RAVENHID: REMOTE BADGE GATHERING

Lucas Morris @lucasjmorris
Adam Zamora @azdmin

About Us

- Lucas Morris
  - Manager at Crowe Horwath LLP
  - “Manager”, Pentester, Code Monkey
- Adam Zamora
  - Senior Consultant at Crowe Horwath LLP
  - Pentester, [something funny here]

Crowe Horwath

Our Plug (cont.)

- **Lucas Morris**
  -  => emperorcow@gmail.com
  -  => @lucasjmorris
  -  => github.com/emperorcow

- **Adam Zamora**
  -  => ninjazamo@gmail.com
  -  => @azdmin

- https://github.com/emperorcow/ravenhid
- https://www.oshpark.com/shared_projects/Kp0nErMB

Crowe Horwath

Overview

- RFID Refresher
- Physical Access Control Systems
- Our Methodology
- Mitigation and Remediation
- Tools!

Radio Frequency Identification (RFID)

- Low Frequency – Used without license
  - Various identification and data collection
- High Frequency
  - Smart Cards, product identification
- Ultra-High Frequency
  - Supply chain tracking, defense applications

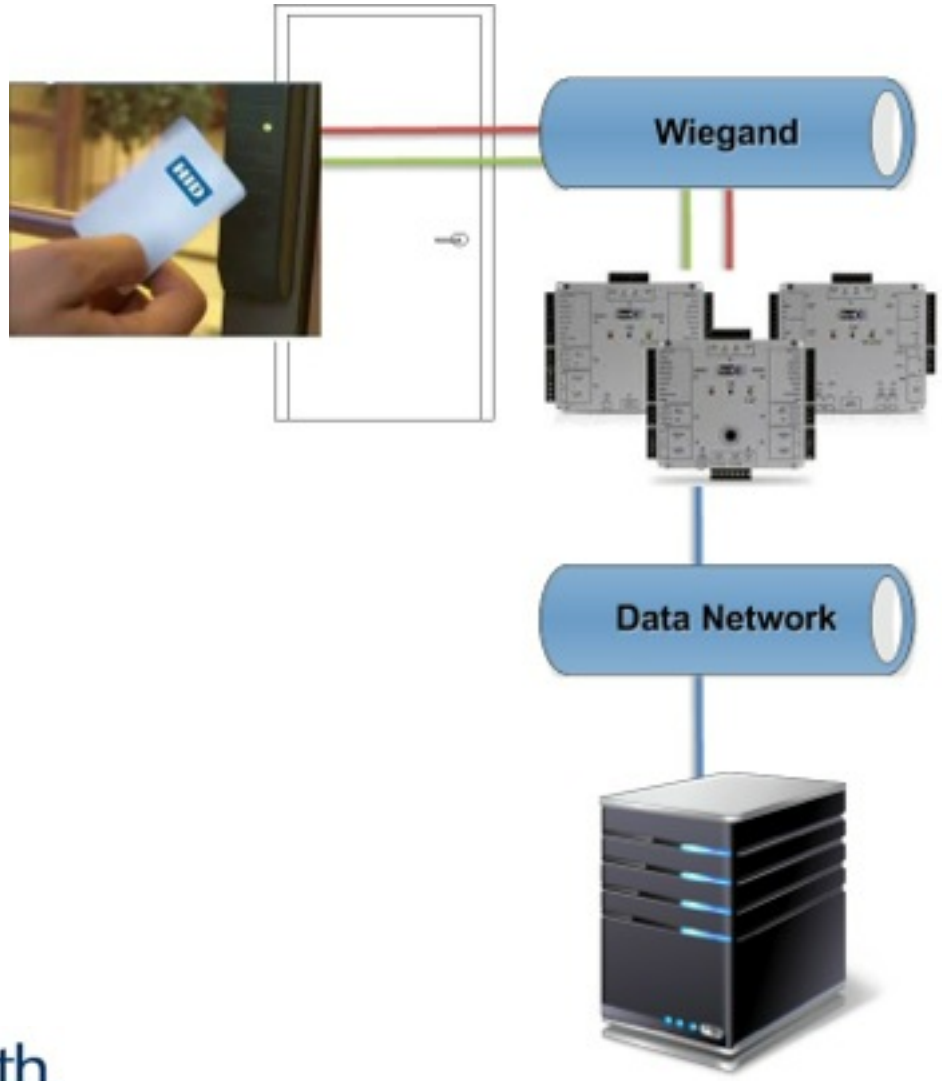
Type	Frequency
LF - Low Frequency	***126 kHz***
HF - High Frequency	***13.56 MHz***
UHF - Ultra High Frequency	***433 MHz***

Physical Access Control

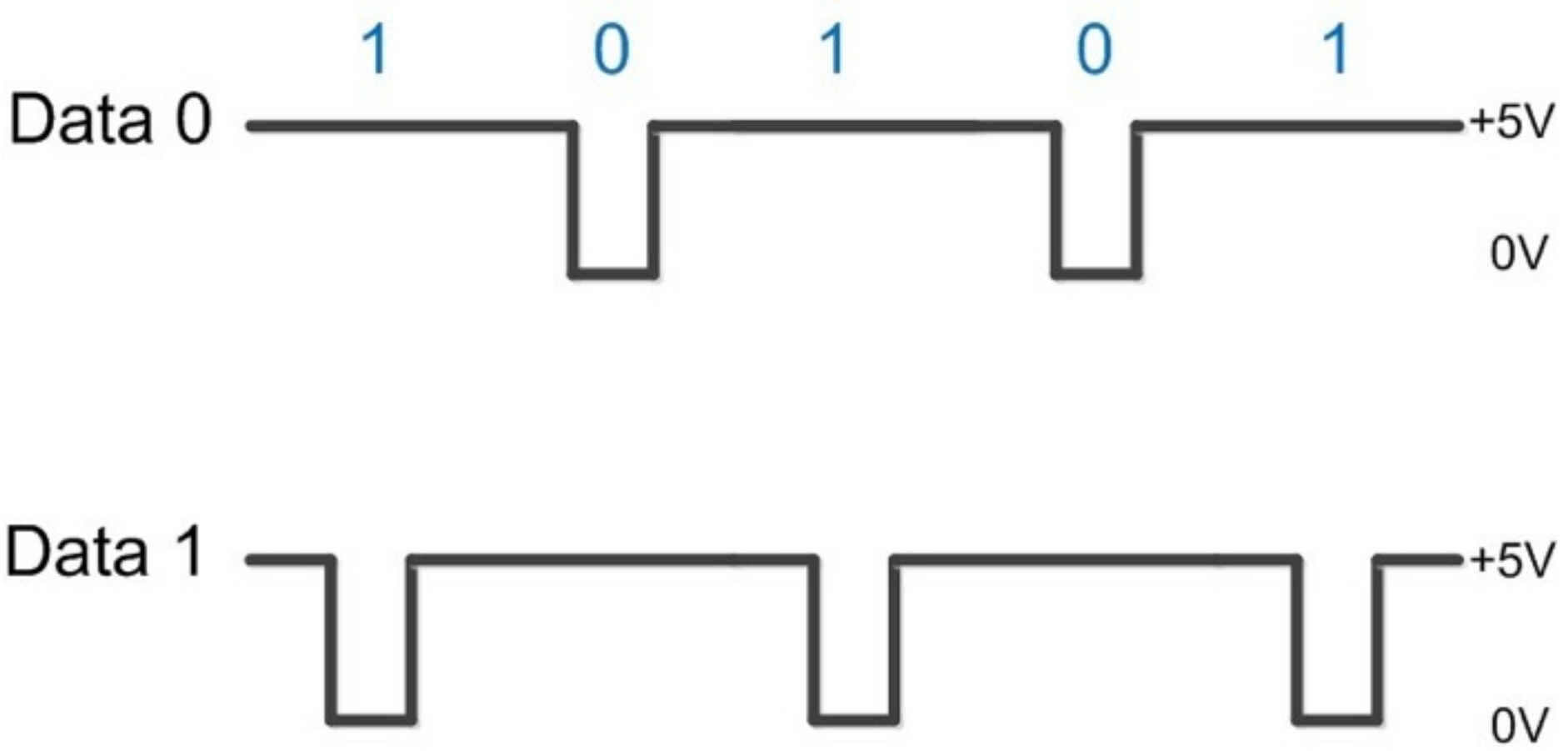
- Low Frequency proximity encompasses 80%+
  - Education Facilities
  - Financial Institutions
  - Medical Facilities
  - Government/Municipalities

- Blank cards (T5577) cost between $0.30 – $1.00 each

How Most Doors Work



How Weigand Works



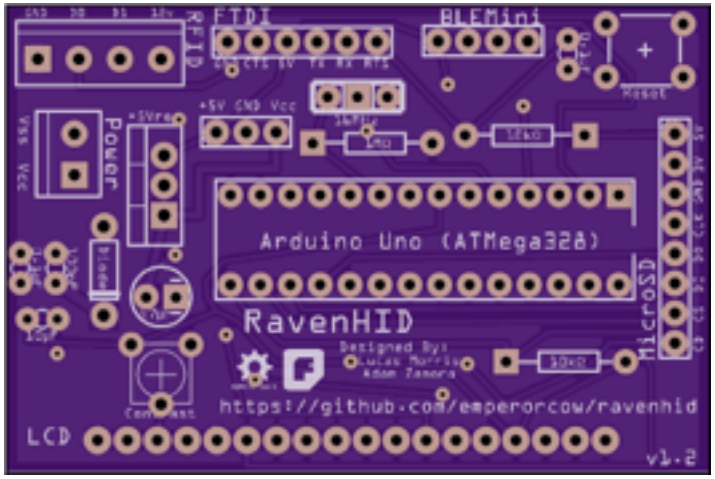
Crowe Horwath

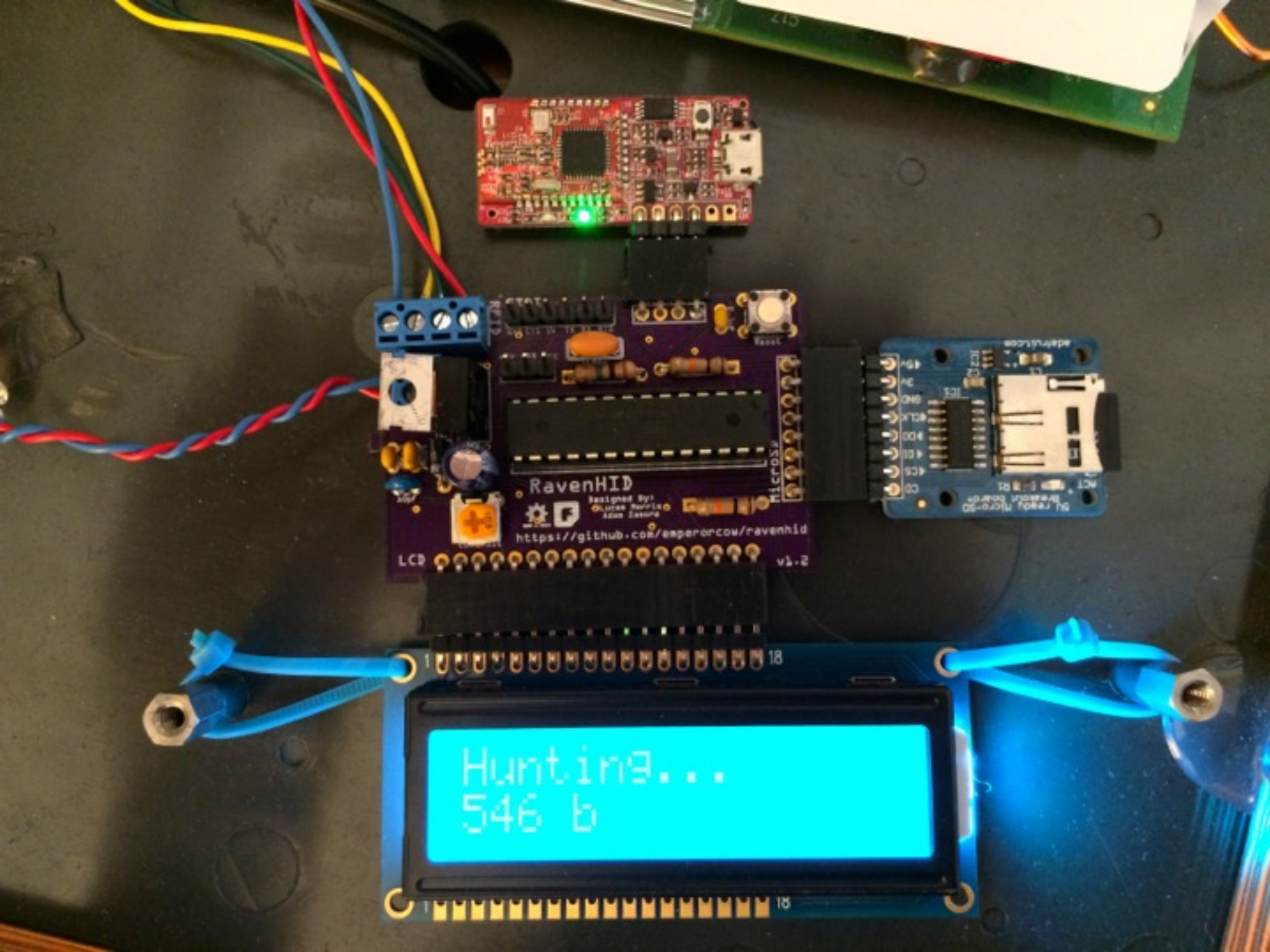
Our Methodology

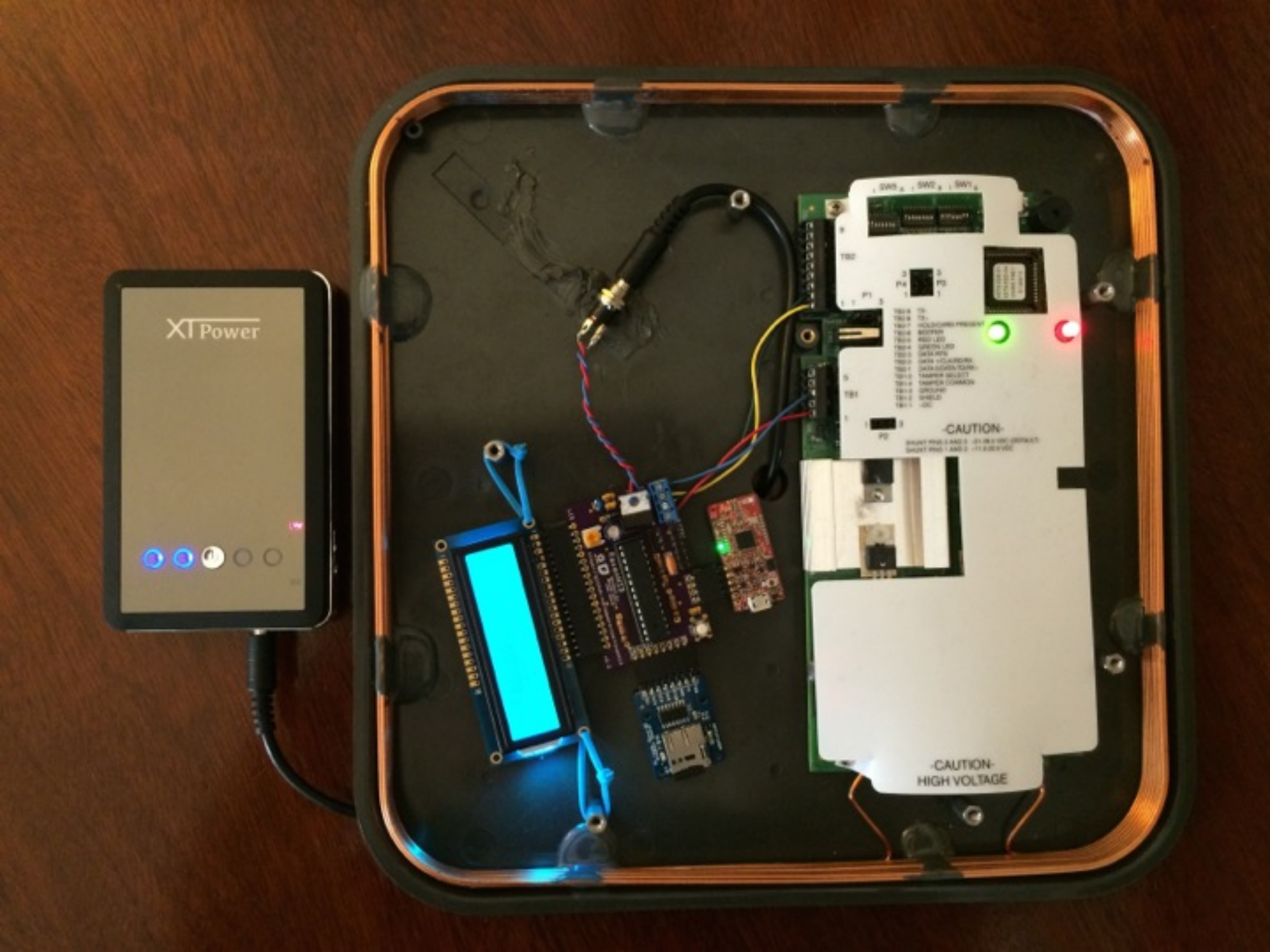
- Identify our targets
  - Shared building
    - Have a lookout for reader to tail
    - Find a common area
    - Patience (and bathrooms!)
- Clone stolen badge (Proxmark)
- Brute-force sequential IDs if necessary

Our Device

- Based on several Internet designs
- Lots of outputs supported (LCD, RGB LCD, BLE, SD Card)
- Application for Phone management (BLE)
- Through hole components for ease of assembly




RavenHID
https://github.com/emperorcow/ravenhid
LCD
v1.2
Hunting...
546 b


XT Power
-CAUTION-
-CAUTION-
HIGH VOLTAGE

Demo!

Mitigation and Remediation

- Badge Protection
- User Education
- Multi-Factor Readers
- Newer Badge Systems?

Questions?

- **Lucas Morris**
  -  => emperorcow@gmail.com
  -  => @lucasjmorris
  -  => github.com/emperorcow

- **Adam Zamora**
  -  => ninjazamo@gmail.com
  -  => @azdmin

- https://github.com/emperorcow/ravenhid
- https://www.oshpark.com/shared_projects/Kp0nErMB

Crowe Horwath