DIY Access Control Systems

John Norman
23b Shop Hacker Space
arclight@gmail.com

Introduction

Why are we doing this?

- Security and Access Control Systems are mostly closed-source and proprietary
- Very little information about their inner workings is published by manufacturers
- We needed an access control system
- Dealing with keys was getting old

Introduction

Defining Security

- Can be defined in terms of:
  - Assets
  - Threats to those Assets
  - Countermeasures
- Differs from safety, but often affects safety (positively and negatively)
- Always involves trade-offs
  - Cost
  - Convenience
  - Creation of new vulnerabilities

Physical Security
Risks and Threat Model

- Physical Security countermeasures perform 4 basic tasks
  - Deter
  - Delay
  - Detect
  - Respond
- Overall purpose is to enforce a Security Policy
  - Security and safety of personnel
  - Prevention of theft or damage to assets
  - Auditing of access and security events

Physical Security

Some “Model Attackers” (Ross Anderson)

- Derek
- Charlie
- Bruno
- Abdurrahman

Threat Model

Derek

- *Derek* is a 19-year old addict. He's looking for a low-risk opportunity to steal something he can sell for his next fix.

Threat Model

Charlie

- *Charliex* is a 40-year old inadequate with seven convictions for burglary. He's spent seventeen of the last twenty-five years in prison.
- Although not very intelligent, he is cunning and experienced; he has picked up a lot of 'lore' during his spells inside. He steals from small shops and suburban houses, taking whatever he thinks he can sell to local fences.

Threat Model

Bruno

- *Bruno* is a ‘gentleman criminal’. His business is mostly stealing art. As a cover, he runs a small art gallery. He has a (forged) university degree in art history on the wall, and one conviction for robbery eighteen years ago.
- After two years in jail, he changed his name and moved to a dif-ferent part of the country. He has done occasional ‘black bag’ jobs for intelligence agencies who know his past.
- He’d like to get into computer crime, but the most he’s done so far is stripping $100,000 worth of mem-ory chips from a university’s PCs back in the mid-1990s when there was a memory famine.

Threat Model

Abdurrahman

- *Abdurrahman* heads a cell of a dozen militants, most with military training. They have infantry weapons and explosives, with PhD-grade technical support provided by a disreputable country.
- Abdurrahman himself came third out of a class of 280 at the military academy of that country but was not promoted because he's from the wrong ethnic group.
- He thinks of himself as a good man rather than a bad man.
- His mission is to steal plutonium.

Threat Model

A typical commercial space

- Most business perimeters are protected by a 5-7 pin mortise lock (Schlage, Yale, Sargent, etc), tempered glass windows, and a basic alarm system.
- A larger site may have electronic perimeter access controls tied into the building systems, an on-site security desk for monitoring, and better locks for key control and master-keying.
- This represents good basic protection from burglary and meets insurance requirements for most businesses. The “Derek” and “Charlie” model attackers are covered here.
- Data centers and businesses with high-value items such as cash or jewelry are typically designed to deter the above attackers and delay a more sophisticated “Bruno” attacker.

Commercial Systems

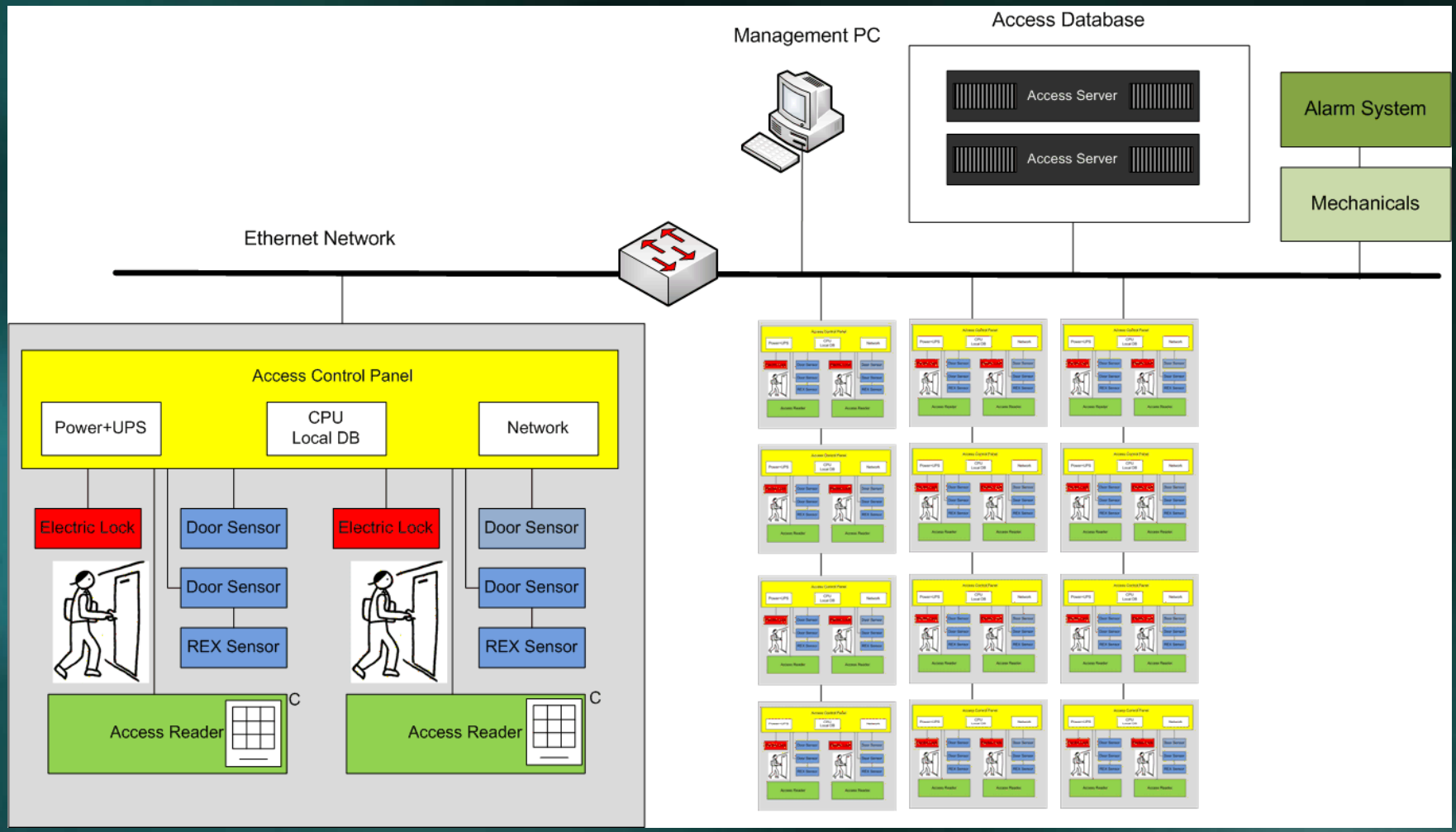
Typical Features of a Building Access System

- Distributed modules that control 1-4 doors
- A centralized Windows computer where access token information is kept and logs are aggregated
- Electromagnetic locks on perimeter and/or suite doors
  - Electric mortise locks
  - Door magnets (1000-2000lb capacity)
  - Electric strikes
- Access token readers
  - Cards (contact or contactless)
  - RFID tokens (EM4100, Mifare, HID, Indala)

Commercial Systems

Typical Features of a Building Access System

- Exit devices for personnel
  - “Push to Exit” device
  - Motion sensors
  - Delayed exit buttons
- May have integration with a centralized console application
  - Surveillance cameras
  - Remote lock/unlock
  - Logging and Audit trail viewing
  - Alarm integration



Typical Access System

Threat Model

Advantages of Electronics Locks

- Easy to revoke keys
- Allow flexible security policies
  - Time, location, security level, etc.
  - Public vs. Private areas easy to control
- More difficult to subvert due to carelessness
  - Doors can be kept “always locked” if access is convenient
  - Alarms for “door prop” and other human failures
- Auditing possible
- Easy integration with other systems
  - Alarms
  - Lighting
  - HVAC

Threat Model

Disadvantages of Electronics Locks

- RFID Tokens can be read at a distance
  - 125Khz RFID tokens 0-5cm, more with large coil
  - 13.8Khz tokens 10-20cm, more with HF antenna
  - If it can be read, assume it can be cloned.
  - Physical Keys can be cloned, but require a hi-res photo (Laxton, Wang, Savage, 2008)
- Require Electricity
  - Power can be interrupted or manipulated
- May fail in unpredictable ways
- Brute-force attacks may be automated
- Depend on security of network, servers, etc.

Open Access Control

Design Criteria

- Relevance to “Derek” and “Charlie” attackers mentioned above
  - Keep the junkies from the alley out of our shop
  - Resistance to a more sophisticated attacker a plus
- Electronic control of (2) doors
- Compatibility with off-the-shelf readers (Wiegand)
- Run independent of a PC or other external device
- Provision for logging and auditing
  - Internal or PC-based
- Alarm and sensor capability
  - Minimum of 4 independent zones
  - Supervision a plus
  - Integration with existing alarm system

Open Access Control

Methodology

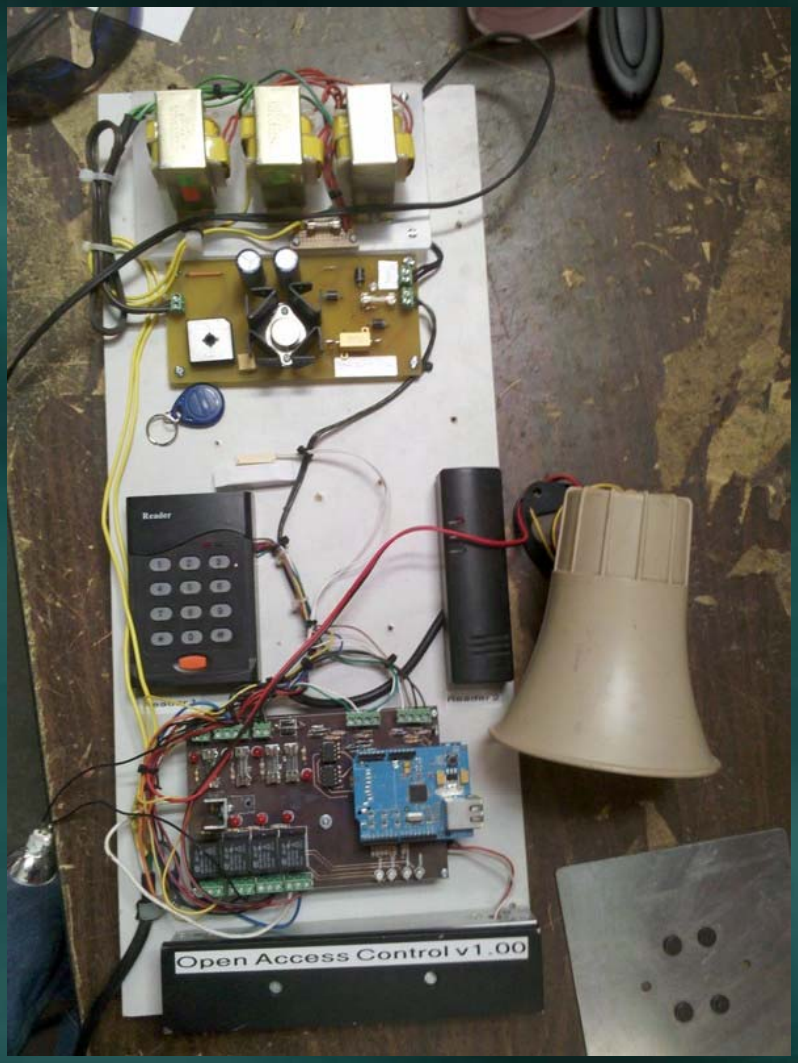
- Allow customizable access policies more granular than metal keys
  - Time/date based
  - Multiple security levels
- Physical Robustness
  - Input protection
  - Battery Backup capability
- Low cost
  - Open-standards readers with inexpensive tokens
  - Controller board that can be made for US$100 or less
- Repeatability
  - Use Arduino or similar microcontroller for maximum hackability and customization
  - Use only commodity components readily available through Digikey, Mouser, Element 14, etc.

The Design Process

- Individual circuits tested on breadboard
  - Had to debug Wiegand protocol timings, card formats
- Prototype PCB layout designed with Eagle CAD
  - Version 1.00 PCB made with toner transfer method
  - Power supply and UPS module PCB created
- EM4100 RFID reader hardware acquired
- System components assembled on plywood fixture
- Code development started
- Version 1.00 of code and software tested

The Design Process

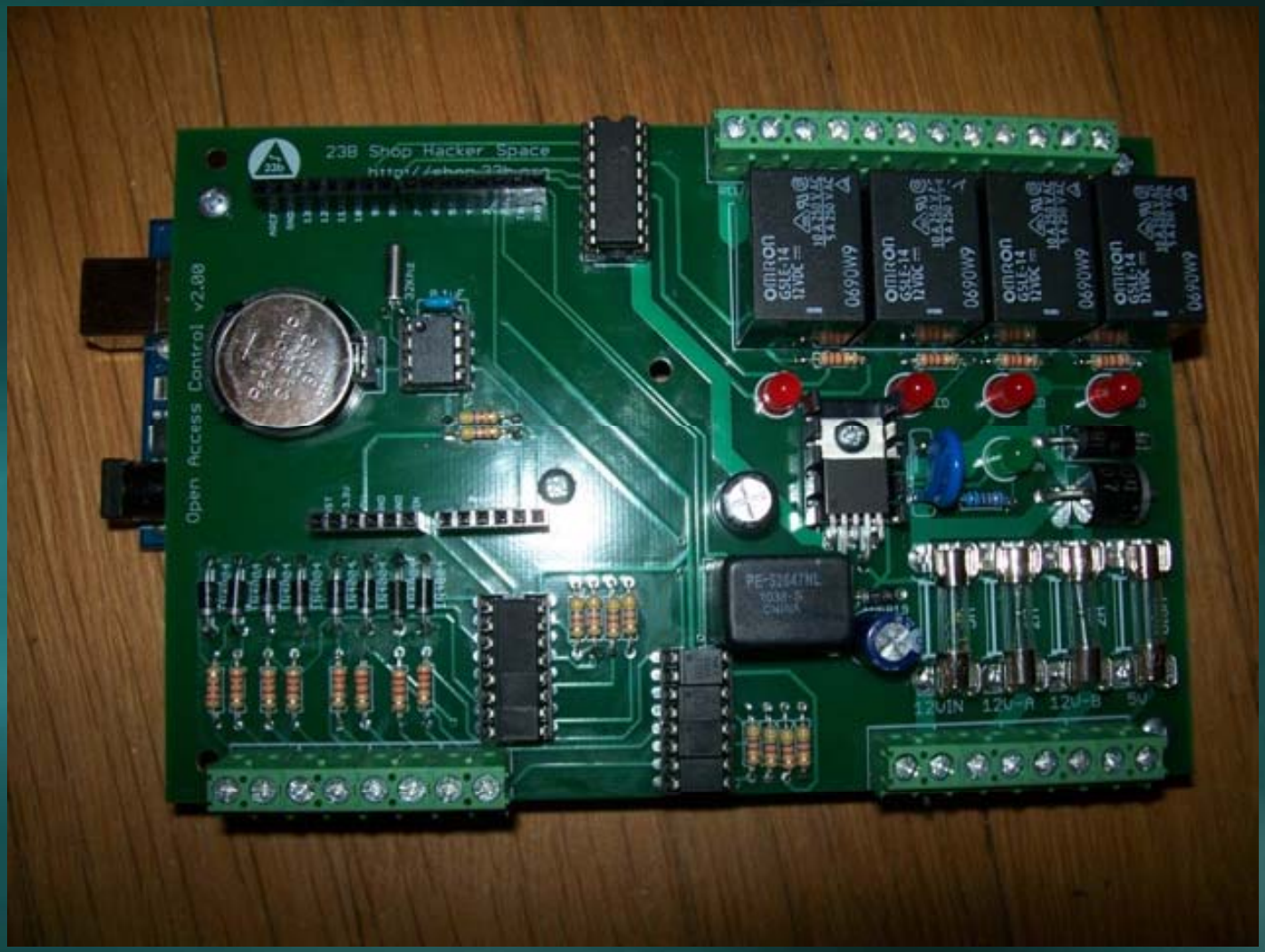
Version 1.0



The Design Process

Finalizing the Hardware

- Code and hardware refined as the result of extensive testing
  - Switching power supply for greater efficiency
  - Higher current capacity on traces
  - Additional input protection
- Version 2.0 PCB created and sent out for manufacture
- Code modified and extended
  - 200 user database stored in Arduino eeprom
  - Interactive console added for administration
  - Alarm and access functions fully implemented
  - Hardware test routine added and documentation created



The Open Access Control (v2.10)

Open Access Control

Current (2.11) Feature List

- Supports Arduino-compatible hardware with Atmega 328 CPU
- Wiegand26 reader support (Two readers in v2.x hardware, up to 3 possible in software)
  - Uses separate 0's and 1's line, 50-200uS pulses
  - Interrupt-driven
- Real-time clock (DS1307 RTC in v2.x hardware)
- On-board 5V switching power supply (1A rating)
- Alarm monitoring with 4xsupervised multiple zones
  - Alarm integration via dry contacts
  - Direct alarm via Linux logging host
- Serial/USB logging to log server
- 200 user local database
  - Records use 5-bytes each of Arduino EEPROM
  - 255 Security levels
- Remote administration via serial console
- Extensible and easy to modify via Eagle CAD files, Arduino IDE

Installation and Commissioning

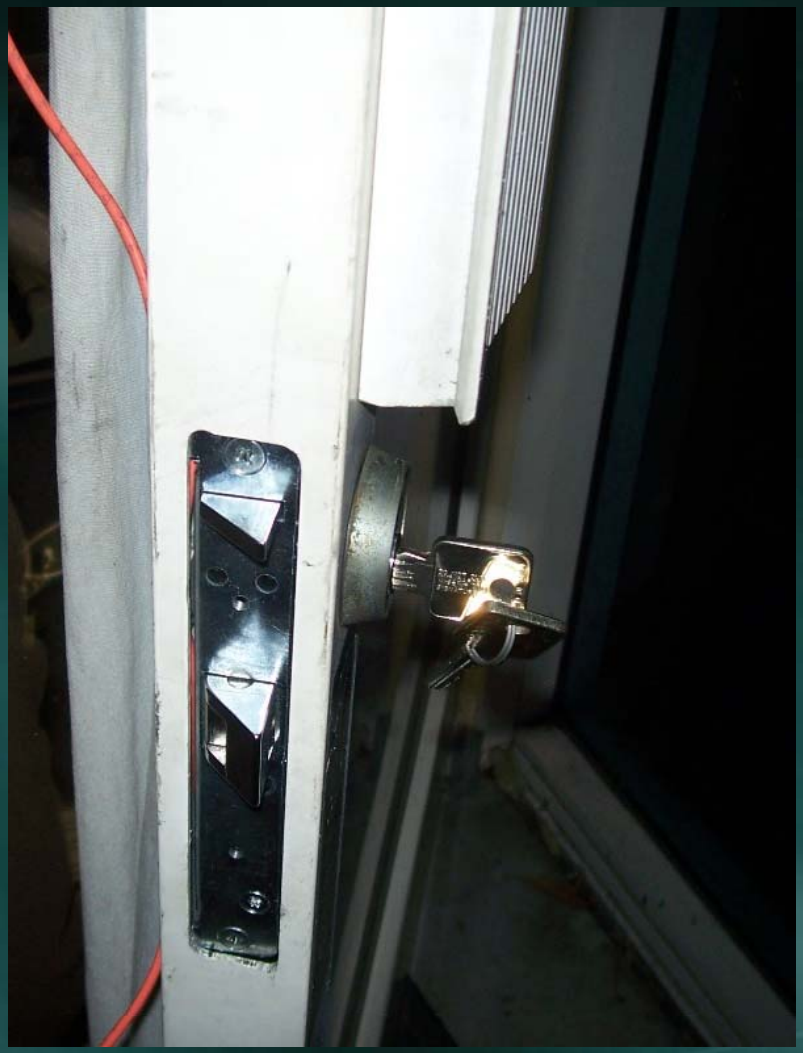
Using the damn thing

- System packaged in recycled alarm panel with new locks
- Commercial-grade 12V electric door hardware installed
- Existing alarm sensors integrated
- User database and sensor levels programmed
- System logic and program flow modified to fit environment

Open Access Control

Version 2.0

- External Switching PS
- Filtered AC power
- Uniterruptable Power Supply (UPS)
- Ethernet Module support
- Locking enclosure



Adams-Rite Model 4200 Electric Strike

Double door Magnets (SDC)

Single Door Magnet with Bosch REX sensor

Security Testing

Wiring and Physical Connections

- Vulnerabilities found in wiring
  - MITM attacks possible with Wiegand Protocol (Zac Franken, LayerOne 2007)
  - Wiring can be shorted out, possibly blow fuse on fail-open doors. (Door magnets are fail open by design)
  - Readers have an LED and chime to indicate door status. Can be back-fed with 12VDC to power up door hardware without authorization
  - Alarm sensors can be shorted out or have power interrupted to improperly indicate an exit request or falsify door status
  - High voltage can be applied to data lines, resulting in unpredictable behavior or system damage

Security Testing
Readers and Tokens

- Vulnerabilities found with readers
  - Contact readers require outside wiring, difficult to protect
    - Can be easily disabled or vandalized, resulting in denial of service
  - Contactless (RFID) tokens can be read by an unauthorized reader
    - Cloning attack on user's token
    - Replay attack on reader
    - Skimmer attack possible using device placed on or near reader
      - Can even use reader's own RF field
  - Readers can be DoS'd if an unauthorized card is held near reader or glued down
  - Very few systems have any type of encryption or challenge-response protocol
    - Systems that use this are expensive, proprietary.
    - Mostly used for payment applications

Some Access Tokens

Security Testing
Physical Hardware

- Vulnerabilities found with door hardware
  - Door magnets depend on perfect contact
    - Normally can hold stronger than the door itself, but holding strength is greatly reduced if a sheet of paper or piece of tape is applied to the magnet or bar
  - Some door strikes made of non-ferrous materials
    - Possible to retract solenoid with strong magnets on some models
  - Exit readers are often installed insecurely
    - Motion detectors can be fooled into opening by items thrown through the door crack
    - A balloon can be inserted under door and inflated with Helium to trigger sensor
    - Buttons can often be accessed with a coat hanger or custom tool

Demo

Recommended Reading

Books

- Ross Anderson “Security Engineering, Second Edition”
  - (Wiley, 2008)
- Thomas Norman “Integrated Security Systems Design
  - (Elsevier Books,2007)
- Klaus Finkenzeller “RFID Handbook”
  - (Wiley, 2003)
- Bruce Schneier “Beyond Fear”
  - (Wiley, 2003)
- Amal Graafstra “RFID Toys”
  - (Wiley ,2006)

Recommended Reading

Links

- “Access Control Systems” - Zac Franken, Defcon 15
  - http://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-zac.pdf
- “Reconsidering Physical Key Security” – Wang, Larson, Savage (2008)
  - http://cseweb.ucsd.edu/~savage/papers/CCS08OptDecode.pdf
- Wiegand Format Documentation (Electrical)
  - http://www.robotshop.com/content/PDF/wiegand-protocol-format-pr25.pdf
- Wiegand Format Documentation (Data Format)
  - http://www.hidglobal.com/documents/understandCardDataFormats_wp_en.pdf
- Alarm Notification and Verification Procedures - CSAA
  - (http://www.csaaul.org/ANSI_CSAA_CS_V_01_20040922.pdf
- “Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities”
  - http://jps.anl.gov/Volume4_iss2/Paper3-RGJohnston.pdf
- Smart Cards and Biometrics in Access Control Systems – SCM Microsystems
  - http://www.biometrics.org/bc2005/Presentations/Conference/Wednesday%20September%2021/Wed_WashAB/Merkert_SmartCards_and_Biometrics.pdf


Questions?

Build it!

- Download the Code and Eagle files:
  - http://code.google.com/p/open-access-control/