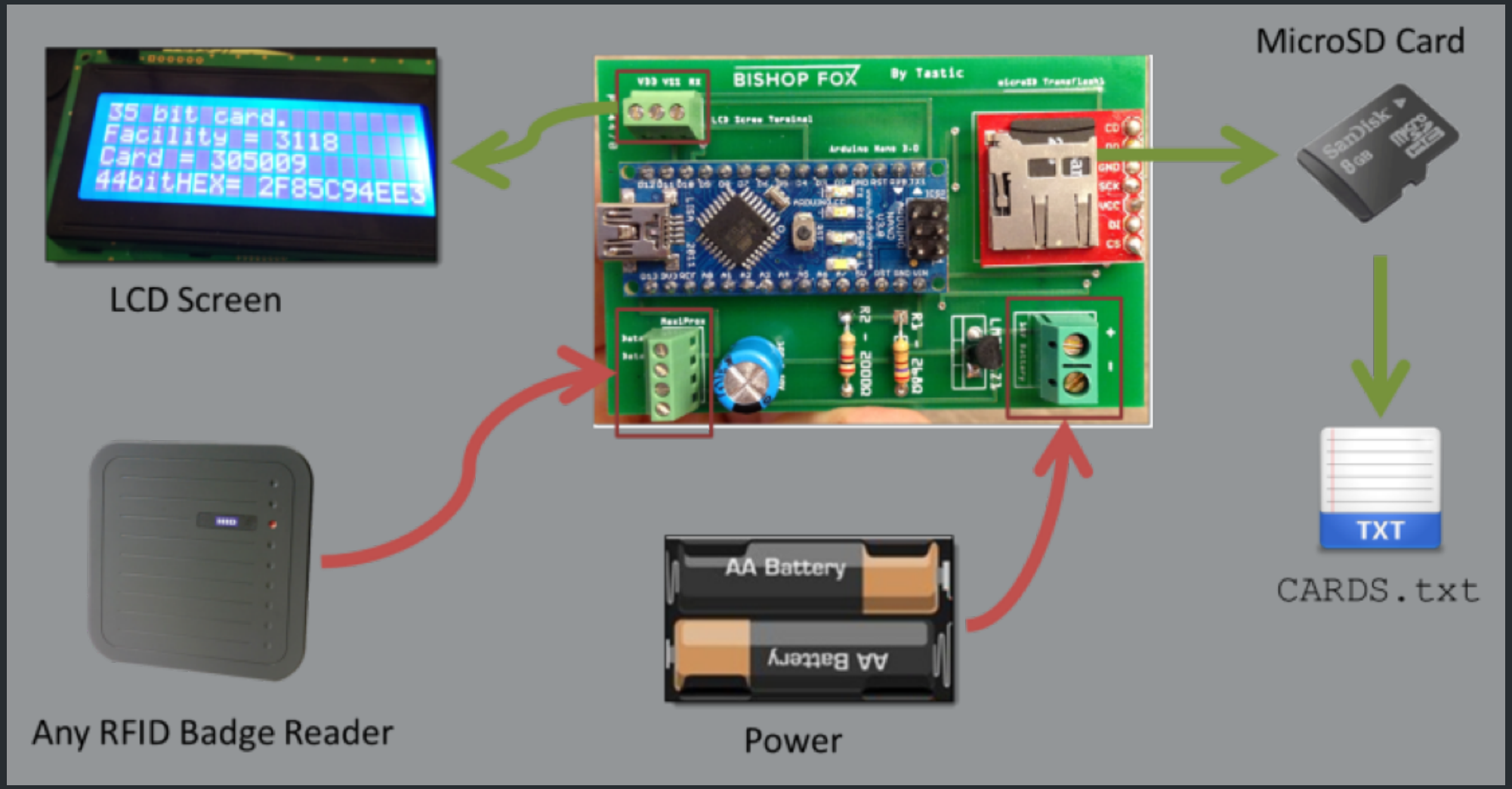
Search for “***Walrus cloning***” or visit

https://play.google.com/store/apps/details?id=com.bugfuzz.android.projectwalrus

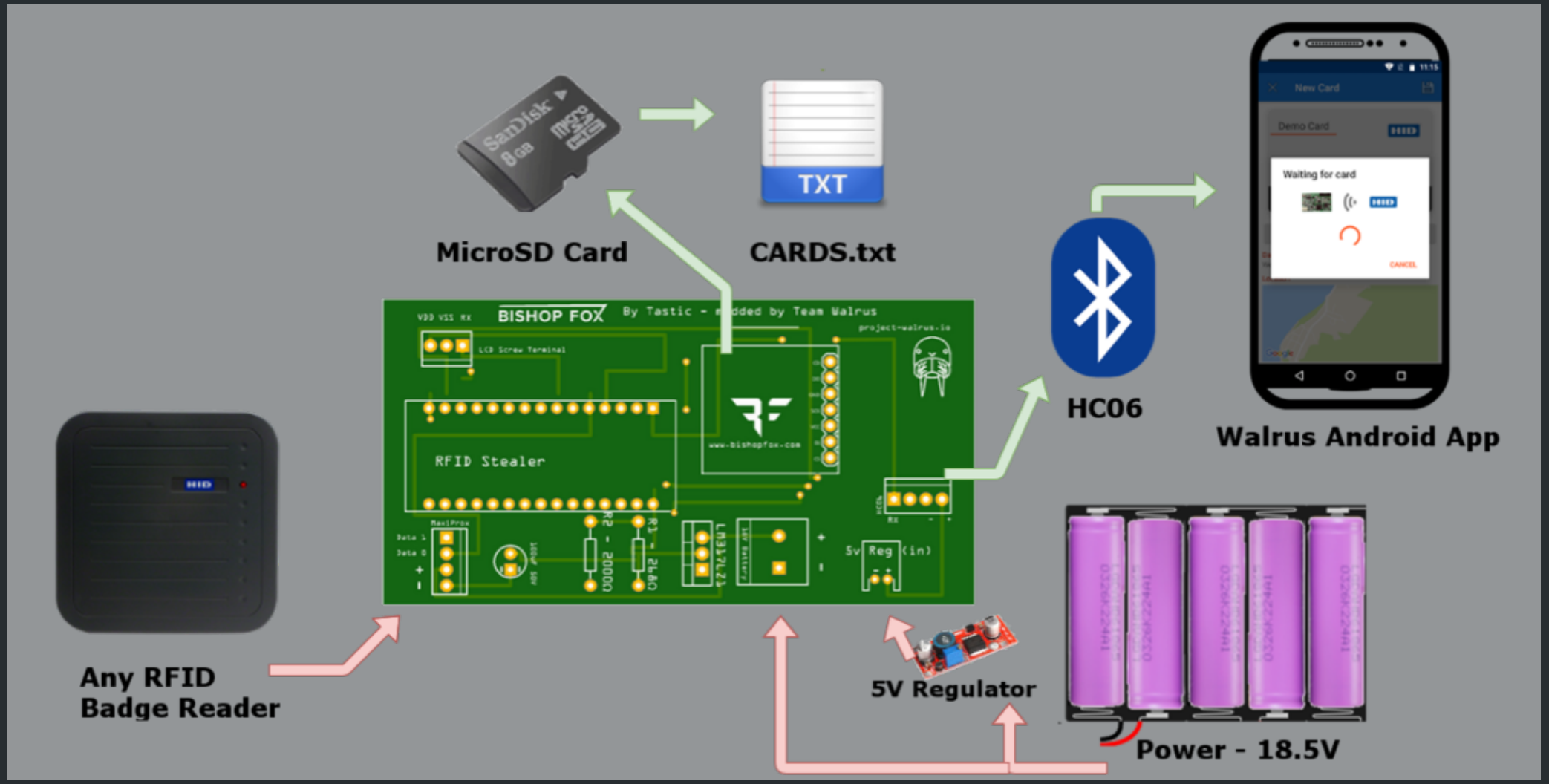
Future Plans

- Modify the Bishop Fox Tastic RFID Thief PCB
- Add features:
  - ❑ Brute force emulation mode
  - ❑ Sharing cards between Android devices
  - ❑ Gamification?
- Add support for additional devices:
  - ❑ Generic Wiegand support via Team Walrus Arduino software
  - ❑ Magspoof
  - ❑ BLEKey
  - ❑ ESP-RFID-Tool
  - ❑ More?

Tastic RFID Thief PCB

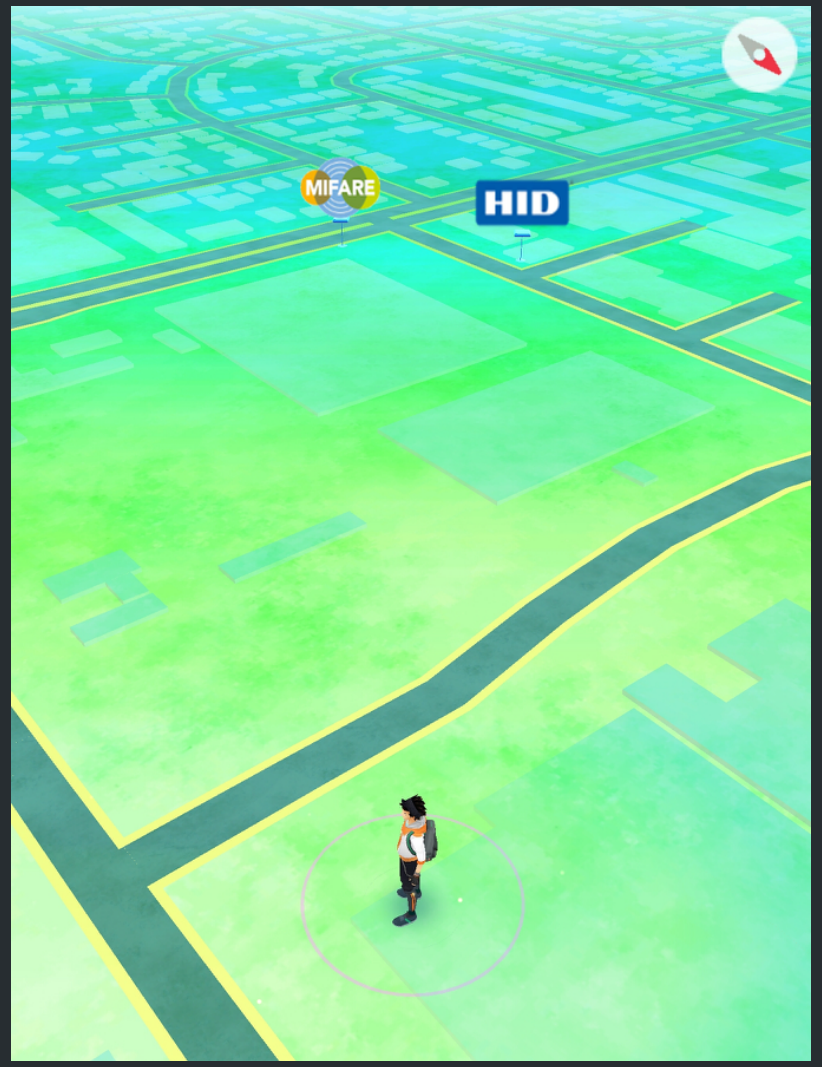


PCB Modification



Gamification (Maybe)

- Wie-Gotta Catch ‘em All
- Not a public database



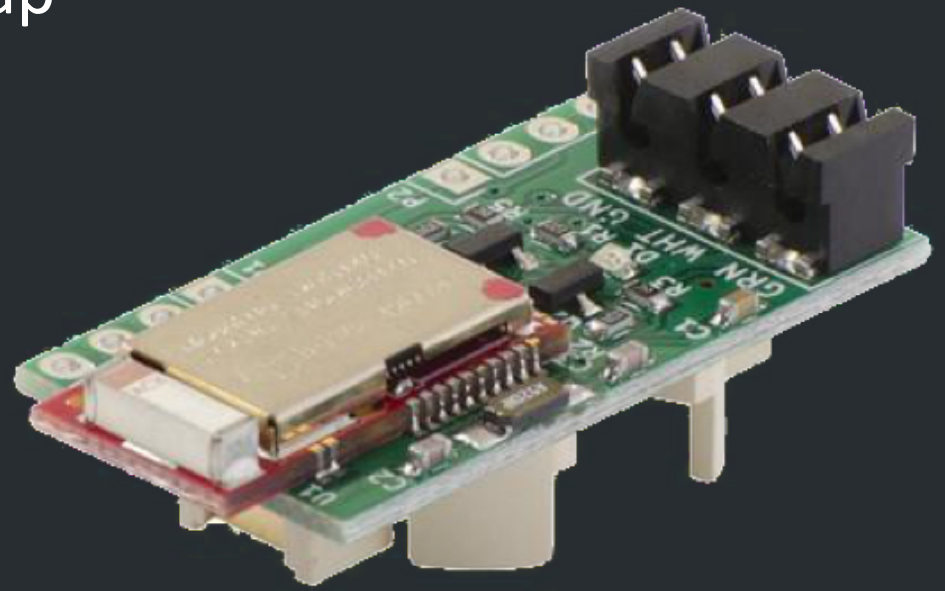
MagSpoof v2

- Created by Samy Kamkar
- Commercialized by Rysc Corp
- Emulate magnetic stripe or credit card data

HTTPS://SAMY.PL/MAGSPOOF/
HTTPS://STORE.RYSCC.COM/PRODUCTS/MAGSPOOF

BLEKey

- Created by Mark Baseggio and Eric Evenchick
- A Bluetooth Low Energy (BLE) enabled tap for the Wiegand devices
- Installed in a reader to passively sniff Wiegand data
- Data can be offloaded to a phone via Bluetooth
- Inject card data
- Cheap
- Emulate cards on that reader



HTTP://WWW.BLEKEYRFID.COM/

ESP-RFID-Tool

- Created by Corey Harding
- A Wi-Fi enabled tap for the Wiegand devices
- Installed in a reader to passively sniff Wiegand data
- Data can be offloaded to a phone via Wi-Fi AP
- Inject push-to-exit signal
- Cheap

HTTPS://GITHUB.COM/RFIDTOOL/ESP-RFID-TOOL
HTTPS://BLOG.APRBROTHER.COM/PRODUCT/ESP-RFID-TOOL

Thank you!

Getting Started:
http://project-walrus.io

Open alpha release on Play Store now:

https://play.google.com/store/apps/details?id=com.bugfuzz.android.projectwalrus

Open source (GPLv3). Code is on Github:

https://github.com/megabug/Walrus