Open Source Physical Security

John Norman
23b Shop Hacker Space
jnorman@accxproducts.com

What this talk is about:

- Physical Security (i.e. people, assets, buildings)
- Electronics locks and access systems
- Intrusion detection and alarm technology

This talk is mostly not about:

- Mechanical Locks
- Network and Information Systems Security
- Video Surveillance
- Security Policy Development

Introduction

Why are we doing this?

- Security and Access Control Systems are mostly closed-source and very little is published about them
- According to their manufacturers, all of the available systems are made of magic and invulnerable
- Consequently, it’s hard to make a real risk/benefit assessment

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

Three Categories of Site Users*

- Those who *support* The Mission
  - Founders, Homeowner, Partners, etc.
- Those who *oppose* The Mission
  - Thieves and other criminals, competitors, etc.
- Those who *sometimes support and sometimes oppose* The Mission
  - Almost everyone else
  - Employees, Contractors, Guests

** (2011) Electronic Access Control by Thomas L. Norman*

Different goals for each Group

- Core users/supporters of The Mission
  - Same safety and security goals as other authorized users
  - Protect people and assets they are responsible for
  - Make it easy to manage the site
    - Auditing, key control, etc.

- Criminals and other outside threats to the facility
  - Prevent, Inconvenience, and increase the risk associated with these activities
- The rest
  - Manage Inside Threats
    - Visitors, contractors, employees, pizza guy
  - Deal with granular access control
    - Limit access by zone, time, group, etc.
  - Auditing
    - Access logs, video, etc.
  - Key revocation/life cycle

Physical Security

Risks and Threat Model

Physical Security countermeasures perform 4 basic tasks

Deter → **Detect** → **Delay** → **Respond**

- Overall purpose is to enforce a Security Policy

Physical Security

Some "Model Attackers"*

- Derek
- Charlie
- Bruno
- Abdurrahman

** (2008) Security Engineering: A Guide to Building Dependable Distributed Systems by Ross Anderson*

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 different 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 memory 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, tempered glass windows, and a basic alarm system that may or may not be used consistently.
- A larger site may have electronic access system, an on-site security staff, and better locks
- Targeted at The “Derek” and “Charlie” model attackers
- Quality data centers and high-value sites also attempt to delay a more sophisticated “Bruno” type attacker.
- Abdurramhan is a problem for the military

Commercial Systems

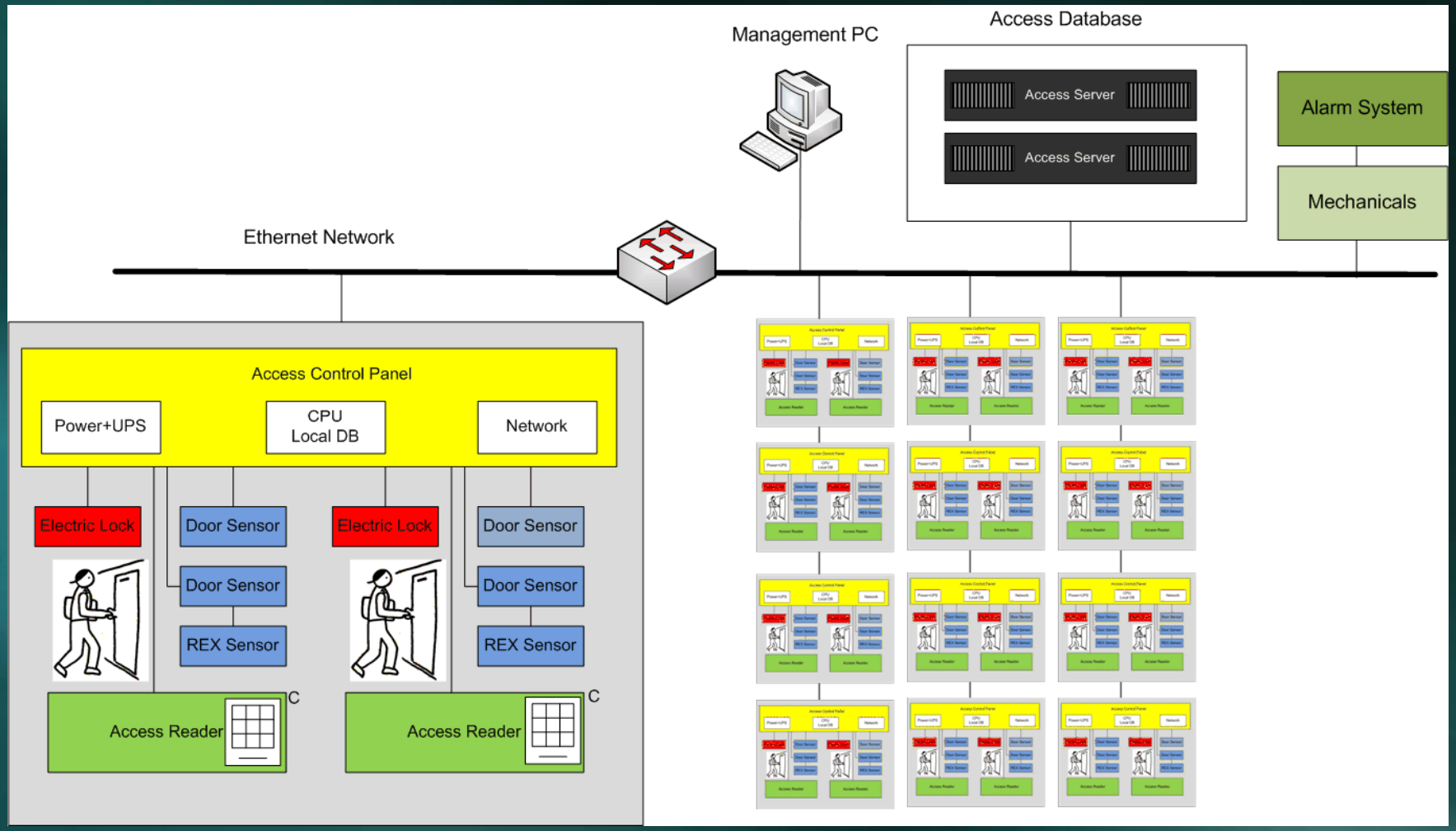
Typical Features of a Building Access System

- Distributed modules that control 1-4 doors. May be server or appliance/panel-based
- A Windows workstation for managing the system
- Electric locks on perimeter and/or suite doors
- Access token readers
  - Cards (contact or contactless)
  - PIN readers, biometrics, other technologies

Commercial Systems

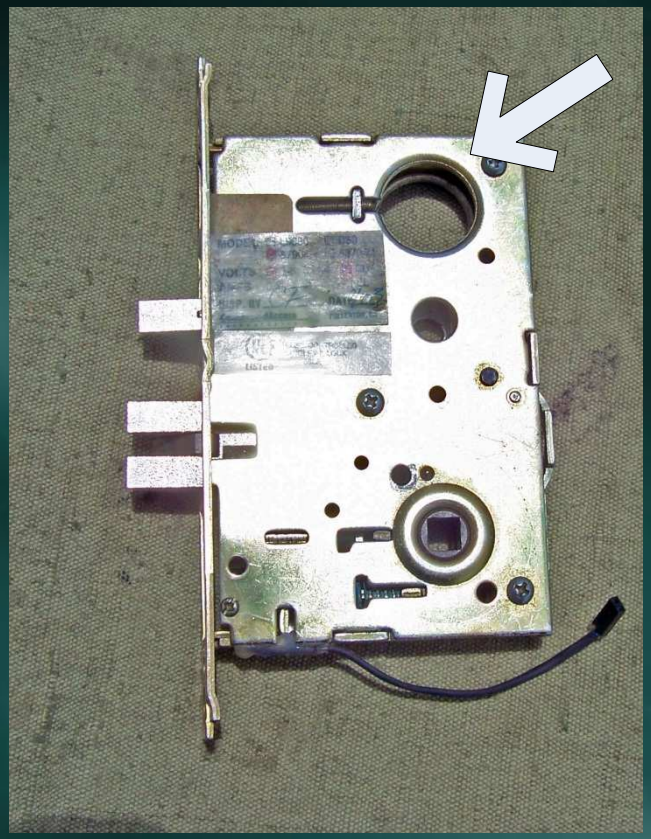
Typical Features of a Building Access System

- Exit devices for personnel
  - Panic bars, handles or “Push to Exit” devices
  - “Request to Exit” sensor also tells panel to suppress alarm when door is opened
  - Motion sensors and buttons for magnets and non-doorknob type locks
- May integrate with alarm or video system
  - Fancy systems can script HVAC and lighting commands



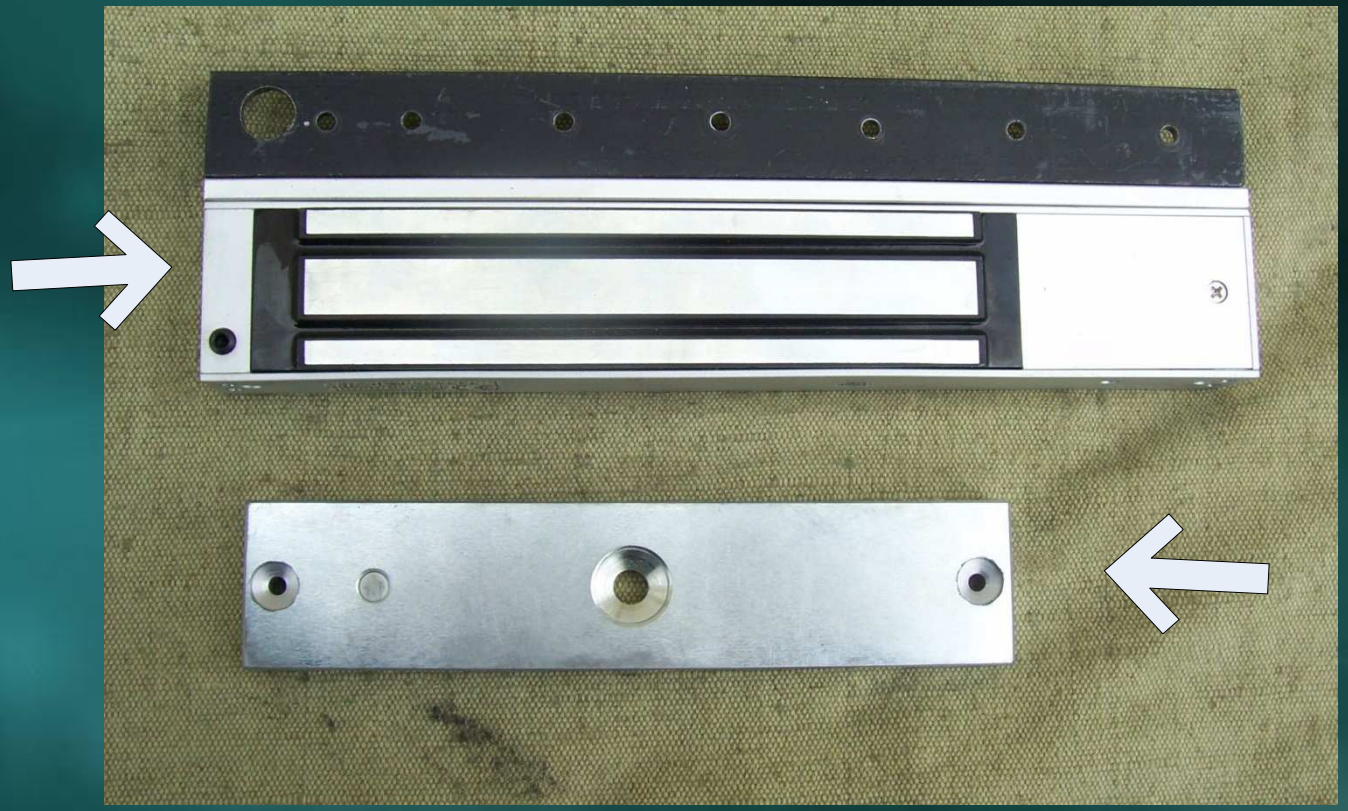
Typical Access System

Mortise Locks



- Embedded inside door, difficult to force open or gain access to the insides
- Bottom “Deadlatch” is locked from being retracted when door is closed
- Activated by solenoid
- Key (1.25” commercial cylinder) and handle bypass

Magnetic Locks

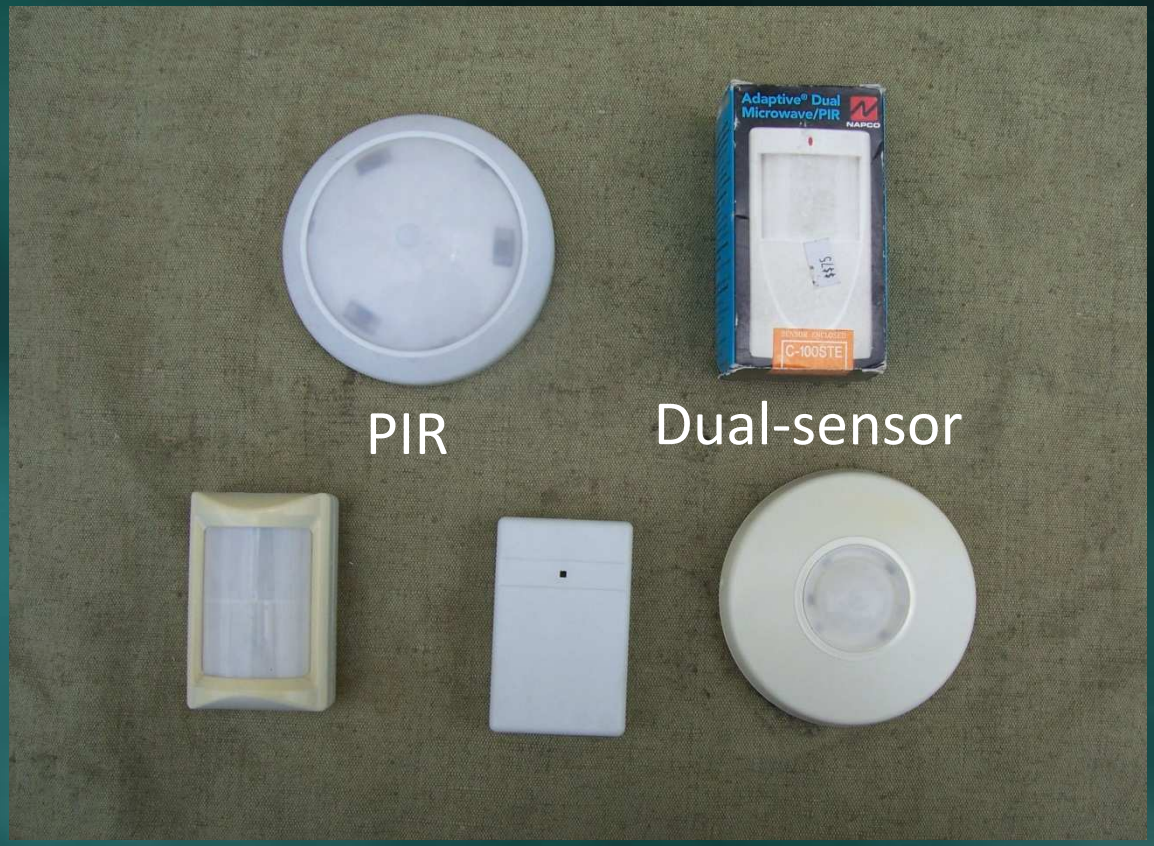


- Fixed part is the electromagnet (150-1200+lbs strength)
- Metal plate is called the “armature” and is mounted to door
- Requires precise alignment
- “Fail safe” operation but requires a separate exit device

Token Readers

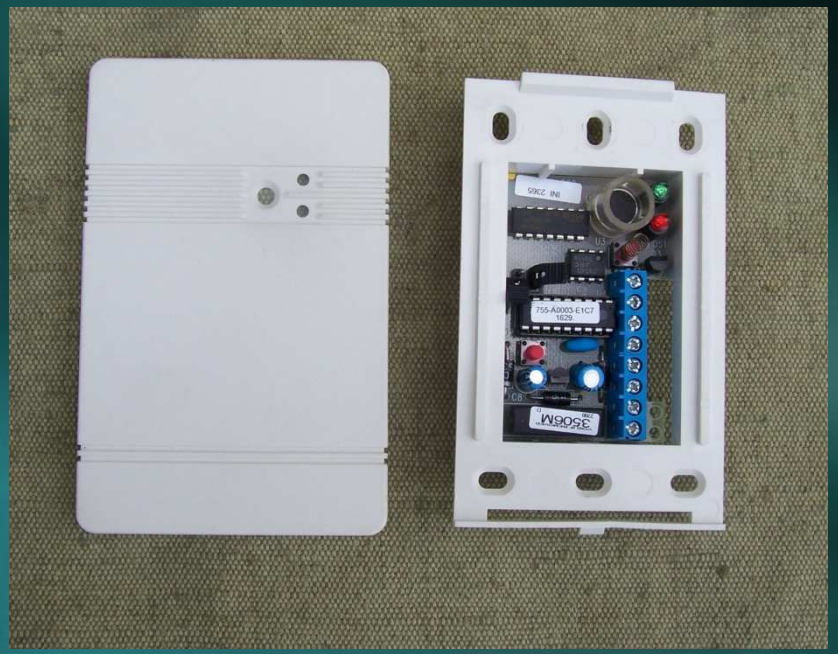
- Available in a variety of configurations (PIN+token, PIN only, Biometrics)
- Wiegand, RS-485 Ethernet, proprietary serial Interfaces

Infrared and Microwave Sensors



- Passive Infrared (PIR) sensors – Detect movement
  - Contain two IR sensors and filters to detect body heat
- Dual-zone – contain both microwave and PIR
  - Much less prone to false triggering

Acoustic Sensors



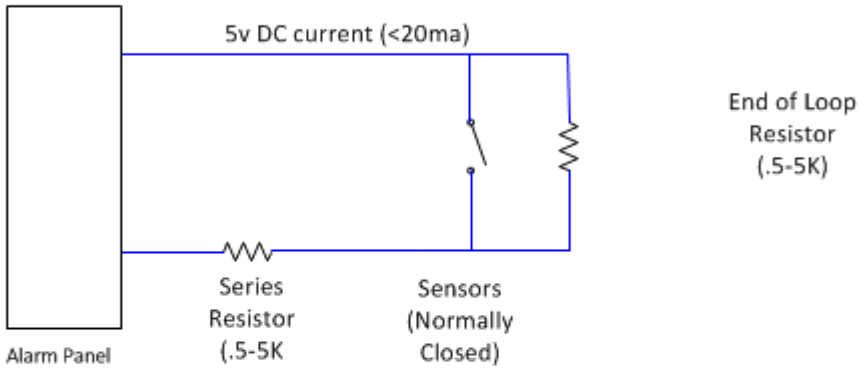
Acoustic Glass Break

Ultrasonic Motion Detector

- Acoustic Glass Break sensors can protect several windows
  - Less prone to false alarms than foil tape
- Dual-zone – contain both microwave and PIR
  - Much less prone to false triggering

Typical Alarm Wiring

3-State Alarm Supervision



1. Normal (current travels through switch(es) and the series resistor.
2. Sensor activated (switch opens, current travels through EOL resistor
3. Wire cut/break (causes open circuit condition)
4. Wire shorted before series resistor (causes resistance drop)

-Requires that the alarm panel be able to detect a ~1K change in loop resistance
-Requires that sensors be in a NC (normally closed) state
-Multiple sensors can be placed in series
-Normally-open sensors can be placed on the series resistor path, eliminates detection of cut state.
-Some installations do not use a series resistor at all

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
- Encourages users to follow security policy
  - 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

- Tokens can be cloned electronically
- 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 and wiring

Types of Access Tokens

- Contact
  - Magnetic Stripe
  - Wiegand Cards
  - Smart card/chip with contacts
  - iButton
- Contactless
  - Passive RFID (typical RFID tags)
  - Active RFID (Mobile Speedpass, asset tracking tags)
  - Remote Controls

125-135Khz (LF) Tags

- Read range of 0-5cm, requires a large coil for longer distances
- Primarily read-only (HID, EM4100), some are read-write (Q2)
- Slow data transfer, typical 32-128bits of storage
- Some have security features (Hitag

Some LF Access Tokens

13.56Mhz (HF) Tags

- Read range of 10-20cm, more with HF antenna
- More advanced features available (Encryption, 3-phase authentication, read/write security)
- Most common is the ISO 14443a, aka Mifare

Some HF Access Tokens

RFIDEAS Card Classifier

EM Card Cloner and Q2 tags

Bottom line on Contactless Tokens

- Most cards with security features are closed-source and not well-documented
- Cards such as the Hitag used in cards have an active cloning community
- Technology was developed for low-cost, not security.
- Cards that have been reverse-engineered have all been found vulnerable
- If it can be read, assume it can be cloned.
- Implement security in software, don’t trust the card!

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 cheap, 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

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 other open micro for maximum hackability and customization
  - Use only commodity components

Open Access Control - Today

- ~15 Active sites worldwide and 300+ users
- 1+ year of Usage and testing
- 4 code contributors
  - Database application in development
  - Simple web-based console available
  - Serial console, Linux script-based monitoring

The Design Process

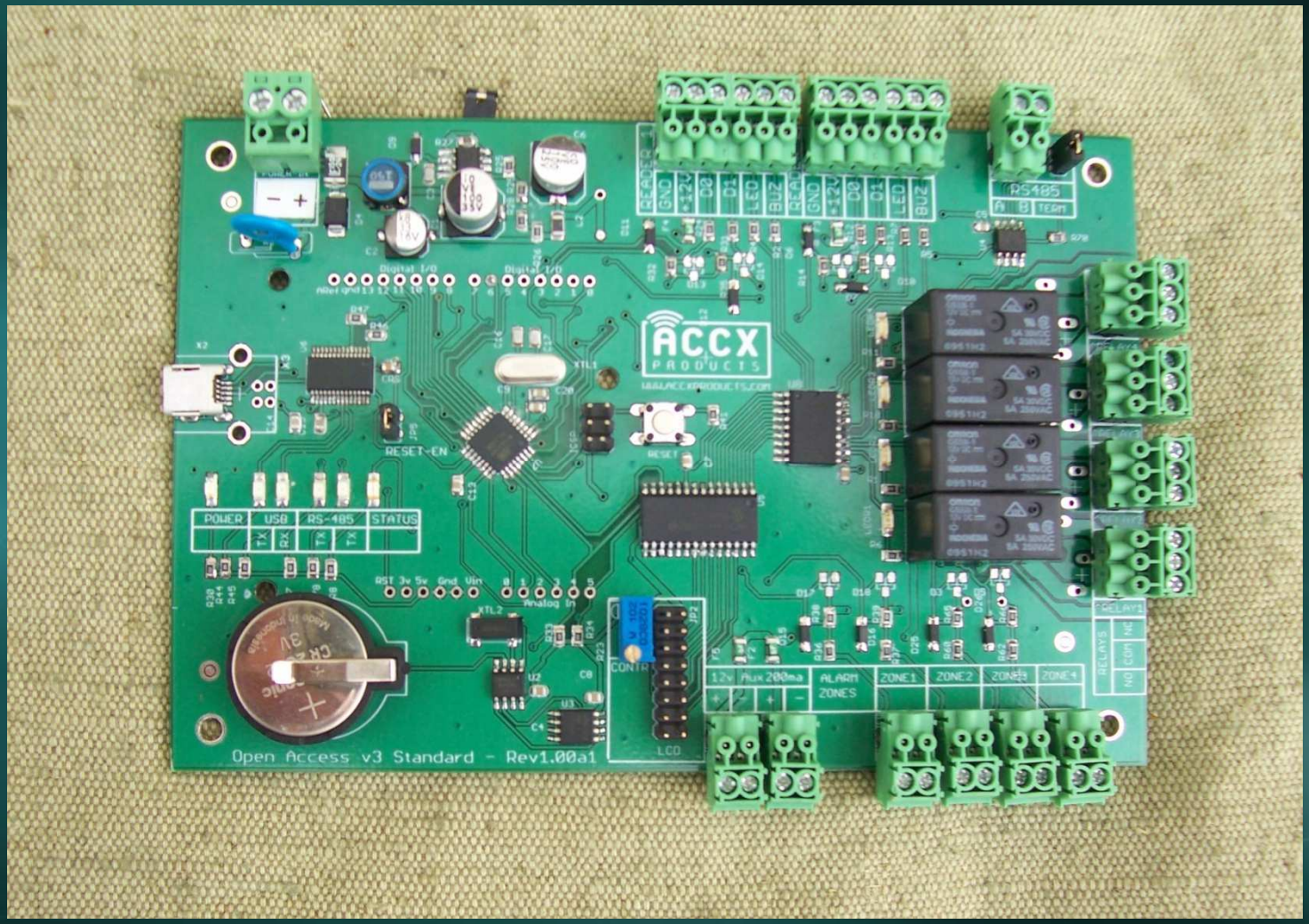
Version 1.0

The Design Process

Version 2.0

The Design Process

Version 3 Standard



Open Access Control

Current Features – V.3 Standard

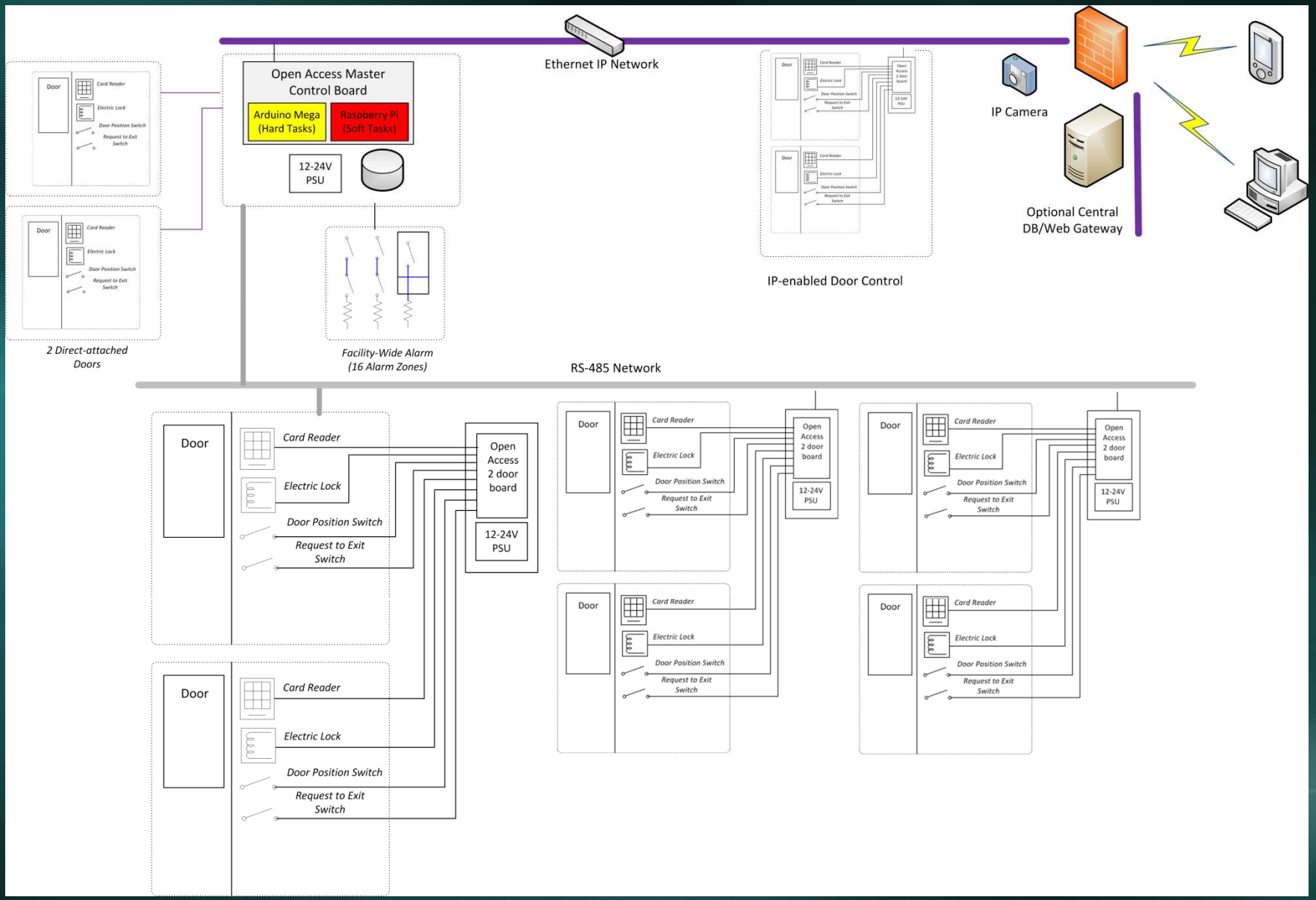
- Code and hardware refined as the result of extensive testing
  - High-efficiency switching power supply
  - (2) Fully-implemented Wiegand Reader ports
  - RS-485 port
  - Built-in Atmega 328P and FTDI USB (Arduino-compatible)
  - 128KB User database
  - (4) Supervised alarm zones
  - LCD and auxiliarry GPIO ports
  - Real-time clock with battery backup

Open Access Control

Current Features – V.3 Mega

- Similar to v3 Standard, but more bigger
  - Uses Arduino Mega (installs as a shield)
  - (8) 5A relays
  - (15) Supervised alarm zones
  - (1) 0-20VDC monitoring zone
  - 128KB User database
  - Real-time clock with battery backup

Network and Architecture



Open Access Control

Version 2.0 Install

- Switching PSU with UPS backup
- Locking enclosure
- Plenty of room left for wiring

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

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

Double door Magnets (SDC)

Bosch REX sensor

Looking to the Future

- Fusion of multiple Sensor zones
  - Train motion detection zones using Monte Carlo algorithms
  - OpenCV machine vision
  - Eliminate Falsing, lower the noise floor
- Linux MCE Integration (Lighting, HVAC, Z-Wave locks)
- Privacy-enhanced video surveillance
  - Use spare relays to only power cameras when alarm system is armed
  - Detect Bluetooth or WiFi from phone, disable surveillance of private areas when owner's phone is associated
- Fault-tolerant notification
  - Network failover (additional wireless access points, GSM, POTS)
- Software-defined radio
  - Detect jamming, cell phone activity, etc

Recommended Reading

Books

- (2008) *Security Engineering: A Guide to Building Dependable Distributed Systems*, Ross Anderson
- (2011) *Electronic Access Control*, Thomas L. Norman
- (2003) *RFID Handbook*, Klaus Finkenzeller
- “Beyond Fear”
- (2003) *Beyond Fear*, Bruce Schneier
- (2006) RFID Toys, Amal Graafstra “RFID Toys”

Recommended Reading

Links

- “Access Control Systems” - Zac Franken, Defcon 15
  - http://www.defcon.org/images/defcon-15/dc15-presentations/dc-15-zac.pdf
- “Practical Attacks on the MIFARE Classic” Wee Hon Tan
  - http://www.doc.ic.ac.uk/~mgv98/MIFARE_files/report.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

Questions?

Build it!

- Access Control Wiki, Kits, etc
  - http://www.accxproducts.com
- Download the Code at:
  - http://code.google.com/p/open-access-control/