Access Control Done Right the First Time

Tim Clevenger

About me

Day job: Network Cybersecurity Engineer

Lenel/S2 certified (access/video) in a previous life

nsfw on the Physical Security Village Discord

About this talk

I’m here to present some tips and tricks for those looking to install, better maintain or upgrade a physical access control system.

Many vendors sell a “minimal viable product”

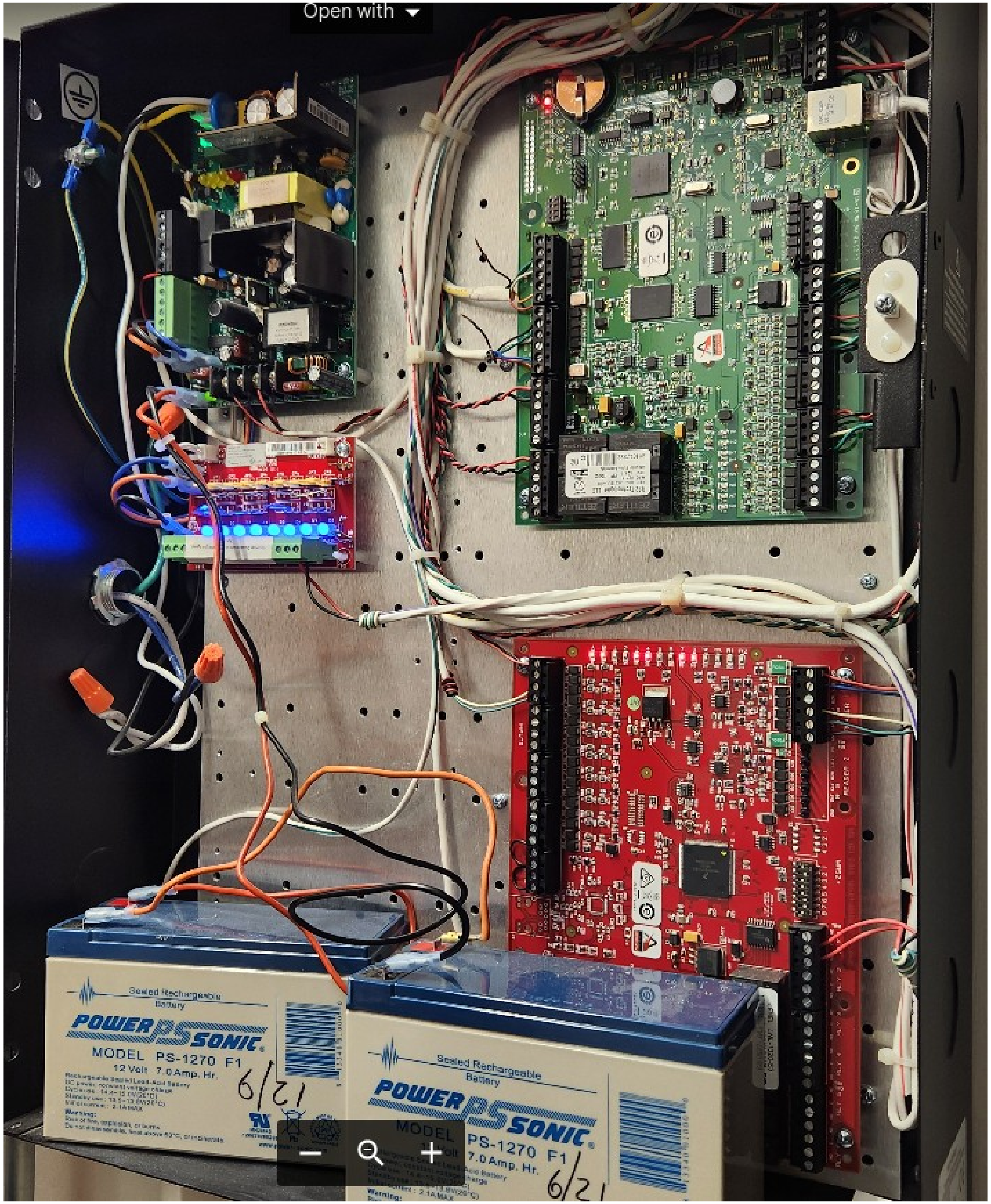
This talk focuses on larger facilities and those who need or want a more secure and reliable access control system

Choosing a system

Mercury Security equipment

- Local storage, independent of network
- Multiple vendor support
- Can be reflashed

Avigilon, Genetec, Honeywell, Lenel/S2, RS2/Acre

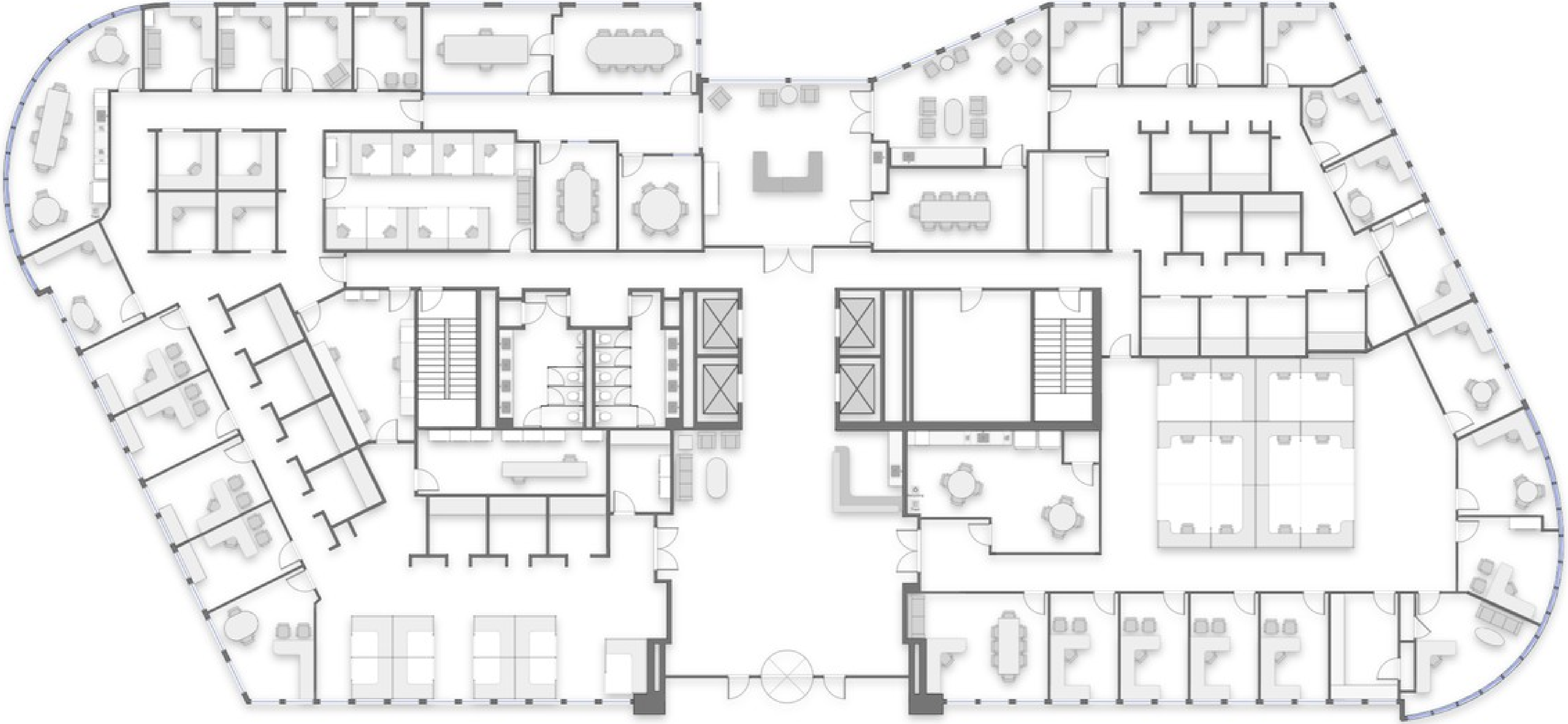

Open with
Sealed Rechargeable Battery
POWER PS SONIC
MODEL PS-1270 F1
12 Volt 7.0 Amp. Hr.
6/21
12/9
Sealed Rechargeable Battery
POWER PS SONIC
MODEL PS-1270 F1
7.0 Amp. Hr.
6/21

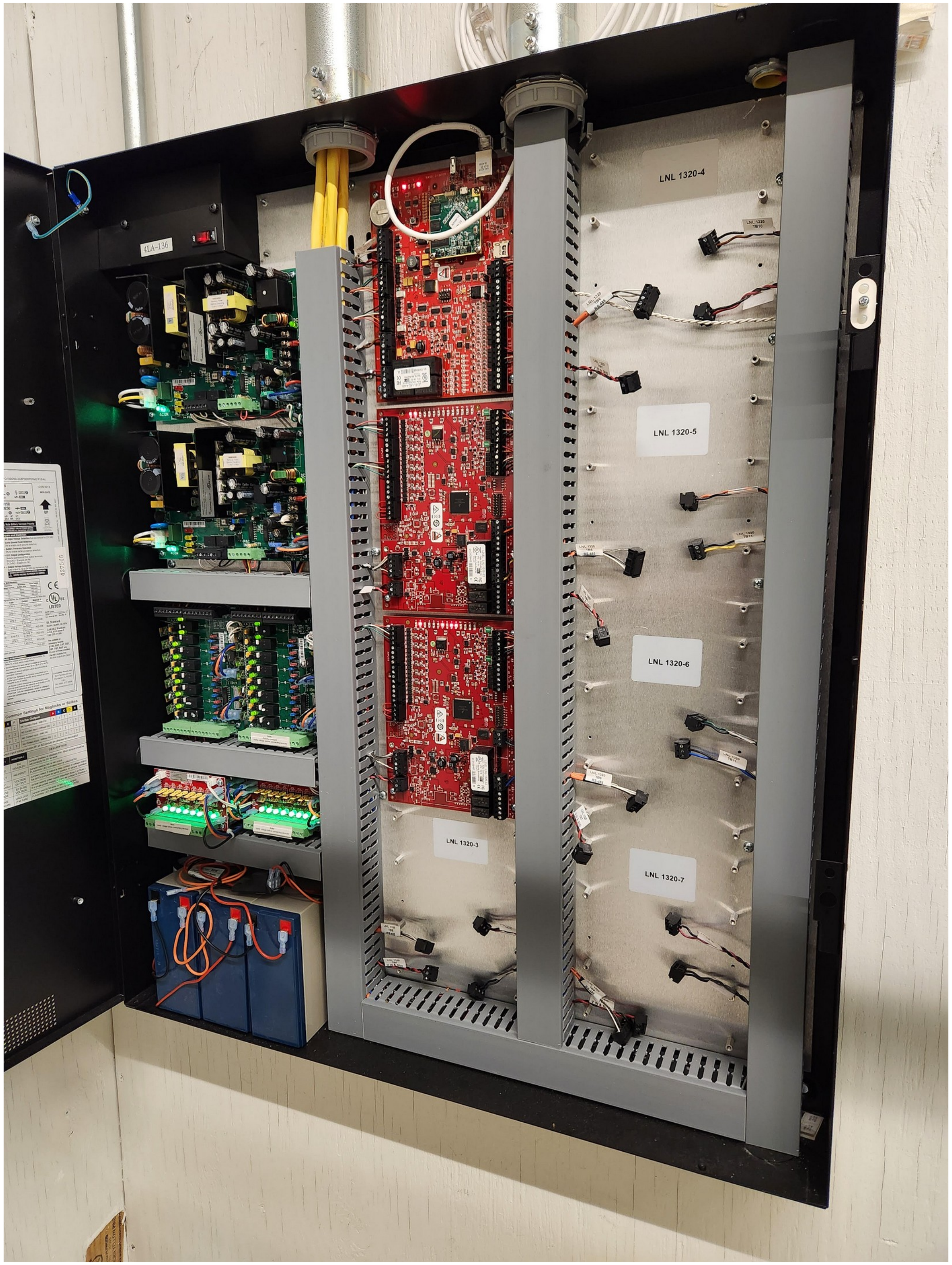
System layout considerations

- Wiring considerations
  - Ethernet drops
  - RS-485 communications: 4,000 feet?
  - Distance to doors: will I need a remote power supply?
  - Hard lid, block walls, integrity/security (conduit)
  - High heat, humidity, EMI situations

System layout considerations

System layout considerations




4LA-136
LNL 1320-4
LNL 1320-5
LNL 1320-6
LNL 1320-3
LNL 1320-7

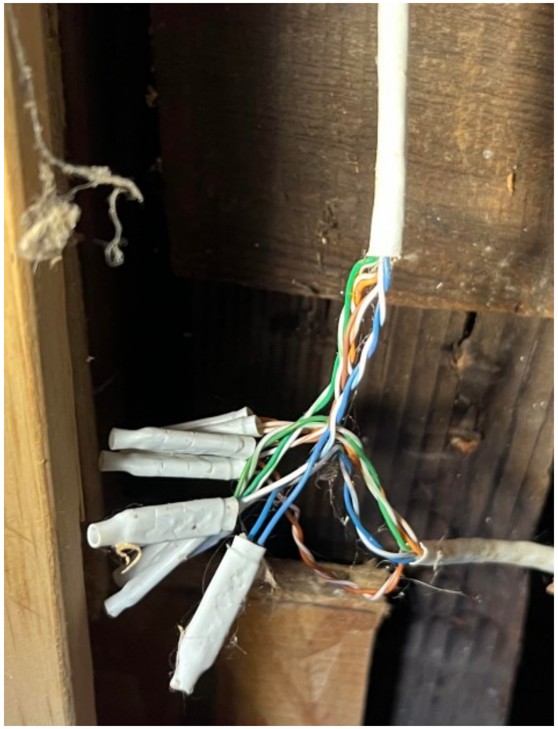
Wiring to the door

- Wiring requirements
  - Power to door hardware, motion sensors
  - Shielded cable to badge reader (or RS-485)
  - Door contact and request-to-exit wiring
  - Tamper switches, aux inputs/outputs

Wiring (the WRONG way)

Undersized or spliced power conductors

- Insufficient power to unlock door
- Fire hazard



Unshielded or spliced cable to reader or controller

- Communications intermittent
- Can't open door

No wiring for tamper and aux inputs/outputs

- Badge duplication/compromise
- Limited expandability

Wiring (the RIGHT way)

Composite access control cable

Multiple options

Properly shielded

Thick exterior jacket

Power and enclosures

Power supply

- Power supply/charger
- Verify amperage and temperature range
- AC fail and battery fail outputs

Power and enclosures

- Enclosure
  - Multiple sizes
  - Sold as kit with power supply
  - Pre-wired or DIY
  - Key lock and tamper switch
  - Optionally weatherproof

Batteries

12V gel-cell batteries in series/parallel

Typically 12 volts, 7 Ah

Write install date on batteries

Replace every 3 to 5 years

Remote power supplies

- Required for power-hungry locks
  - Motorized crash bar
  - Magnetic locks
- Often hidden in the ceiling
- Power supply/charger
- Tamper/battery fail/AC fail
- Batteries

Fire safety

Fail safe vs. fail secure

Local code and AHJ

Building fire alarm

Door hardware

Electrified strike
- Noisy and finicky

Solenoid
- Can get hot/fail

Magnetic lock
- Needs more power
- Always fails safe

Motorized crash bar
- Expensive

Door hardware

- Door contact
  - Door status (open or closed)
  - Reed switch on door frame or integrated into handle
- REX (Request to Exit)
  - Allows door to open from “secure” side
  - Button, buzzer, motion detector or integrated into handle

Supervision

For door contact and REX

Resistors in serial/parallel
- As close to contact as possible

Different resistance readings (NC)
- Wires cut: infinite ohms
- Wires shorted: zero ohms
- Contact open: 1,000 ohms
- Contact closed: 2,000 ohms

Motion detectors

Used for REX (request to exit)
- Often triggers an unlock

Attack examples
- Mylar balloon
- Frozen spray from air duster

Mitigations
- Move motion farther away
- Don’t trigger unlock
- Use different lockset
- Use other REX methods

Door handle attacks

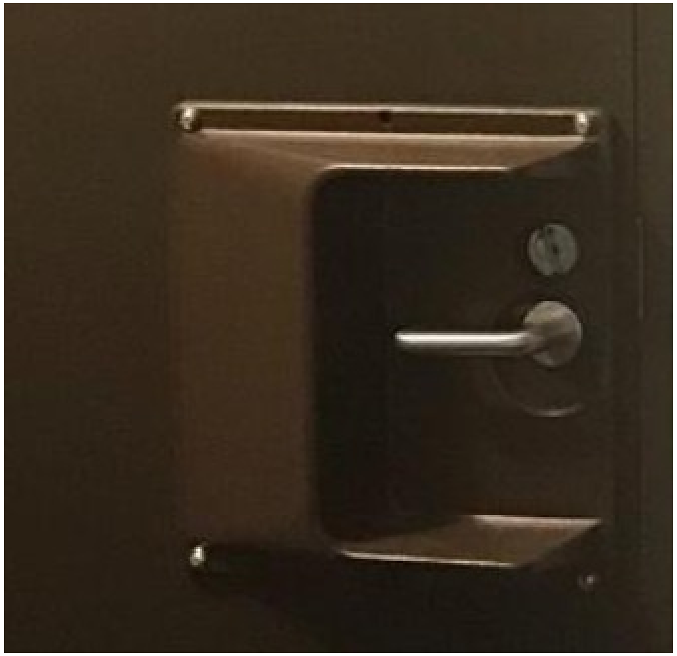
Under-door attack

- "Door forced" alarm won't be triggered if door handle has integrated REX

Attack: Under-door tool

Mitigations

- Door handle surround/skirt
- Dual REX (handle AND motion)
- Second badge reader for exit
- Pushbutton REX



Badges and readers

- Badge readers
  - Multiple sizes and shapes
    - Fobs, badges, smart cards, Bluetooth, magstripe cards
  - Additional factors
    - Biometric, PIN keypad

- Badges
  - 125KHz Prox (trivially broken)
  - 13.56MHz iClass (broken)
  - Mifare DESfire (not broken...maybe)
  - Seos (not broken...maybe)

Badges

- Prox and iClass have facility code and badge ID
  - Facility code 0-255 (26-bit format)
  - NOT random (132 is common)
  - Cards can be purchased with any facility code and valid range of badge IDs

- 26-bit format is trivial to clone
  - All readers can read it
  - Data can be captured from portable reader

Badges

Solution: custom formats

- HID Corporate 1000
  - - Seos
  - - Dedicated facility code
  - - 48-bit format

Disable older formats

- Configuration cards

Badge readers

- Wiegand communications protocol
  - Low-speed serial protocol from 1975
  - Inline capture/replay devices common

Badge readers

- OSDP – Open Supervised Device Protocol
  - High-speed two-way protocol from 2015
  - 128-bit encryption
  - Badge reader enrollment
  - RS-485 with daisy chaining
  - Not perfect:
    - Compromise during reader pairing
    - 84% of installers “never or seldom use it* ”
  - Mitigation:
    - Mind your daisy chains
    - Reader tamper switches

* https://www.sageintegration.com/blog/wiegand-nostalgia

So what should I do?

Work closely with your PM

Set expectations

Document!

Spot check

Do regular maintenance

Visit the Physical Security Village

Thank you very much!

Sample RFP on my Github:

https://github.com/TClevenger/access_control