

# Physical access control systems

Zachary Crandall

# Agenda

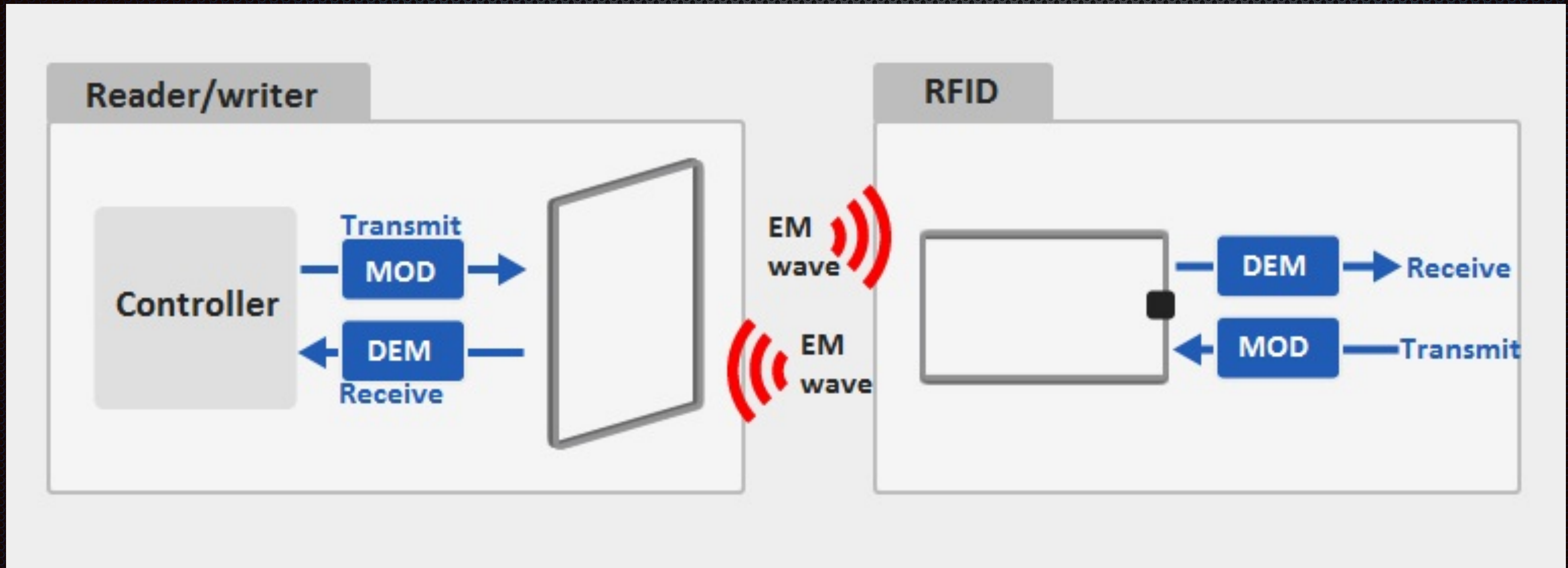
- ✦ Different Types
- ✦ ICLASS GL
  - ✦ System Configuration
  - ✦ Common Vulnerabilities
  - ✦ How to Clone them using a proxmark3
- ✦ Other Types and How to clone them
- ✦ References

# Different Types

- ✦ Magstripe
- ✦ HID
- ✦ HITAG
- ✦ Mifare
- ✦ NFC
- ✦ LEGIC

- ✦ ICLASS
  - ✦ GL
  - ✦ SE
  - ✦ Seos

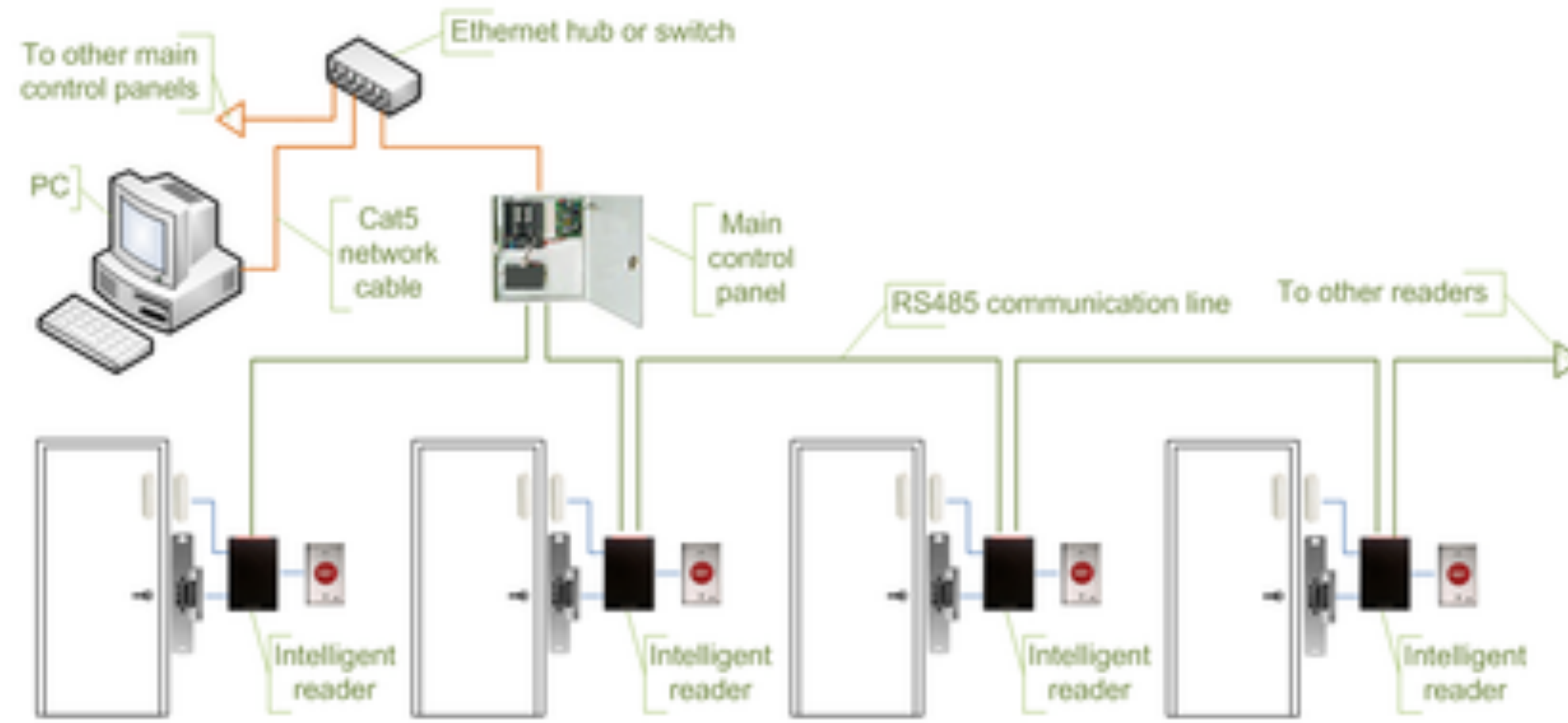
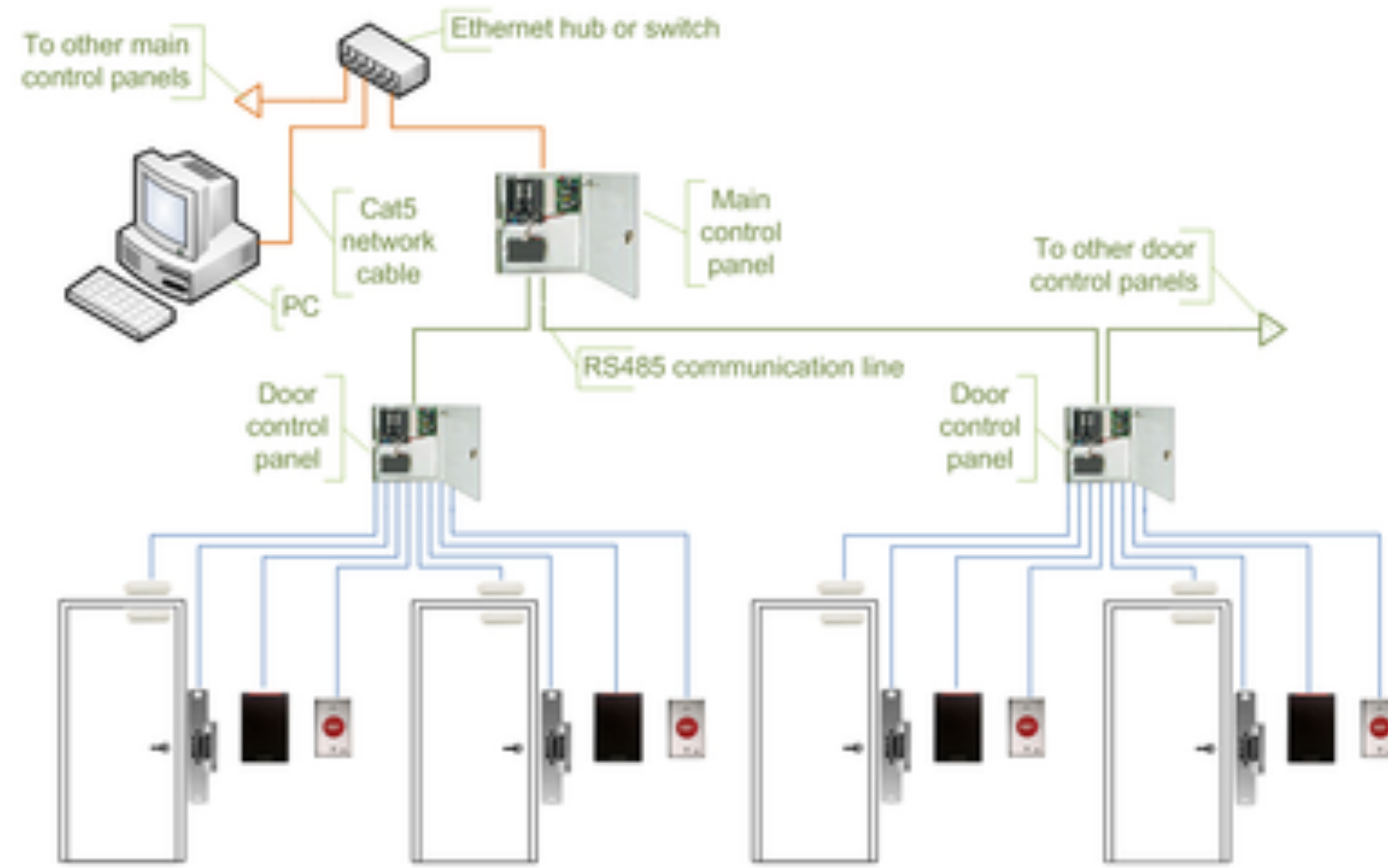
# Basic interaction



# ICLASS GL

- ✦ Use 13.56Mhz range
- ✦ One of the most widely used
- ✦ Readers and writers use a shared key
- ✦ Talks to a central server





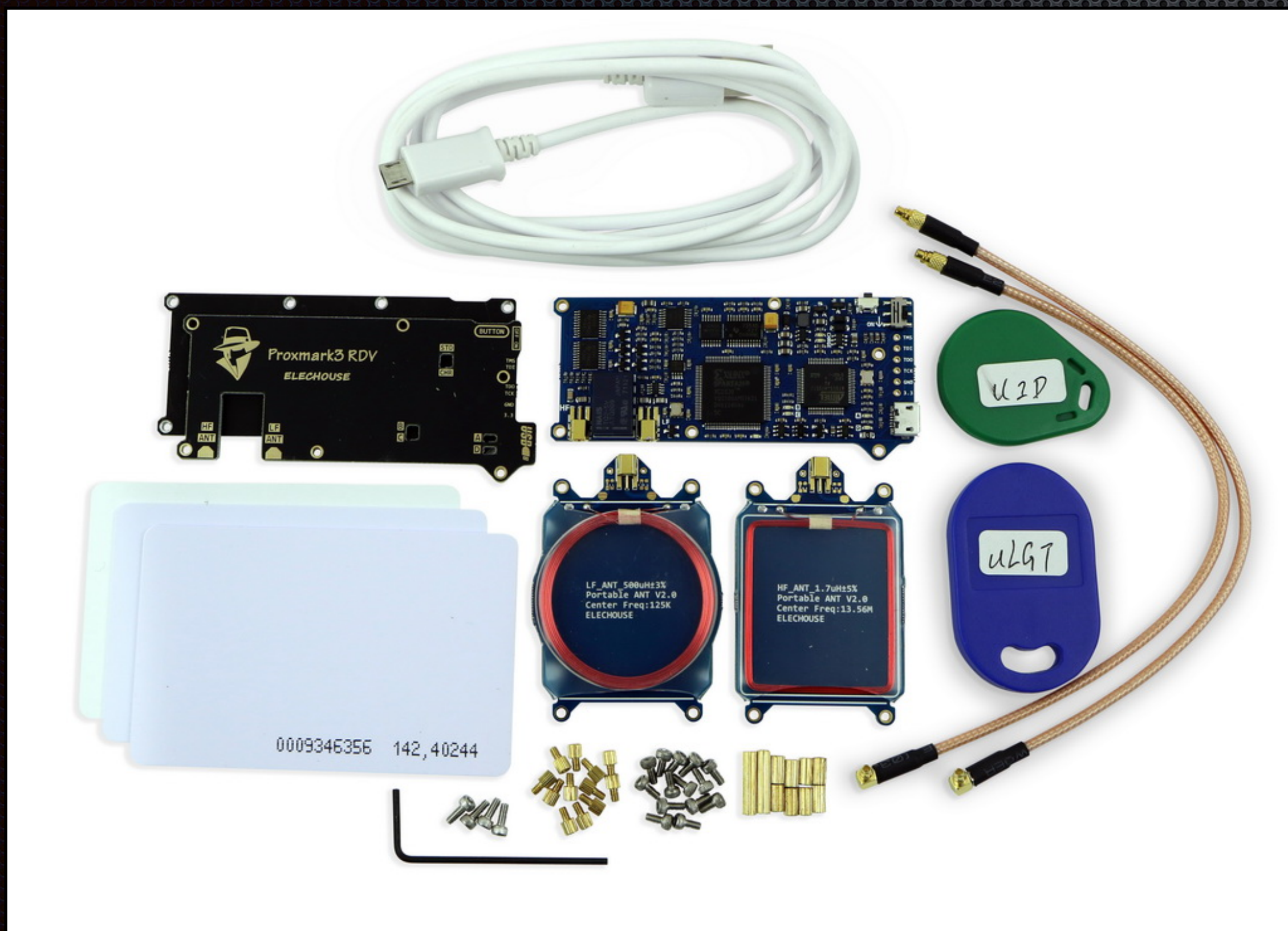
# ICLASS - Vulnerabilities

- ✦ S.E. - Steal someones card
- ✦ Default Keys
  - ✦ Most readers have them if not configured
  - ✦ Can be obtained by reverse engineering a reader
  - ✦ or Twitter...

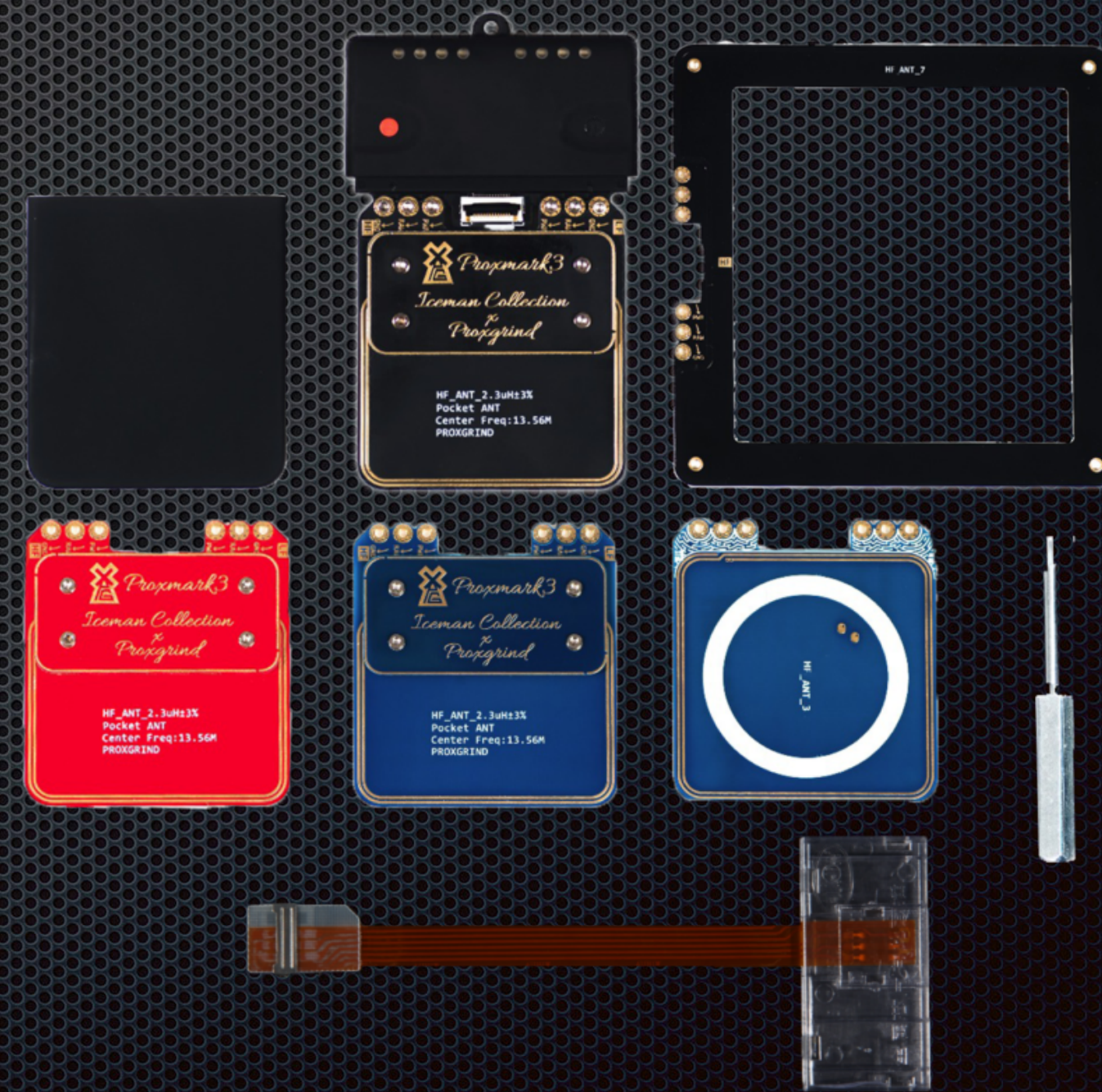


# Proxmark3

## ✦ RDV2



## ✦ RDV4





# A little about the Proxmark

- Supports 125khz, 134khz, and 13.56
- Can be used in stand alone mode to capture and replay
- IT'S OPEN SOURCE!!!
- Must flash firmware to change from low to high frequency
- Only works standalone for non-encrypted cards

# What if they changed the Keys

- ✦ What you need
  - ✦ A computer (can be a Raspberry Pi) and a Proxmox3
  - ✦ A writable ICLASS card (optional)
- ✦ Find a reader that is accessible discreetly

# How do we get the key

- ✦ With the Proxmark hooked up to a computer using the cli
- ✦ Start by using it to get a Binary Dump of the reader
  - ✦ Using `hf iclass loclass`
- ✦ Then from there run a brute force attack against the dump to obtain the key

# YOU HAVE THE KEY!

- ✦ Now for the hard part
  - ✦ Get close enough to someone to read their card
- ✦ This is where the key is needed

# What to do with it

- ✦ Use the Proxmark to replay the card
- ✦ Write it to another card

# Magstripe


- Work by reading the direction of a lot of tiny bar magnets
- To change the data a writer changes the direction of the magnetic field
- The standard format has 3 tracks
  - Track 1 holds 79 6 bit blocks plus parity bit read only characters
  - Track 2 holds 40 4 bit blocks plus parity bit read only characters
  - Track 3 holds 107 4 bit blocks plus parity bit read only characters
- All data can be read by anyone
- <https://www.youtube.com/watch?v=yoLGFHqoAs0>
- <https://www.youtube.com/watch?v=UHSFf0Lz1qc&t=46s>

# Low Frequency - 125khz

- ✦ HID Proximity
- ✦ HITAG

# Handheld RFID LF Cloner

**BUY 1, GET 1 AT 7% OFF** (add 2 to cart) [See all eligible items](#) ▶



### 125KHz Handheld RFID Duplicator Key Copier Reader Writer ID Card Cloner & key HQ

★★★★★ Be the first to [write a review](#).

Condition: **New**

Quantity:  2 available / **6 sold**

Price: **US \$11.85**

[Buy It Now](#)

[Add to cart](#)

[Add to watch list](#)

[3-year protection plan](#) from SquareTrade - \$1.99

**Limited quantity remaining** More than 74% sold Free shipping

Shipping: **FREE** Standard SpeedPAK from China/Hong Kong/Taiwan | [See details](#)  
See details about international shipping here. ⓘ  
Item location: ShenZhen, China  
Ships to: Worldwide [See exclusions](#)

[\\$ Have one to sell?](#) [Sell now](#)

<https://www.youtube.com/watch?v=7rQSBXSBpTE>



# High Frequency

- ✦ Like ICLASS Default keys
- ✦ Some are unencrypted
- ✦



**M1 Key Tags Programmer ID IC Card Cloner RFID Duplicator Copier Reader Writer**

Condition: **New**

Size: **- Select -**

Quantity:  4 available

Price: **US \$49.71**

[Buy It Now](#)

[Add to cart](#)

[Add to watch list](#)

3-year protection plan from SquareTrade - \$6

**Free shipping** 30-day returns Ships from States

Shipping: **FREE** Economy Shipping | [See details](#)  
Item location: La Puente, California, United States  
Ships to: United States [See exclusions](#)

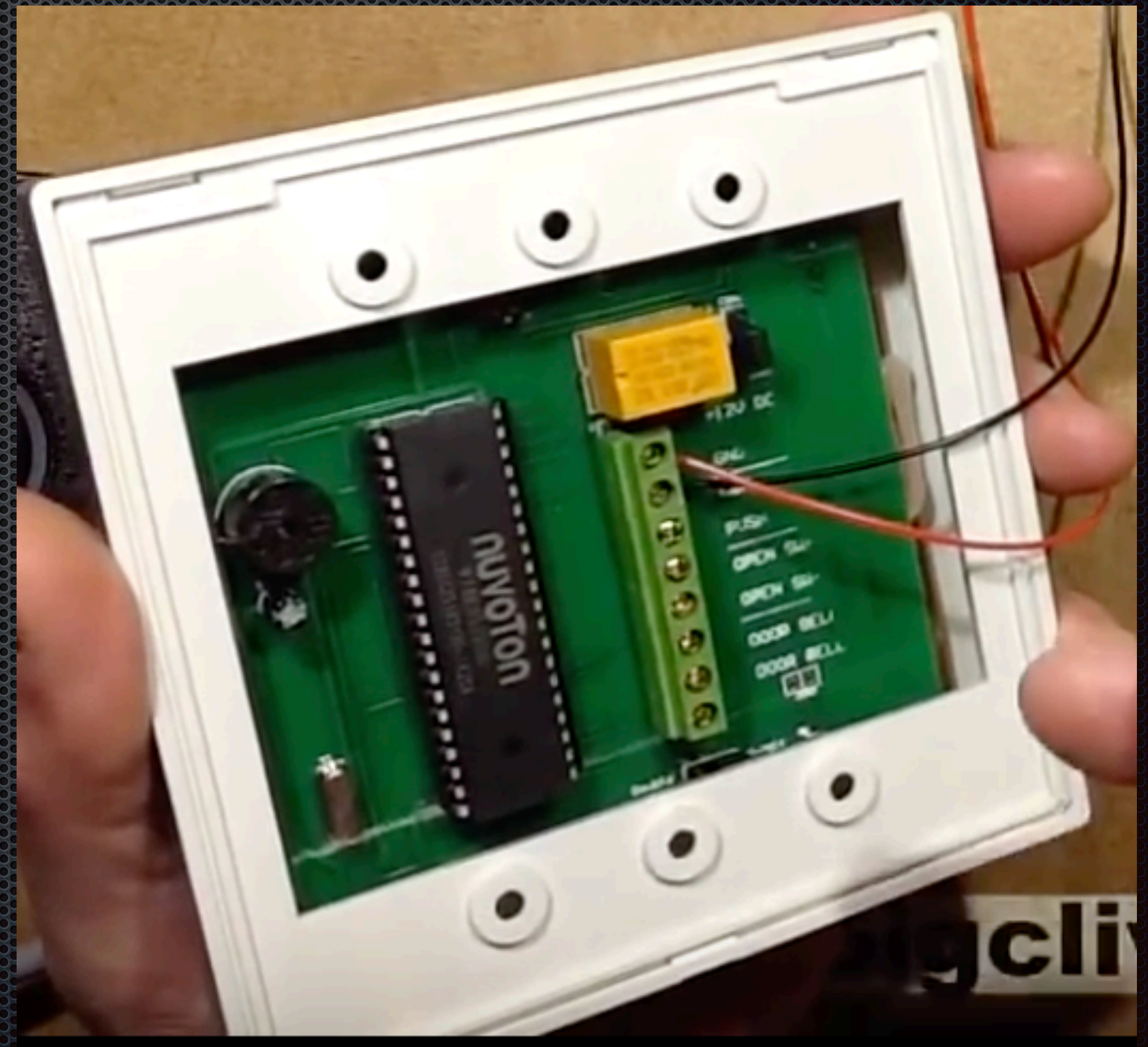
Delivery: Estimated between **Wed. Apr. 17 and Thu. Apr. 30**

Payments: [PayPal](#) [VISA](#) [MasterCard](#) [AMERICAN EXPRESS](#) [DISCOVER](#)

**PayPal CREDIT**  
Special financing available. [Apply Now](#) | [See terms](#)

Returns: 30 day returns. Buyer pays for return shipping.

# Bypass???



# References

- <https://twitter.com/InfoSecFriends/status/799003935876870144>
- <http://blog.opensecurityresearch.com/2012/11/dumping-iclass-keys.html>
- <https://blog.kchung.co/reverse-engineering-hid-iclass-master-keys/>
- <https://github.com/Proxmark/proxmark3>
- <https://scund00r.com/all/rfid/2018/06/05/proxmark-cheatsheet.html>
- [https://www.hidglobal.com/sites/default/files/resource\\_files/hid-rfid-il-frequency-tags-ct-en-plts.pdf](https://www.hidglobal.com/sites/default/files/resource_files/hid-rfid-il-frequency-tags-ct-en-plts.pdf)

# References

- <https://www.shopnfc.com/en/content/6-nfc-tags-specs>
- <https://hackerwarehouse.com/>
- <https://github.com/samyk/magspoofer>
- <https://www.youtube.com/watch?v=kUduHlygbY8>