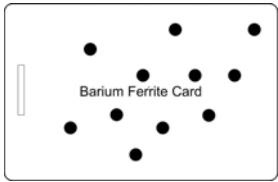


# **PHYSICAL ACCESS CONTROL SYSTEMS**

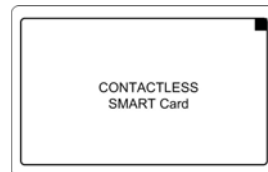
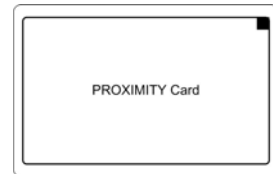
**Are you protected by two  
screws and a plastic  
cover?..... Probably!**

**Zac Franken  
Defcon 15**

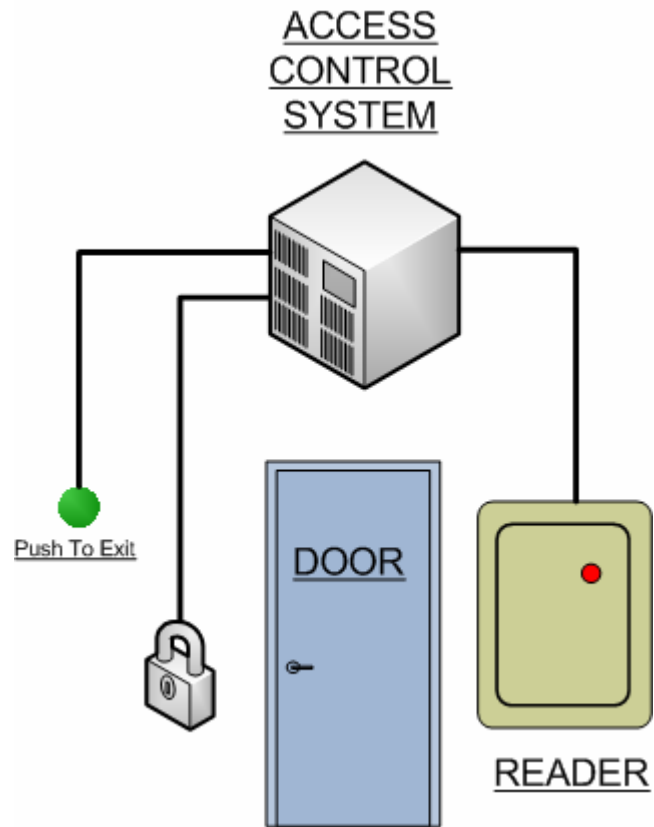
# What we are going to cover:



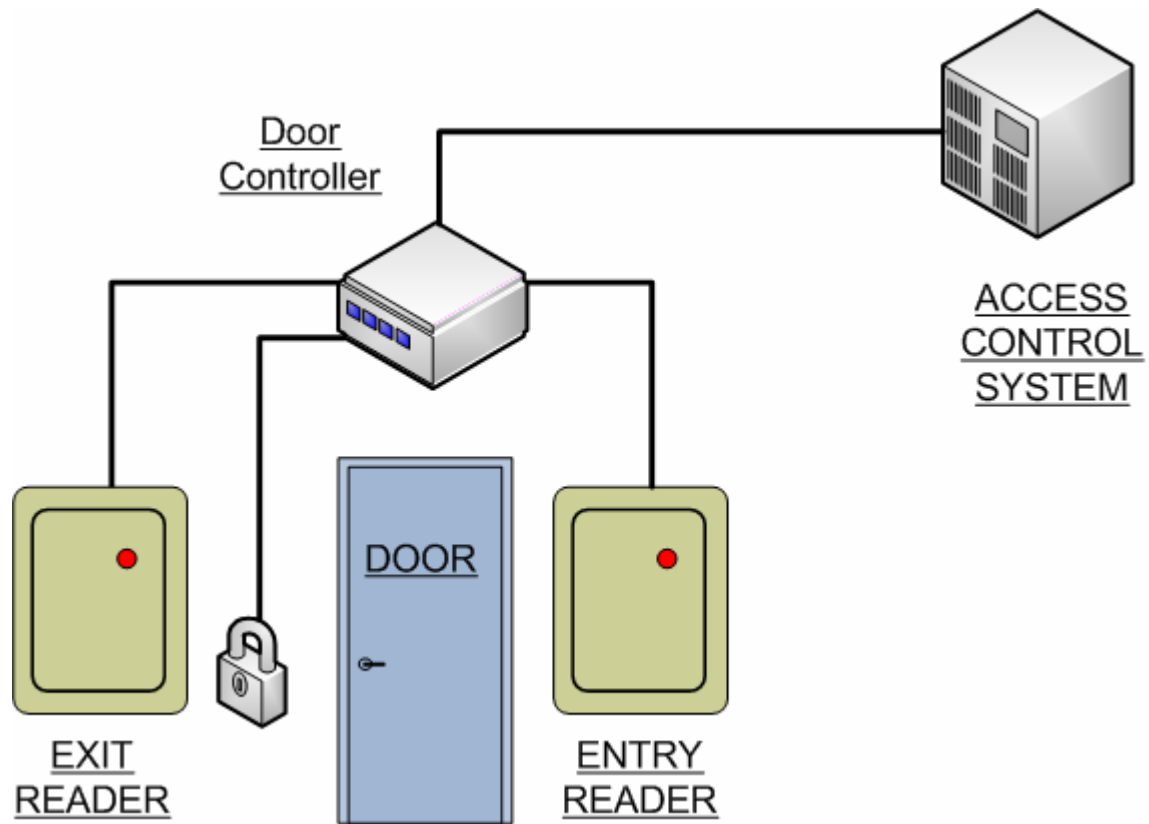
- Overview of physical credentials
- Brief overview of biometric systems
- Biometric worked example
- Demo of attack



# Basic system

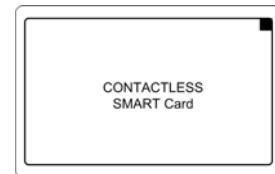
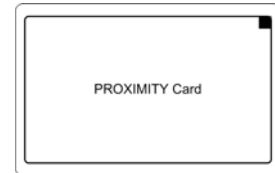
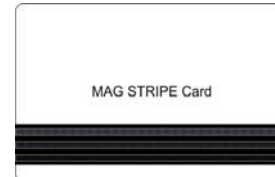
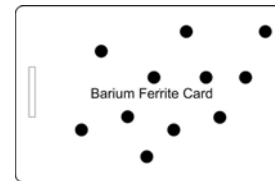


# Anti-Passback system



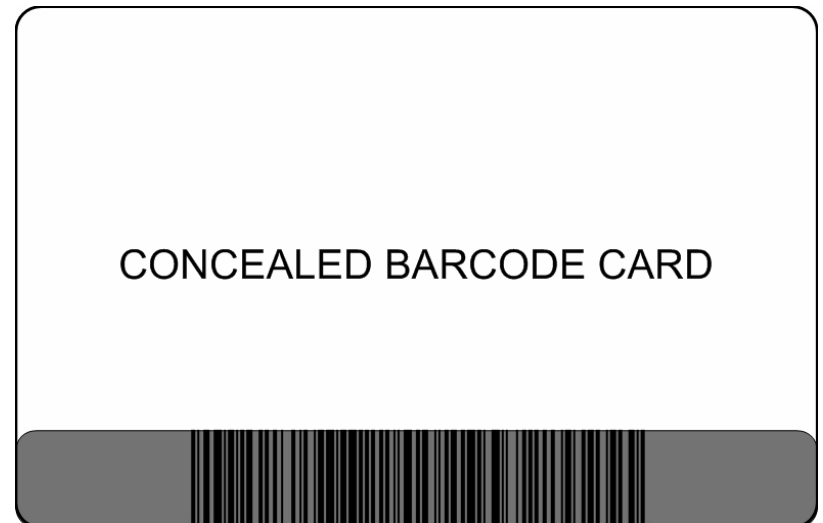
# Physical Credential Technologies

- Magnetic Strip Card
- Wiegand Card
- Proximity Card
- Barium Ferrite Card
- Concealed Barcode Card
- Smart Cards

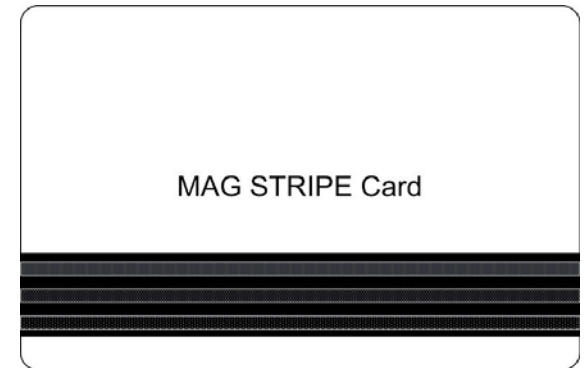


# Concealed Barcode

- As crappy as it sounds
- Regular barcode obscured by IR transparent material (a la Remote control)
- Just Fucking Embarrassing



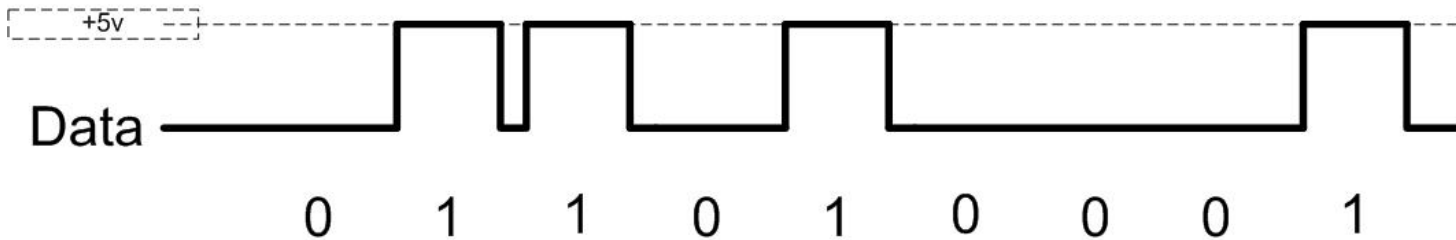
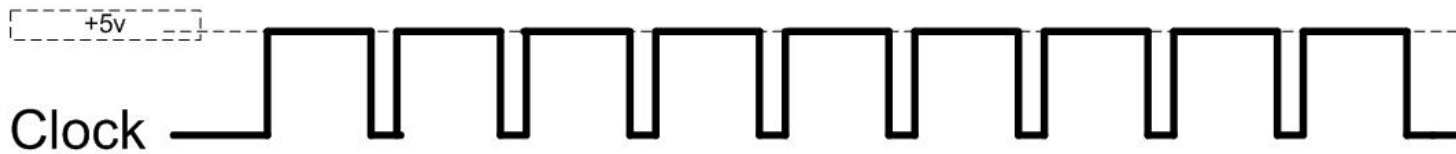
# Magnetic stripe



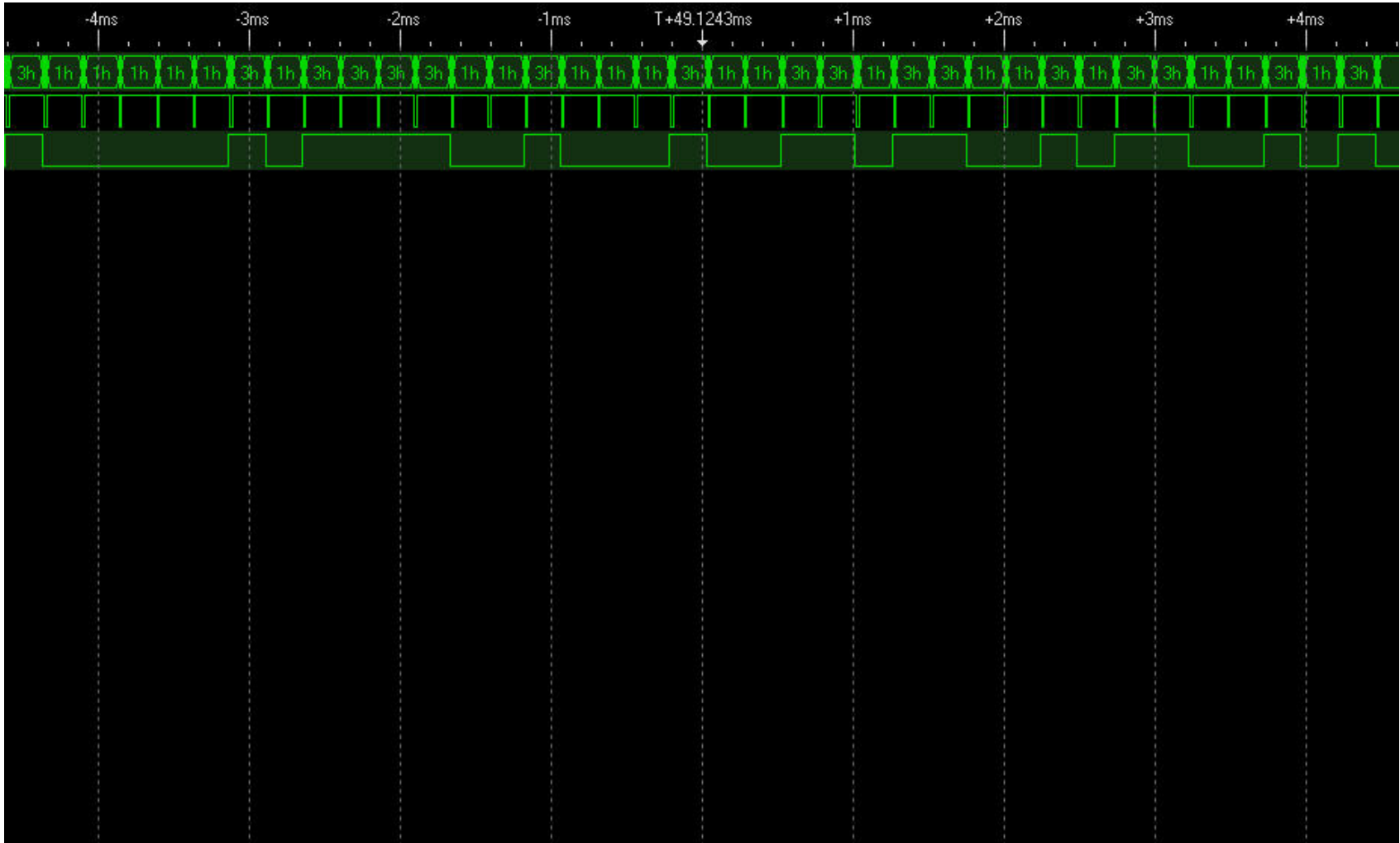
- Normally 3 tracks
- High Coercivity- 4,000 Oersted
- Low Coercivity- 300 Oersted
- Cards are read by an exposed read head in the reader
- “High security” cards can mean simply offsetting the track

# Clock & Data Protocol

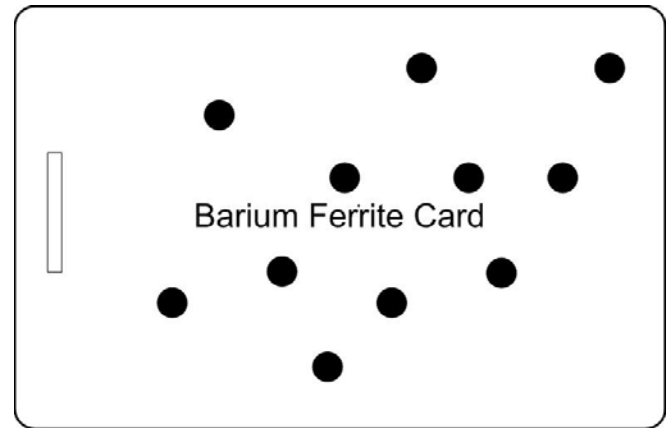
- 3 Wires required: Clock, Data & Ground
- Standard output from a mag stripe reader



# Clock & Data



# Barrium Ferrite



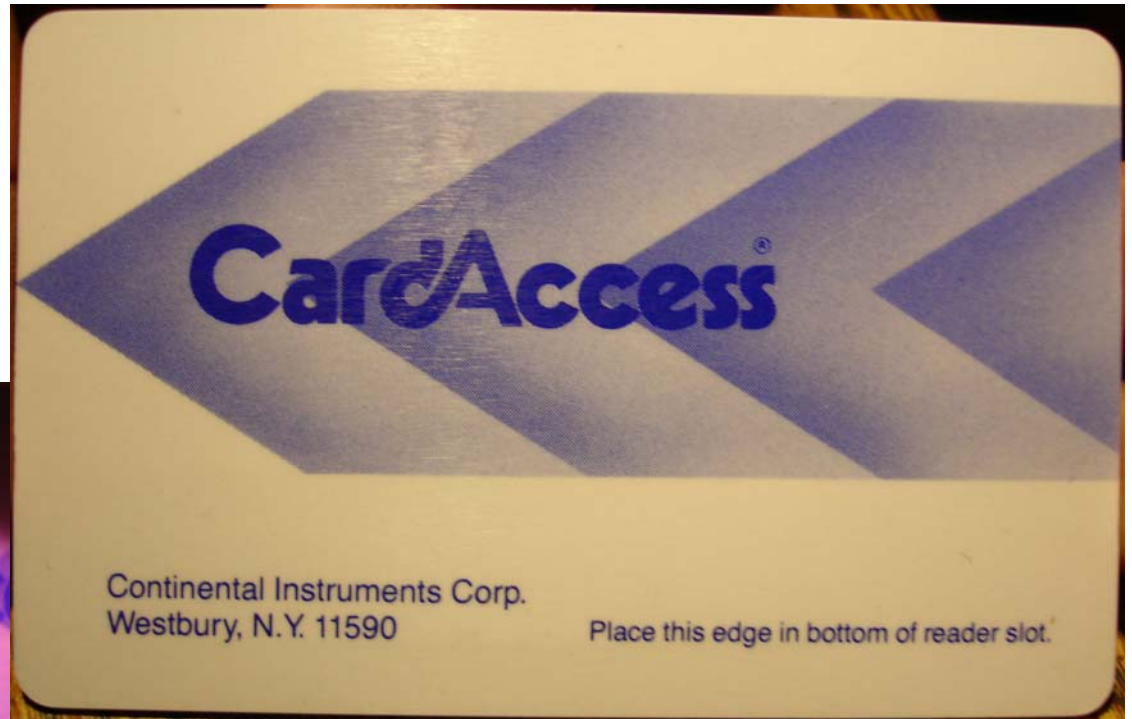
- Tends to use an insertion reader
- Card contains discrete magnetic domains
- Normally encoded in “fridge magnet” type material
- This was the original “Card Key”

# Wiegand card



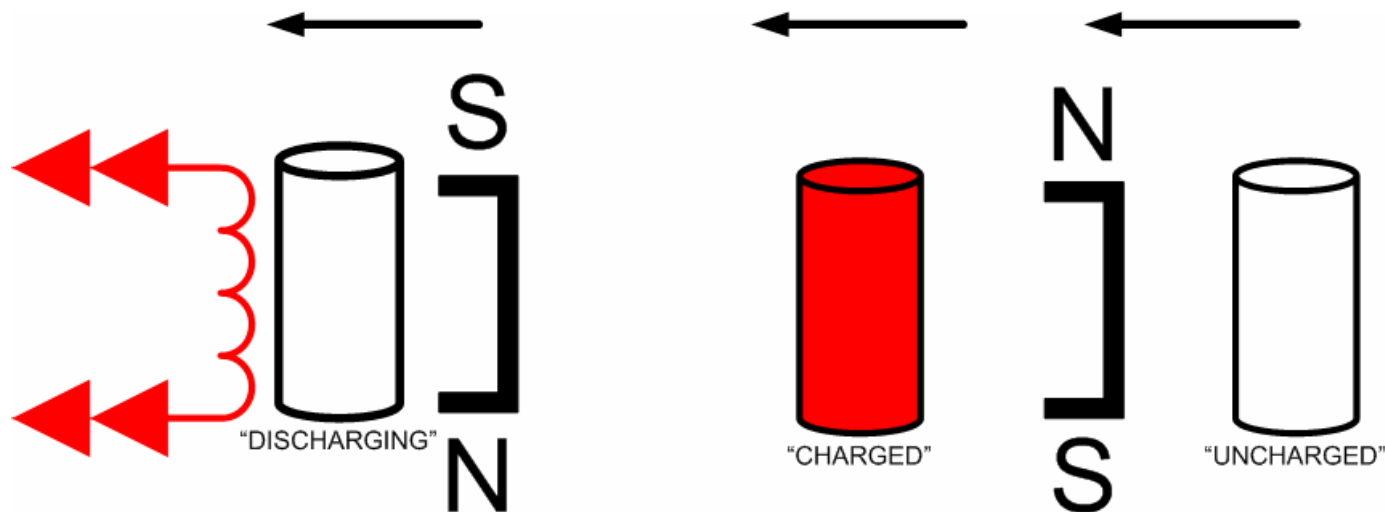
- Special alloy wire is processed in such a way to create two distinct magnetic regions in the same piece of wire when passed over a magnetic field
- Wire is embedded in the card in a distinct order to create an individual code
- Each Wiegand pulse is translated to a digital 0 or 1 depending on wire location

# Wiegand card



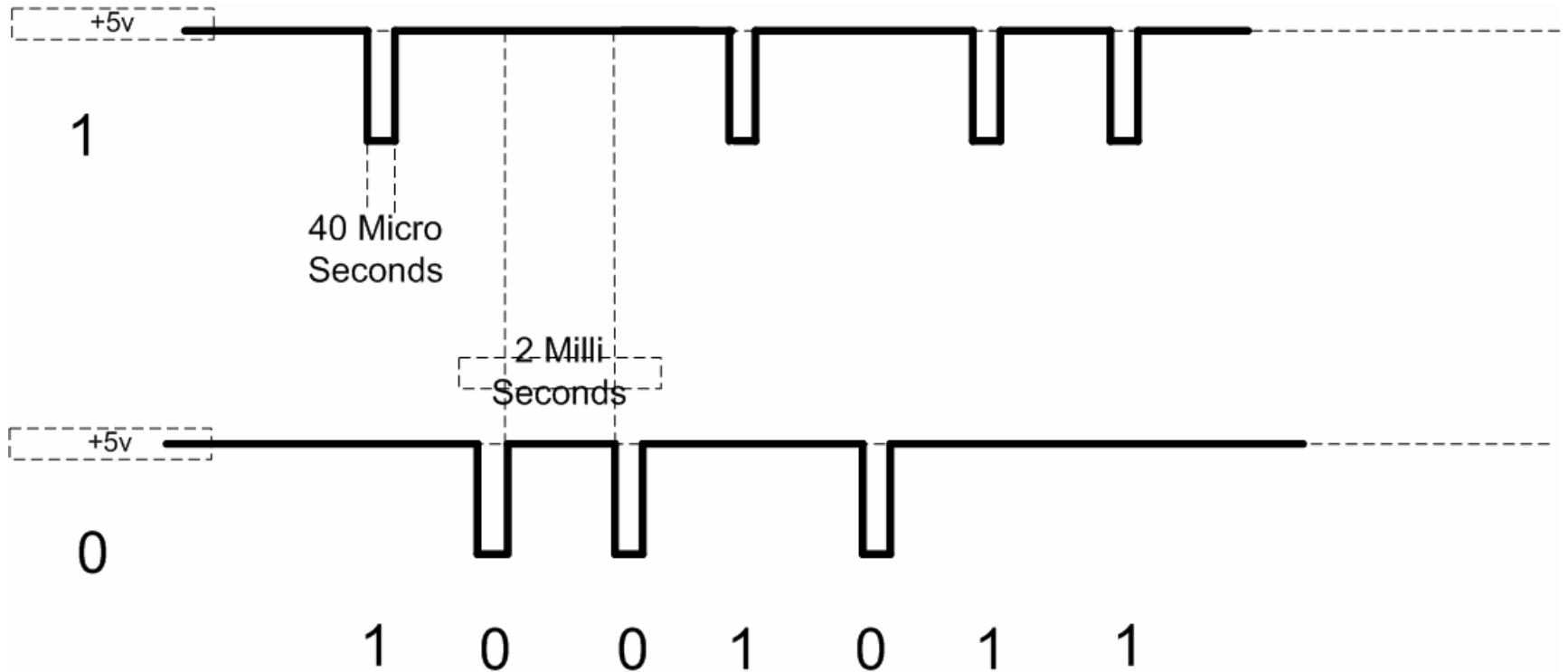
# Wiegand Effect

- When Wiegand wires go by a magnet they store the energy from the magnet
- If the wire is passed by an opposite polarity magnet, the wire releases the energy
- If a coil is placed near the wire as it releases the energy, you can convert the energy into an electronic pulse.

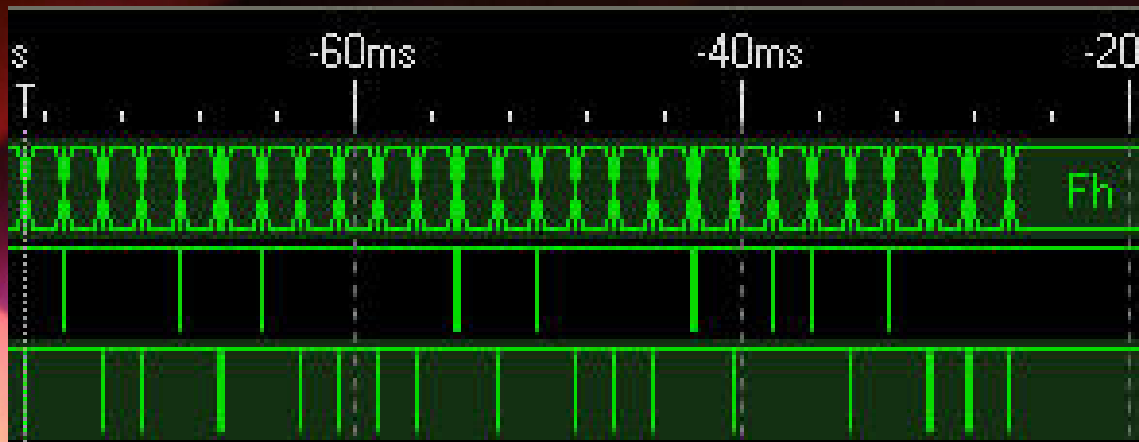


# Wiegand Electrical protocol

- 3 wires required: Binary 1, Binary 0, Ground



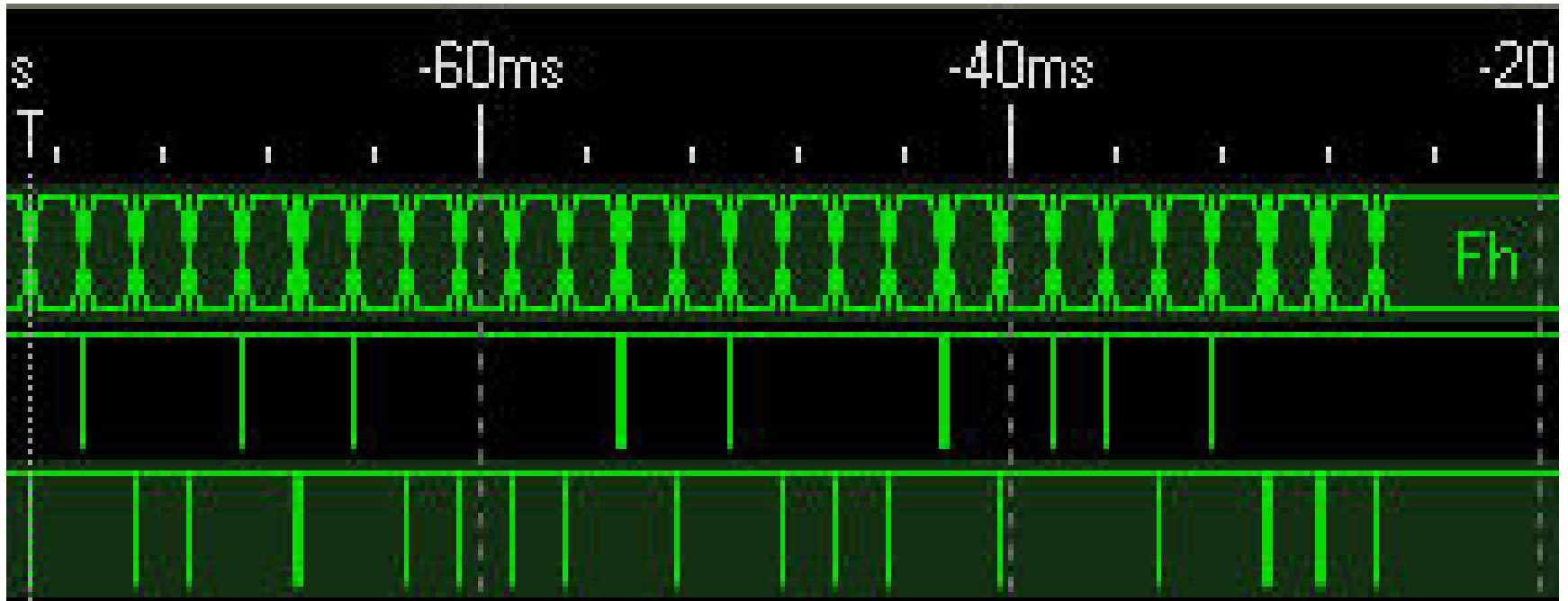
# Look familiar?



Continental Instruments Corp.  
Westbury, N.Y. 11590

Place this edge in bottom of reader slot.

# Real Wiegand Data



# Wiegand format

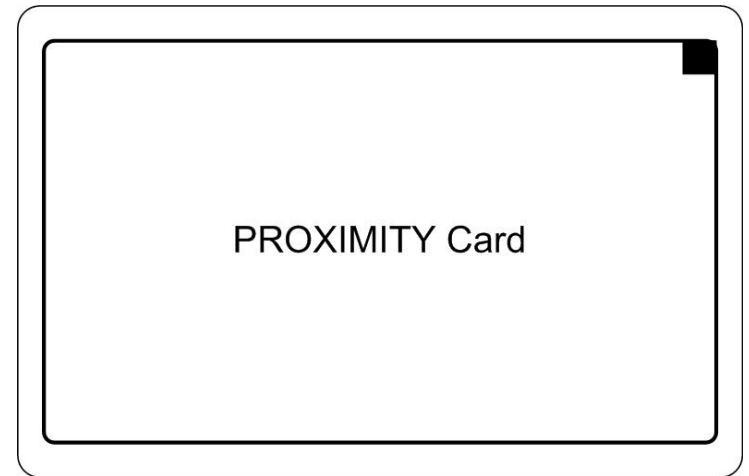
- 0s and 1s are divided into bit fields known as Wiegand format
- 26 bit is a “universal format”
- Most access card manufacturers have proprietary formats which they sell at additional cost

Most Significant Bit

Least Significant Bit

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26
	A	A	A	A	A	A	A	A	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
	Site or Facility Code Range = 0 - 255								PIN, Badge or ID Number Range = 0 - 65,535																
P	E	E	E	E	E	E	E	E	E	E	E	E	0	0	0	0	0	0	0	0	0	0	0	0	P
	Even Parity Field								Odd Parity Field																

# PROXIMITY



- Passive
- Reader emits an RF field that powers the card
- Card sends its data back to the reader where it is read by the host system
- An active card emits a field to the reader

# Proximity and RFID

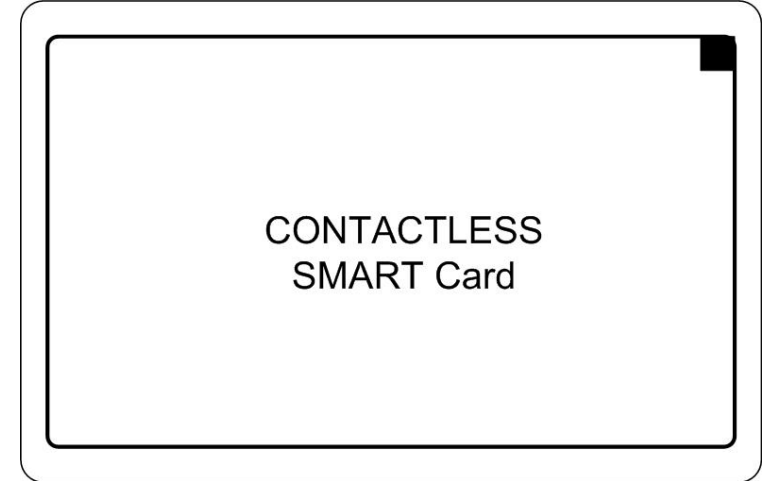
- Proximity cards are MAGNETICALLY coupled.
  - Short read range
  - Transmit response by shorting out own receive coil and causing minute power drops in readers transmit coil.
- RFID cards can have longer read range
  - Energised by signal on frequency  $X$
  - Transmit response on a fraction of frequency  $\frac{1}{2} X$

# Proximity ID cards

- Barf back a single bitstream
- Nominally 26 bits
- “high security” can be 40 bits, though there are rumours of up to 84 bit versions.
- Security by manufacturers restricting “sitecodes”
- The world generally uses 26 bits

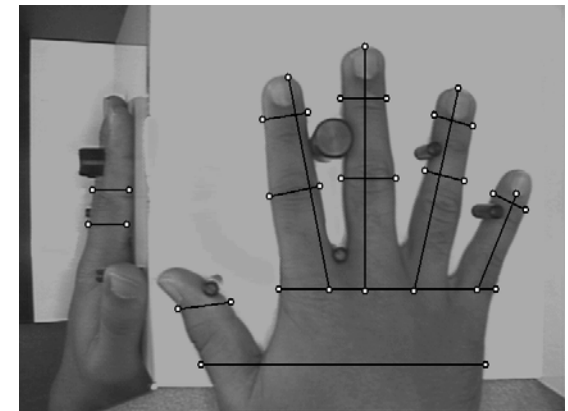
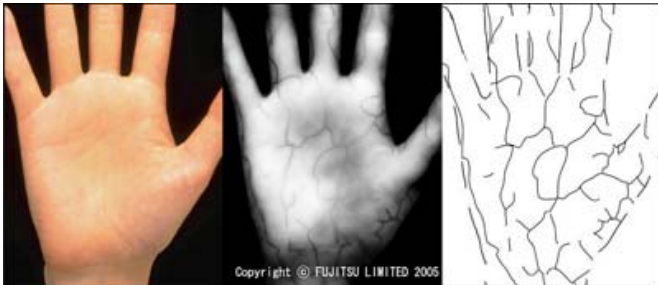
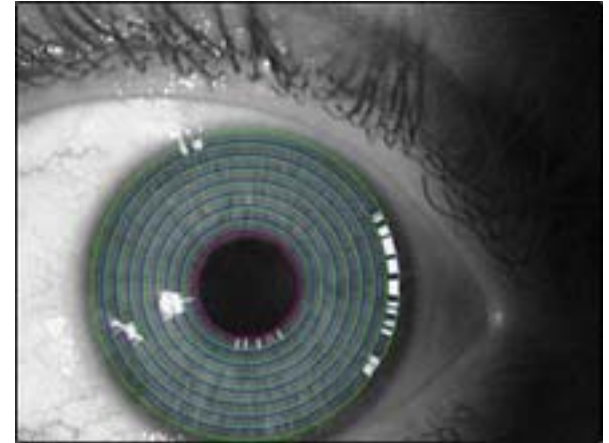
# Contactless Smart Card

- The way to go
- Authentication between reader & card
- Strong Crypto



# Biometrics

- Retina Scan
- Iris Scan
- Venial hand/finger map
- Hand Geometry
- Fingerprint



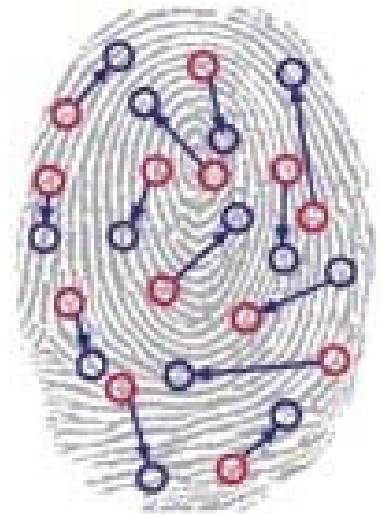
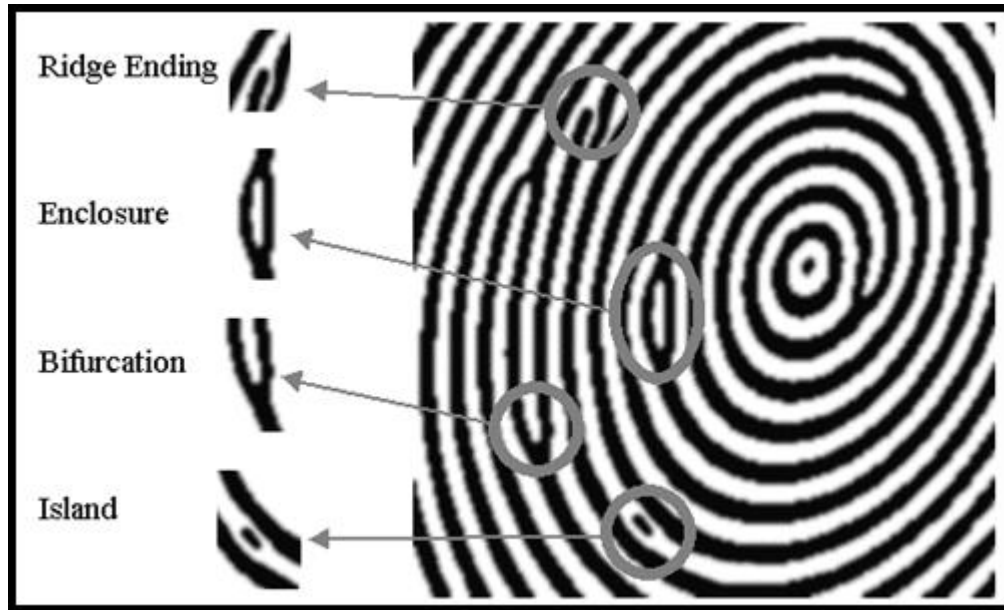
# Fingerprint



- image capture & feature compare
- 2 technologies
  - Optical
  - Capacitive (semiconductor)
- Easily defeated
- Gummy bears
- Licked photocopies
- Silicone fingertips etc



# Fingerprint Feature Analysis

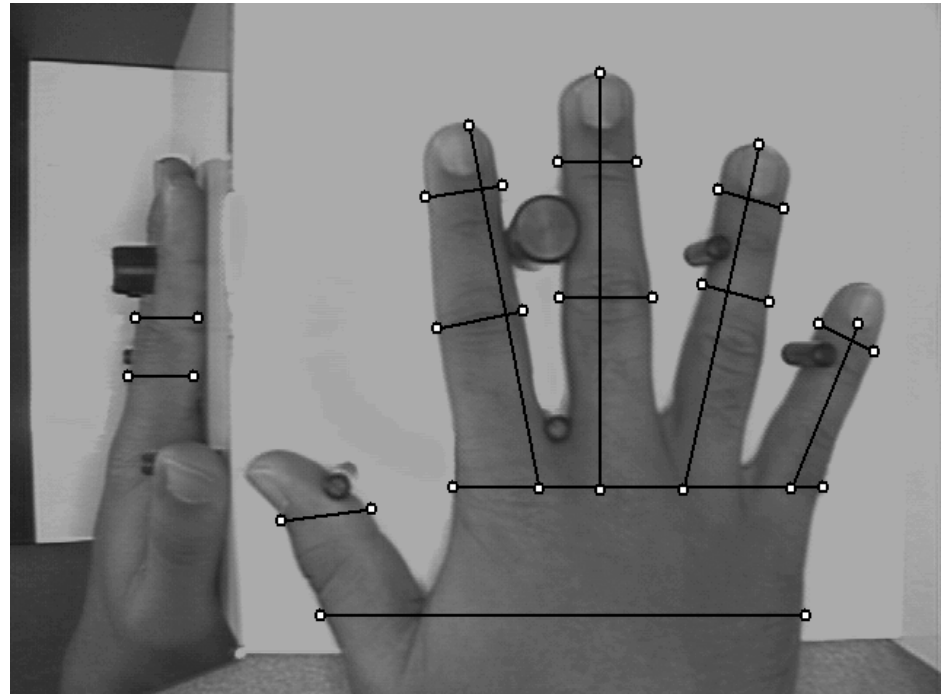


# Hand Geometry



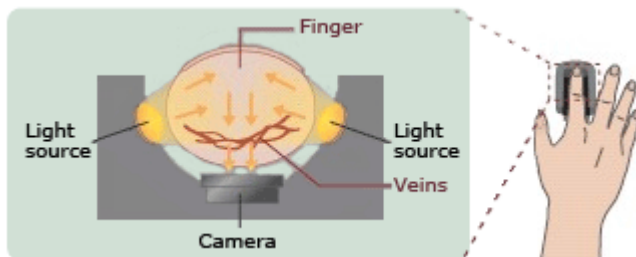
- Images again
- Note the pegs to center the hand

The addition of a 45 degree mirror allows them to add a check on the 3<sup>rd</sup> dimension.



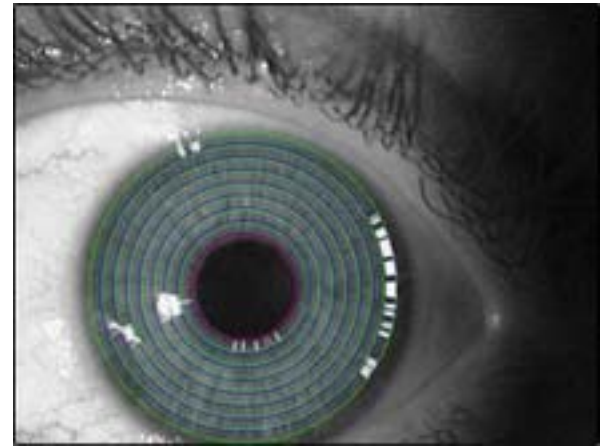
# Veinal hand Scan

- Another image capture, this time with an infra-red camera.



# Iris Scan

- Just an image!
- Potential for walk by capture!
- All biometric devices on the market today are basically image capture devices.



# Retina Scan

- More secure
  - Hard to “steal credential”
- Hard to use
  - Needs training & practise
- Manufacturer went bust
  - ☹️



This is actually a good example of how biometrics work and the challenges of getting them to work at all!

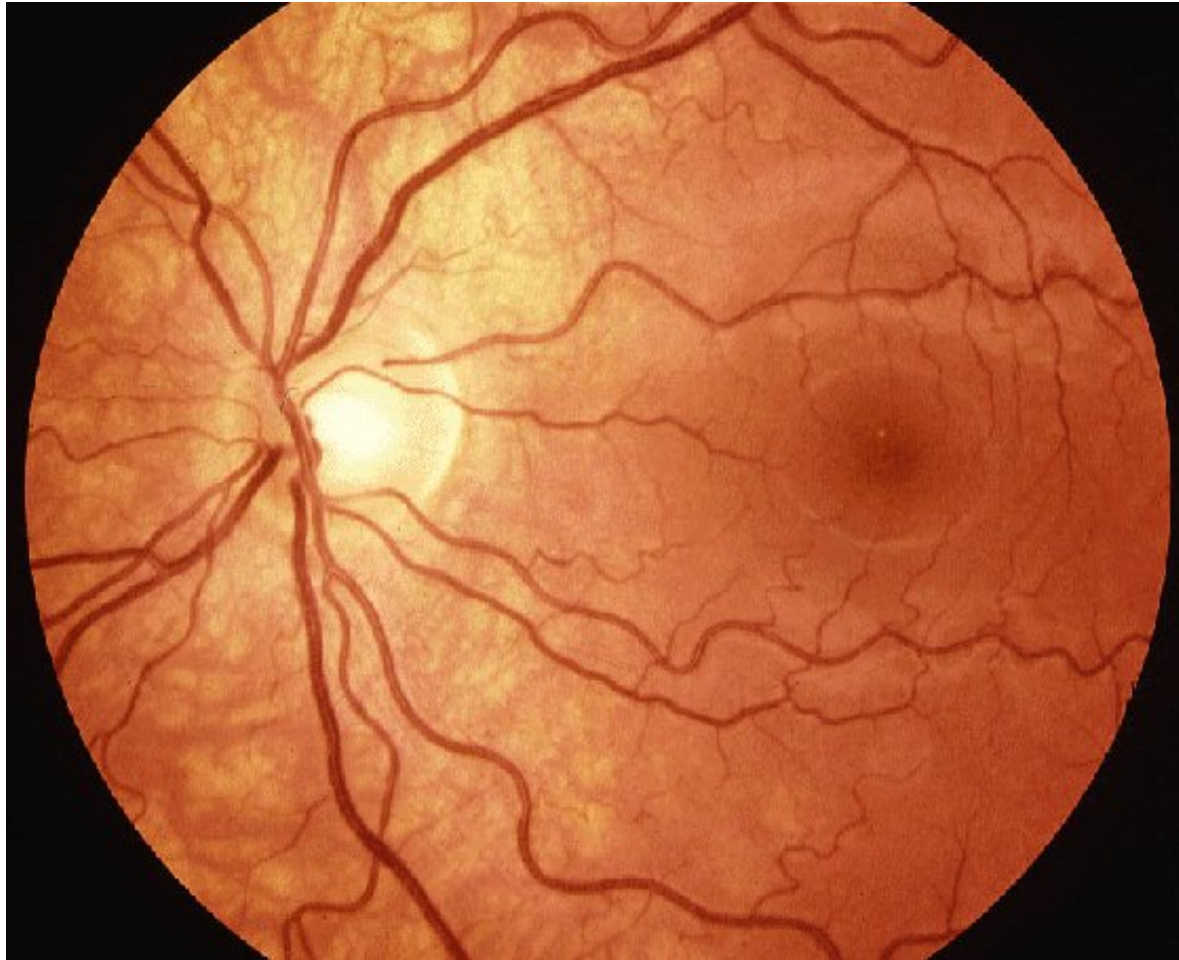
# An Example of how it works

- First the user enters code on reader
- Visual dot and target is displayed in eyepiece
- (Tip: put finger on scan button)
- look into eyepiece
- move head to align dot onto target
- Once you have correct alignment user presses scan button.
- **HOLD STILL!!!**

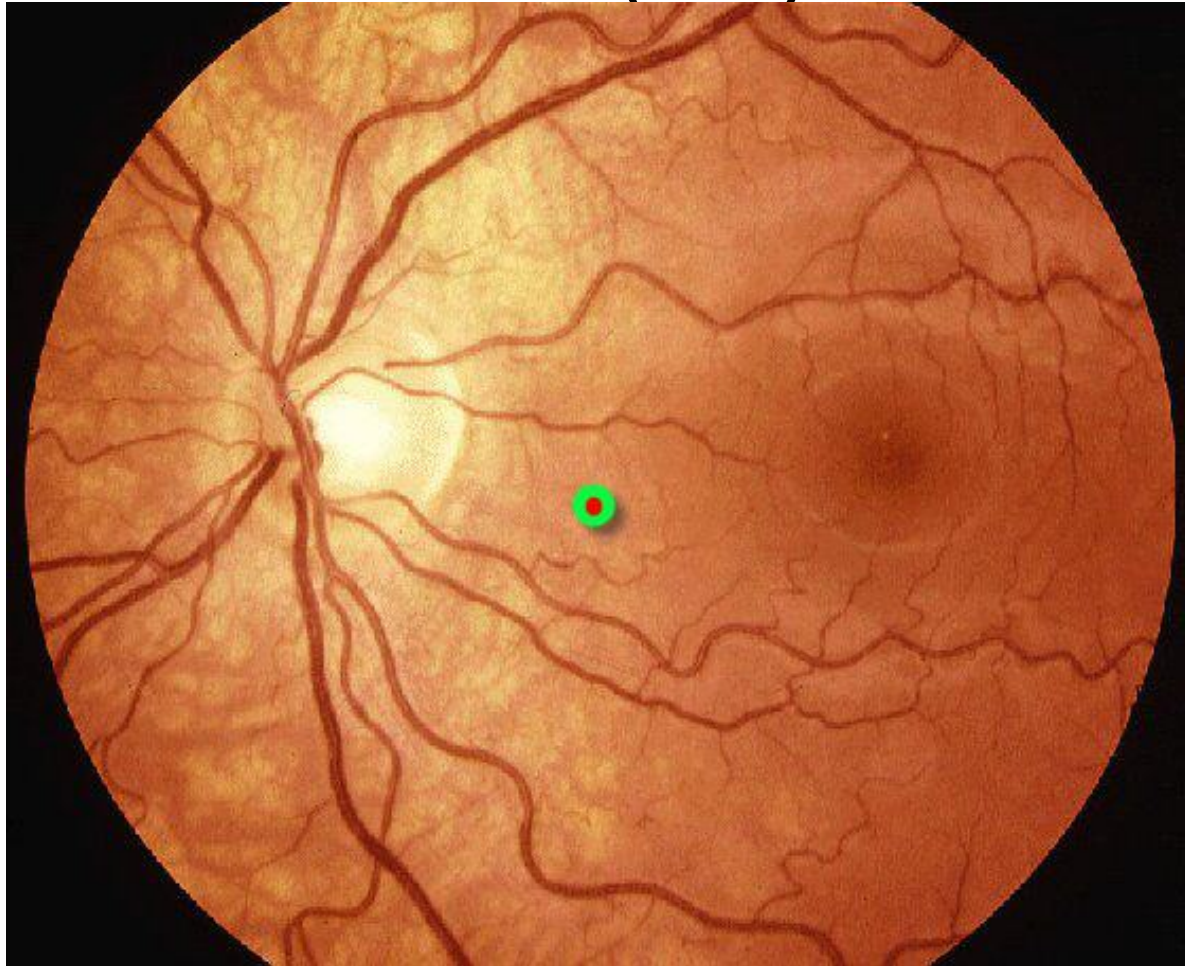
# Not as easy as it sounds..

- Not that it sounded that easy
- All biometric devices have a variance factor.
  - No two reads will ever be identical
  - There must certain amount of leeway allowed

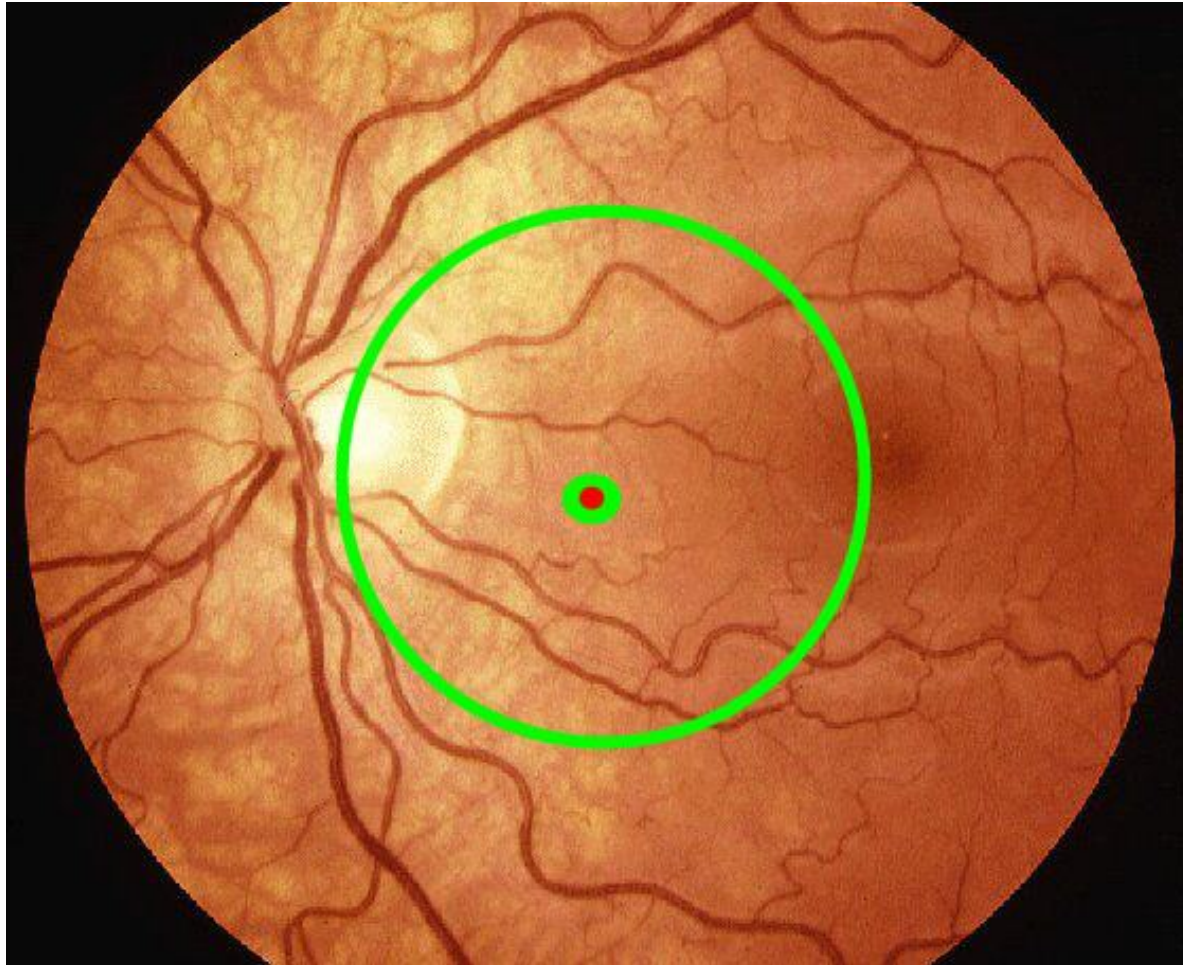
A retina (Not mine !)



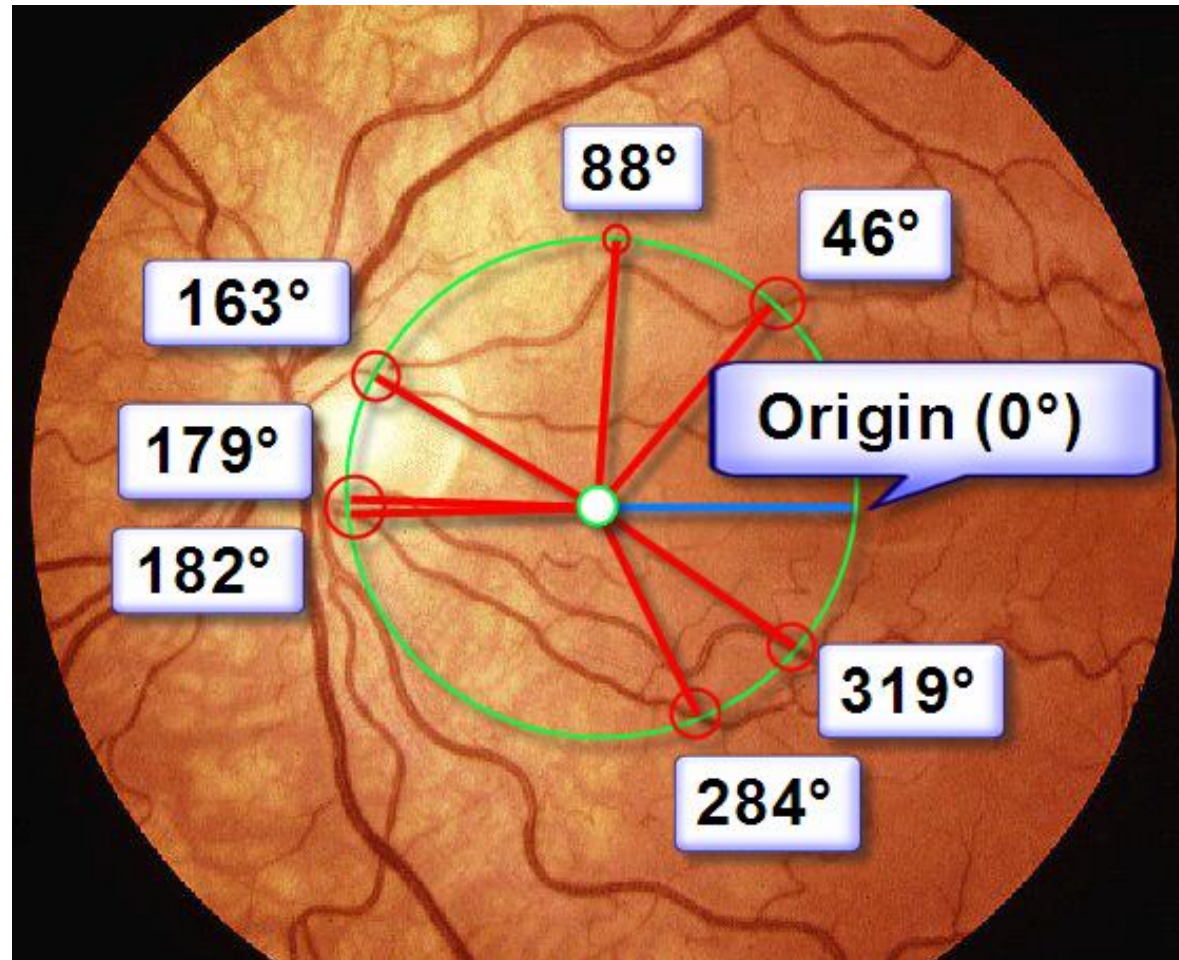
The user target alignment aligns the eye to the same position each time (sic)



When the scan button is pressed  
the reader scans a circle of the  
retina



Along the circle it spots the dark bits (Veins) and notes their location on the circle



Surprisingly enough.... The user credential is 360 bits long 😊

This changed with later models but it shows how the designers think.

# Coolness factor:- High

- Alignment
  - Totally subjective
  - Almost like including a brain print
- Fudge factor
- ID generally ends up as a hash

# Statistically speaking

- **False Acceptance Rate:**
  - Rate at which someone other than the actual person is falsely recognized.
- **False Rejection Rate:**
  - Rate at which the actual person is not recognized accurately.
- Also All of these technologies are coupled with a user id!

# Credential Revocation



Fingerprint / Hand revocation device

# Credential Revocation



Retina / Iris revocation device

# **The Catch**

You knew it was here  
somewhere...

Why backwards  
compatibility in the  
security industry is a  
**BAD THING™**

# Wiegand

- When Wiegand cards came out they were considered “The shit”
- Access control manufacturers all made sure that their systems could interface with wiegand enabled readers
- They still do.....

- Every reader we saw today, from the super secure biometric retina scanner to as “crappy as it sounds” concealed barcode **uses the wiegand electrical and data protocols to communicate** to the access control system.

# EEEEK!

- “PLAIN TEXT”!
- Easily intercepted!!
- Easily replayed!!!
- Includes output from biometric readers!!!!
- Includes output from strong crypto contactless smart card readers!!!!

# The Goal..

- Record wiegand id's
- Replay wiegand id's
- Small
- Easily installable
- Cheap (if poss)

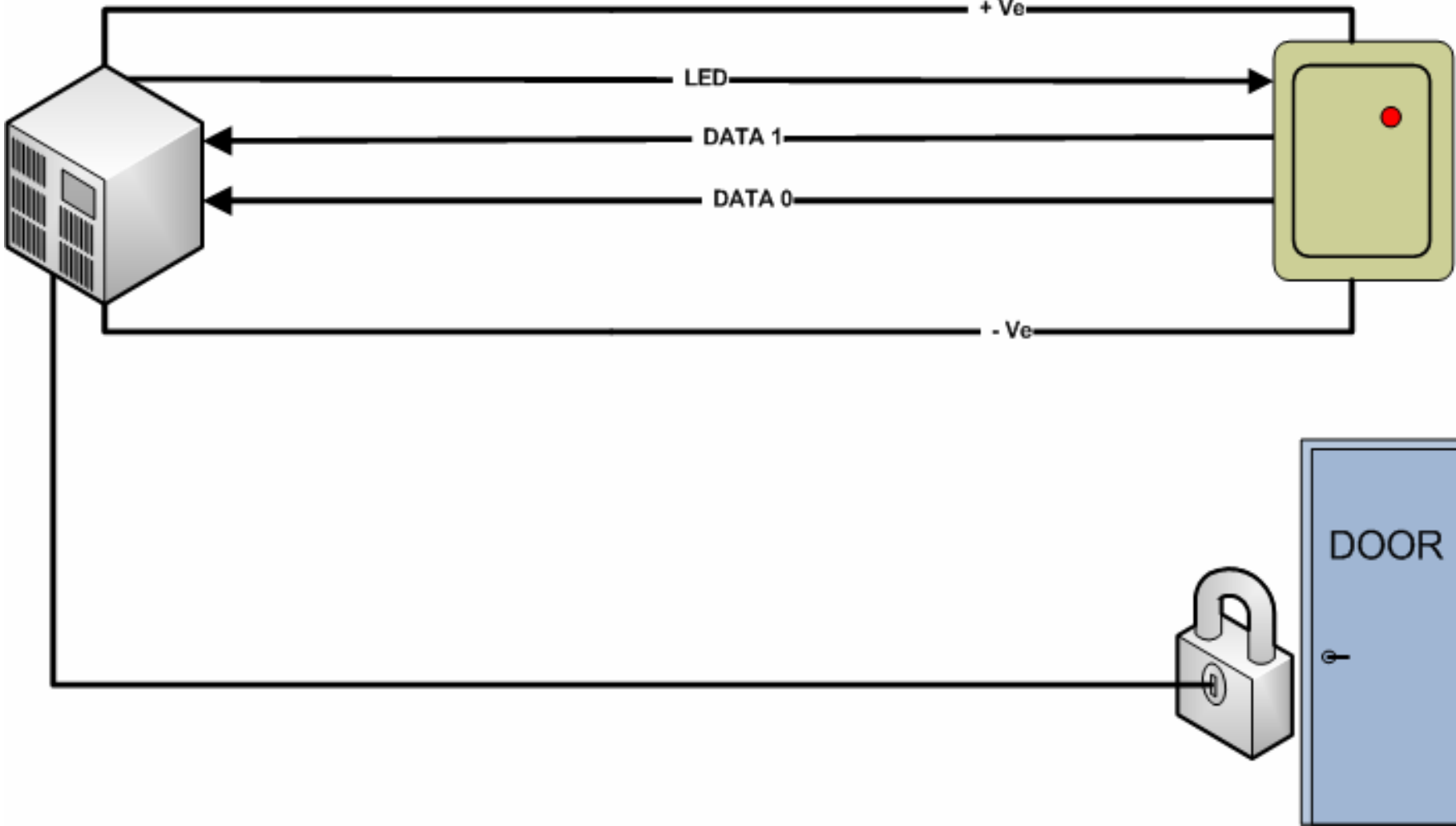
# Challenges..

- Unit control (send replay command)
  - Don't really want wires hanging out
- Card validation (don't record bad cards)
  - Hmm
- Data Extraction (read out card id's)
  - Still don't want wires hanging out

# Connection

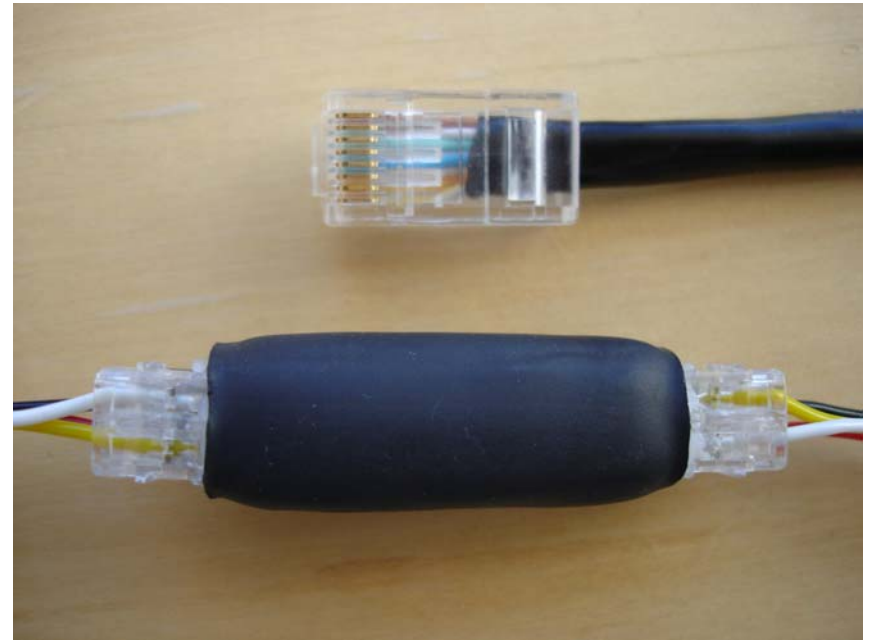
ACCESS  
CONTROL  
SYSTEM

READER



# Say Hello to Gecko

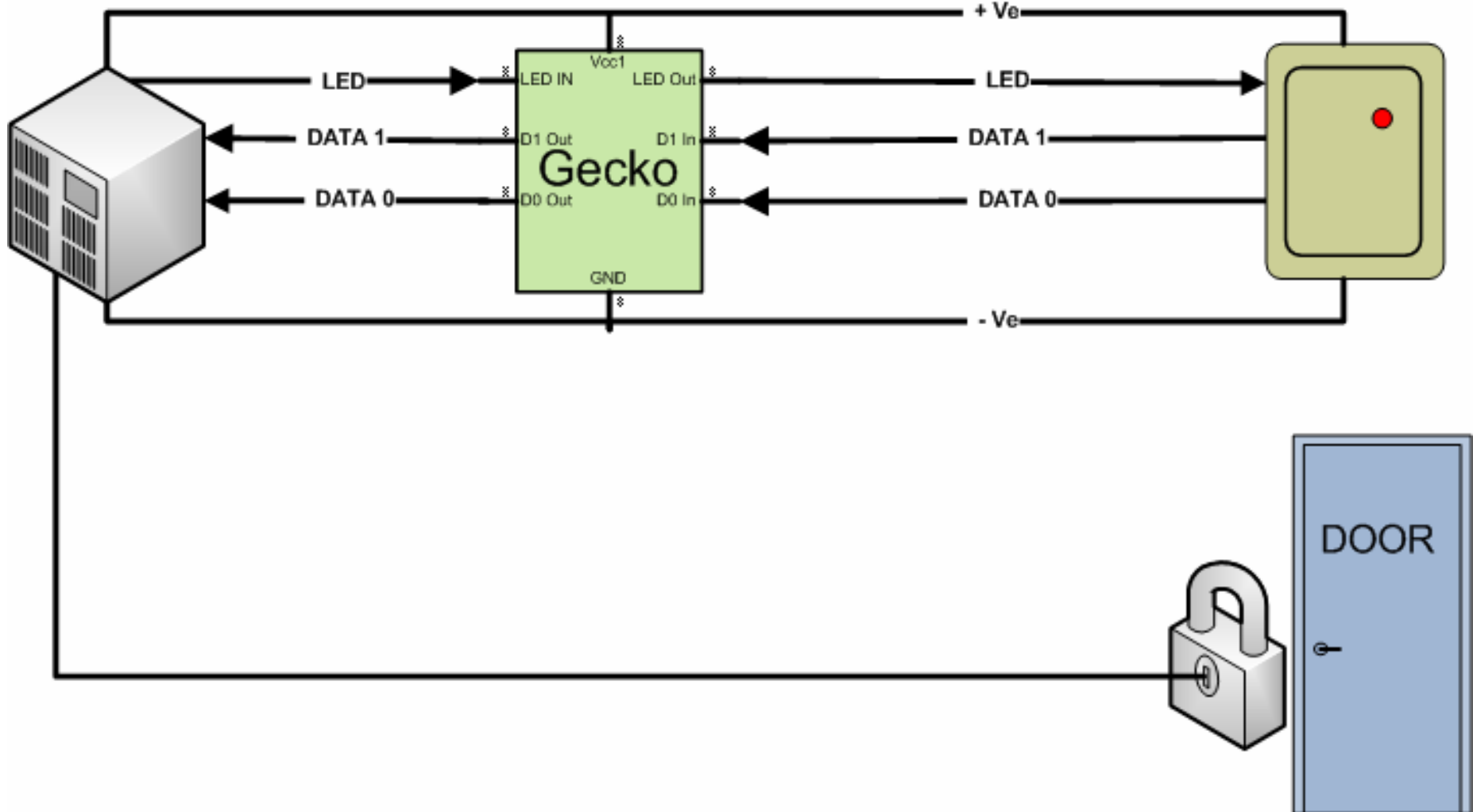
- Uses “Command Cards” to control functions (Replay etc)
- Uses “Access Allowed” LED Control line to validate cards
- Uses “Access Allowed” LED to download data



# Connection

ACCESS  
CONTROL  
SYSTEM

READER



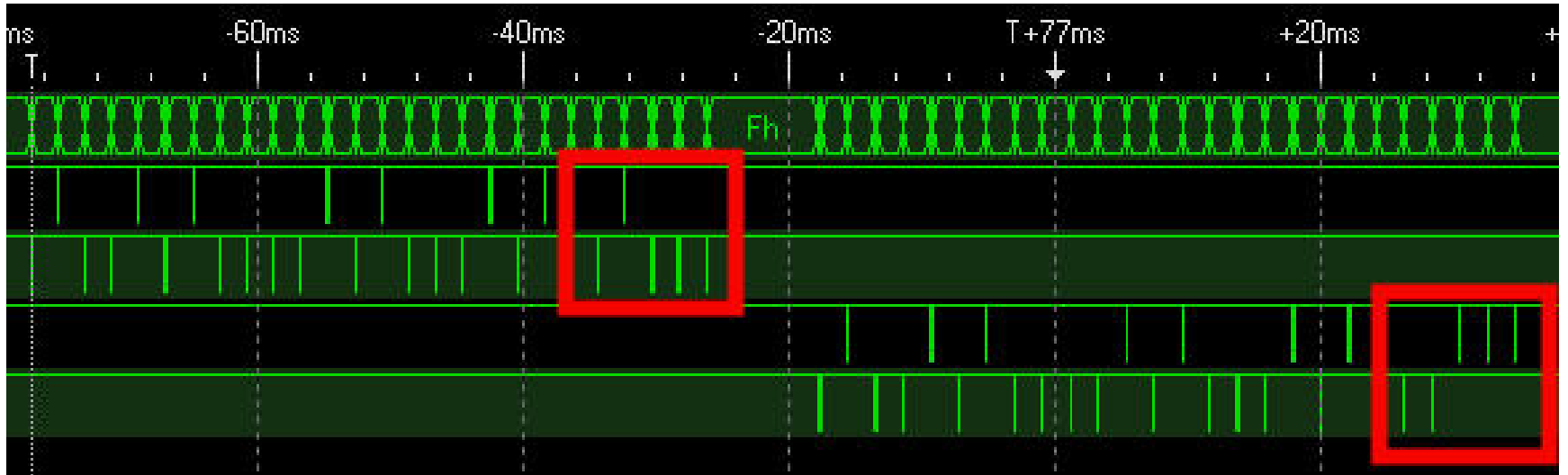
# Demo

Standard Demo Disclaimer Applies:

**This is a demo, so nothing will  
work.**

**However, if it does, I'm totally  
prepared to take all the credit  
for it!**

# Replay in progress...



# Development V1

- Proof of concept
- Basic feature set:-
  - Record
  - Replay
  - Disable
  - Enable

# Version 2

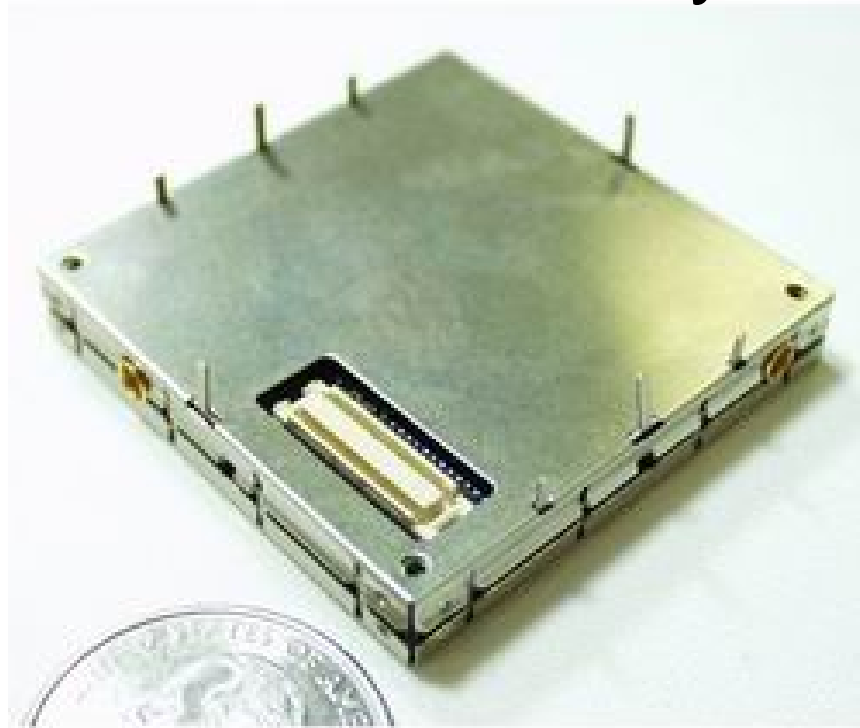
- Store multiple ids to eeprom/flash
- Check validity of card by monitoring reader led line
- Download data via reader led 😊
- Load data via command cards

# Version 3

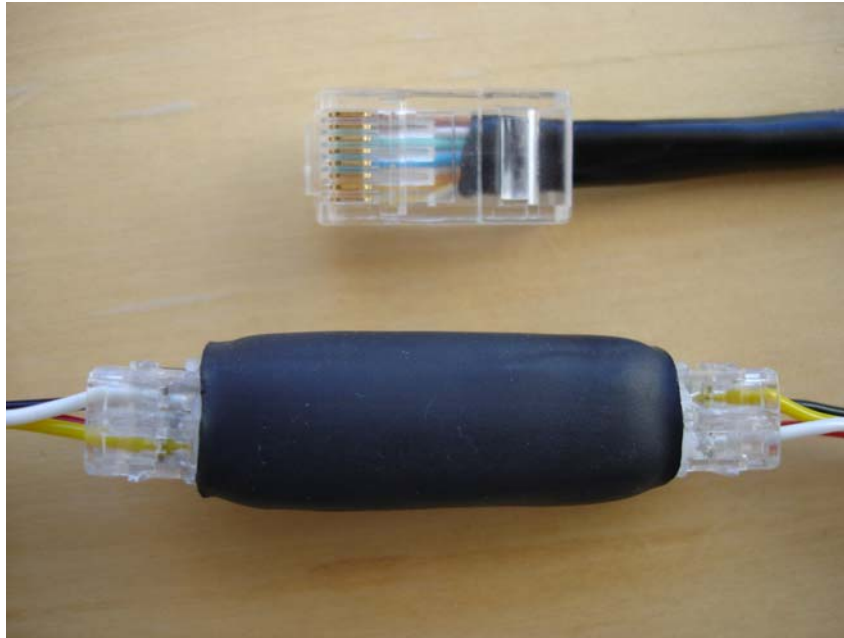
- All the functionality of V2, but with a bluetooth control interface.
- Ideal for biometric devices

# Version 4

- All the functionality of V3, but with a GSM interface.
- Monitor access to the facility remotely



# Q & A



Zac Franken  
zac@riptalon.com

# PHYSICAL ACCESS CONTROL SYSTEMS

Were you screwed by two  
screws and a plastic  
cover?.....

Zac Franken  
zac@riptalon.com  
Defcon 15