Cybersecurity: Getting Physical

Noah Black, Student

Looking Two Moves Ahead
Attacks of Tomorrow

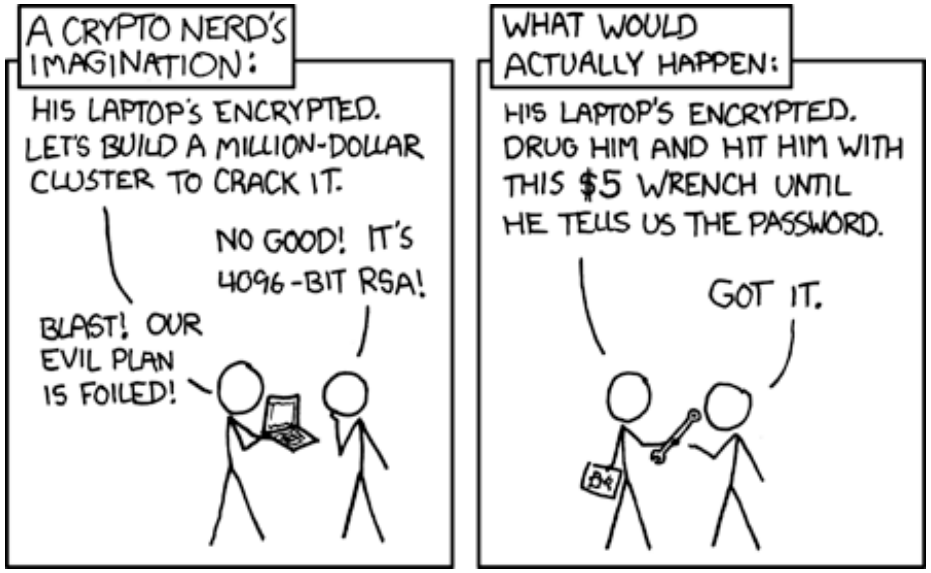
- As Networks Become more secure
  - Offensive Cyber Operations may once again become a ground game.

- Physical break-ins might prove more Clandestine
  - Computers log everything; Locks have a harder time.
  - Firewalls see every connection; Surveillance cameras can be blinded.
  - LAN Taps are hard to detect and harder to remove.
  - People are terrible witnesses

- Physical security is thus integral to cybersecurity

Background

- The field of cybersecurity has made amazing strides in recent years
- Even Industry leading Firewalls can be bypassed with the right methods.
- Physical Security is much like the $5 wrench problem

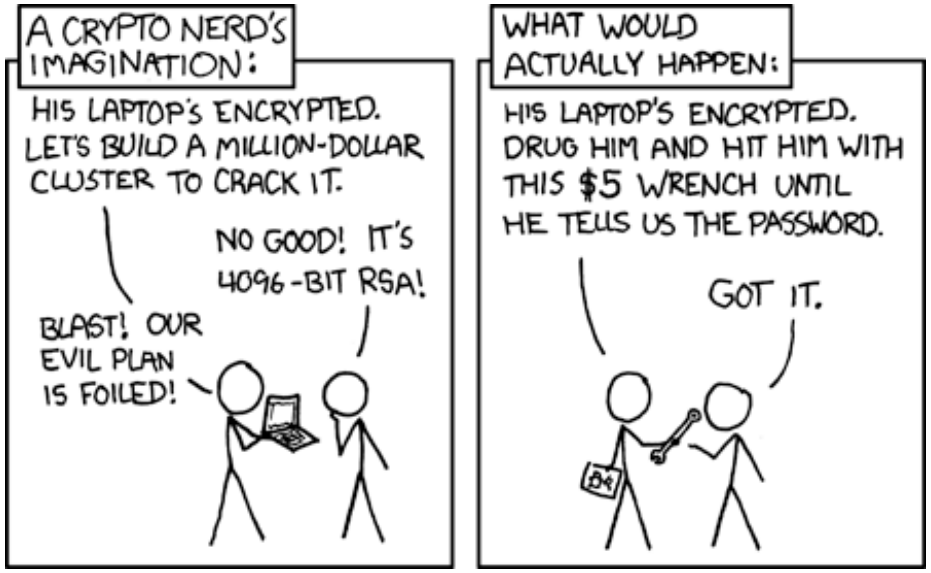


Meme Creds: https://xkcd.com/538/

$5 Wrench Problem

Reject Modernity; Embrace Tradition

- Humans can be coerced, convinced, and tricked
  - Bribery
  - Blackmail Opportunities
    - Affairs
    - Narcotics
    - Historic Criminal Activity
  - Lack of training
  - Psychology
    - Tropes
    - Subconscious Assumptions
    - Dirty Tricks



Meme Creds: https://xkcd.com/538/

Physical Compromise:

All Starts With a Single Step

Intelligence Gathering

- OSINT: Open-source intelligence
  - Documents from websites
  - Google Dorks
  - Google Earth
  - Anything willingly disclosed by the enemy
- HUMINT: Human Intelligence
  - Police reports
  - Legwork
  - Rumors, drunken stories
- ELINT: Electronic Intelligence
  - MAC addresses
  - Metadata
- Much, much more.

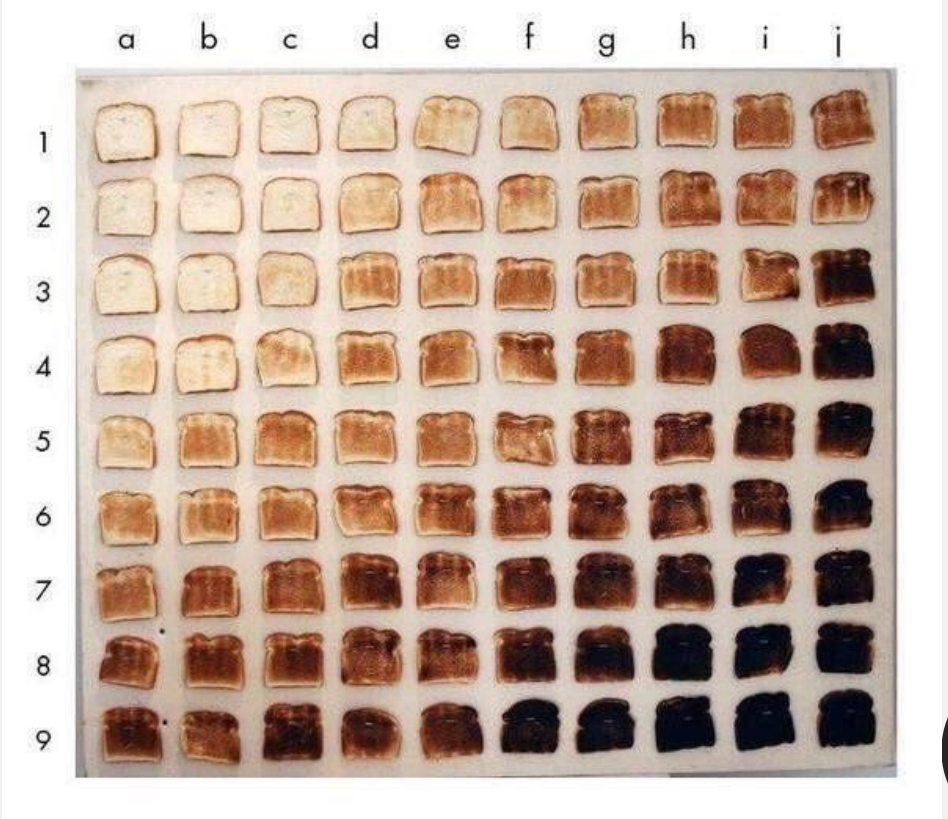
Avoiding Discovery while Gathering Intel

Intro to Making Toast, a Hackers breakfast.

- Think of discovery as burning your toast.
- The more overt fun you have, the more burnt your toast.

- Ideally, you want to have enough fun to get the job done but not so much that you get burnt.

For simplicity: Noise = Overt Activity = Heat



Humans: The weakest link.

- The human is, and always will be the weakest link in Cybersecurity.
  - Humans need to use the system for it to function.

- Human attack vectors include:
  - Social Engineering to gain unauthorized access
  - Some of the first things us hackers look to use:
    - Reused passwords
    - Improperly configured services
    - Phishing

- Even with training, it's still an issue.
  - Because we're only human.

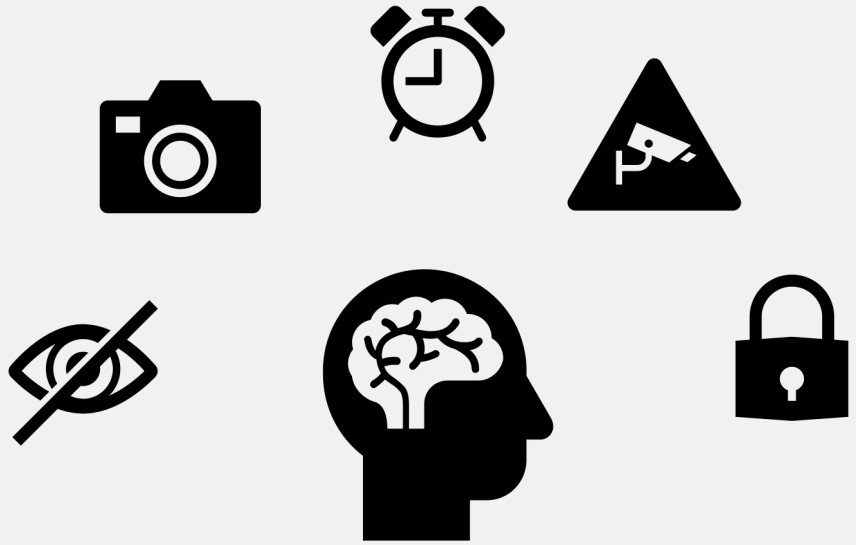
- This is only the surface of this attack vector.

Leverage Over Humans

- Depending on the actor
  - Certain things should be expected
    - Blackmail over
      - Affairs
      - Narcotics
      - Depraved Activities
      - Crimes
    - Bribery
    - Threats of violence
- These threats should be considered
  - Adequate background checks
  - Psych evaluations
  - Counterintelligence

Gaining Access

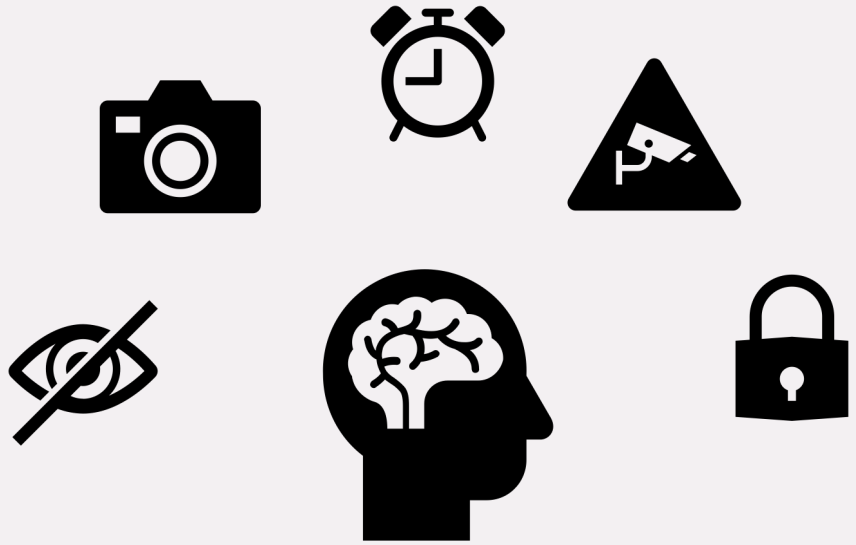
- After intelligence gathering and processing
  - Put the black hat on
  - The ‘how’ generally becomes apparent
    - Plans A, B and C can also be formulated
  - Social engineering plots form
    - If the operation necessitates
  - Pretexts fall in line
  - Soon, You’re ready to rock



Social Engineering

- It’s not just phishing or hiding payloads in word documents

- You don’t need an MS in Psychology
  - Just understand the basics
    - How people form suspicion
    - How they see others around them
    - Common subconscious ticks
    - Default trusting state



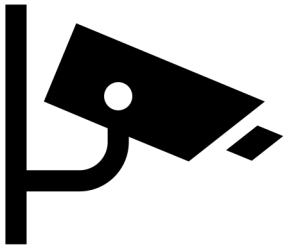
Looking the part: implied trust.

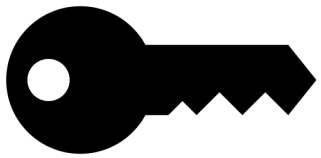
Social Engineering

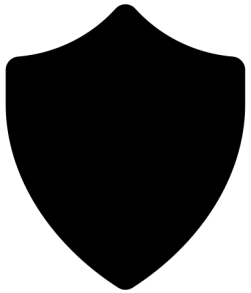
- People don’t bother you if you look like you belong.
- Walk with purpose and they will assume you have one
- How do you look the part?
  - Hi-Visibility vest or tee-shirt
  - Clipboard
  - Tool bag
  - Big old key ring

Typical Setups

- Access control:
  - Locks, padlocks
  - RFID
- Recording devices
  - Security Cameras
  - Motion Sensors
- Security Guards
  - Armed
  - Unarmed
- Employees







Video Surveillance

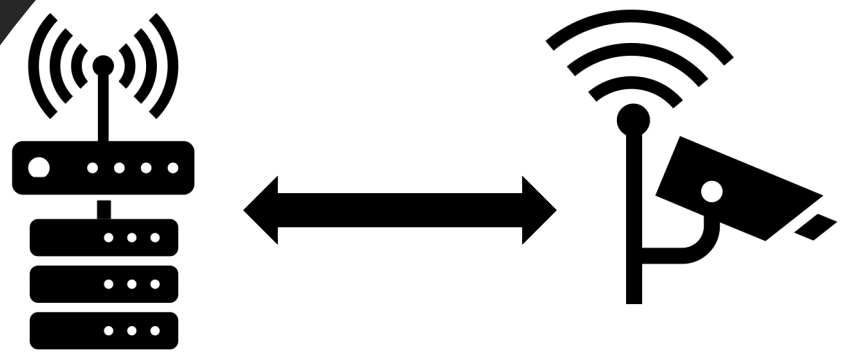
- Surveillance Cameras
  - Used for intrusion detection
  - Static Deterrent
  - Insurance purposes
- Main Types
  - CCTV (Coaxial)
  - CC/IP (Ethernet/POE)
  - Wireless (Wi-Fi)

Tampering

- CCTV
  - Hard, but not impossible (High Heat)
  - Bugging Complicated
    - Social Engineering required
    - Target the recorder, not the camera
- CC/IP (Ethernet/POE)
  - Bugged easily (Medium Heat)
  - LAN Tap (Low/Medium Heat)
- Wireless
  - Bugged easily (Medium Heat)
  - Vulnerable to Wi-Fi MITM (Low Heat)
    - Harry Potter Invisibility cloak

Wi-Fi Camera Hacks
Ferris Bueller Style

- Hybrid use of known attacks
- Evil Twin Attack
- Leveraging Default Configurations
- What you need:
  - Vendor
    - Retrieved using ELINT (MAC Address)
  - SSID (Network Name)
    - Retrieved using OSINT or ELINT
    - Even if the network is Hidden!
  - Password not necessary for DOS
    - Flaw in 802.11 (Wi-Fi) Protocol
    - Client attempts connection anyway

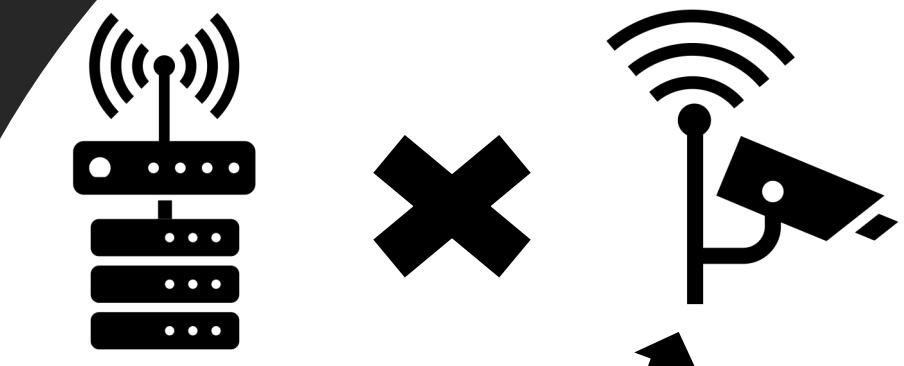


NVR Recorder

Hak5 Wi-Fi Pineapple

Wi-Fi Camera Hacks
Ferris Bueller Style

- Hybrid use of known attacks
- Evil Twin Attack
- Leveraging Default Configurations
- What you need:
  - Vendor
    - Retrieved using ELINT (MAC Address)
  - SSID (Network Name)
    - Retrieved using OSINT or ELINT
    - Even if the network is Hidden!
  - Password not necessary for DOS
    - Flaw in 802.11 (Wi-Fi) Protocol
    - Client attempts connection anyway



NVR Recorder

Hak5 Wi-Fi Pineapple

RFID Cards: How they work

- How do RFID Cards work?
  - The Reader emits a radio signal
  - This signal is used to power a microchip
    - Magnetic Inductance
  - This microchip screams data
  - That data is read by the reader for authentication

Mifare Reader

HID Prox Reader

HID iClass Reader

Common RFID Hardware

- RFID Electronic Access Control
  - Two Major Types:
    - Low Frequency (LF)
    - High Frequency (HF)
- Products
  - Hid Prox (LF)
  - Hid iClass (HF)
  - Mifare (HF)
  - Multi-tech LF/HF variants also exist

Mifare Reader

HID Prox Reader

HID iClass Reader

Common RFID Vulnerabilities

- Low Frequency (LF)
  - Ease of cloning
  - Read Range (3 Feet)
  - (Really) Weak Card Cryptography
  - Default Configurations
  - Ease of Tampering
- High Frequency (HF)
  - Ease of Cloning
  - Weak Card Cryptography
  - Default Configurations
  - Designer implementation = Designer exploits

Mifare Reader

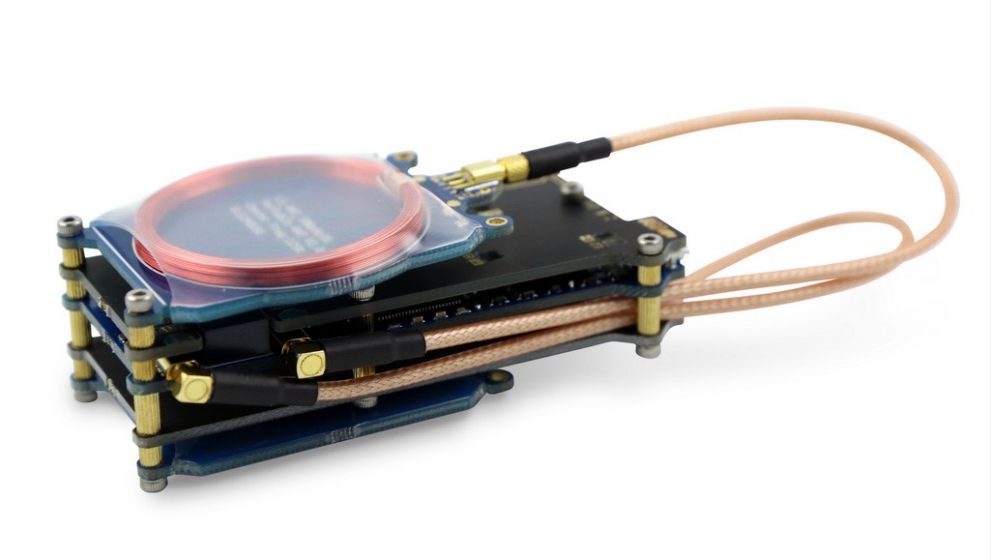
HID Prox Reader

HID iClass Reader

LF/HF Card Cloning

- What is Cloning?
  - If the card or the data is intercepted
  - The card can be impersonated
    - The reader is none the wiser

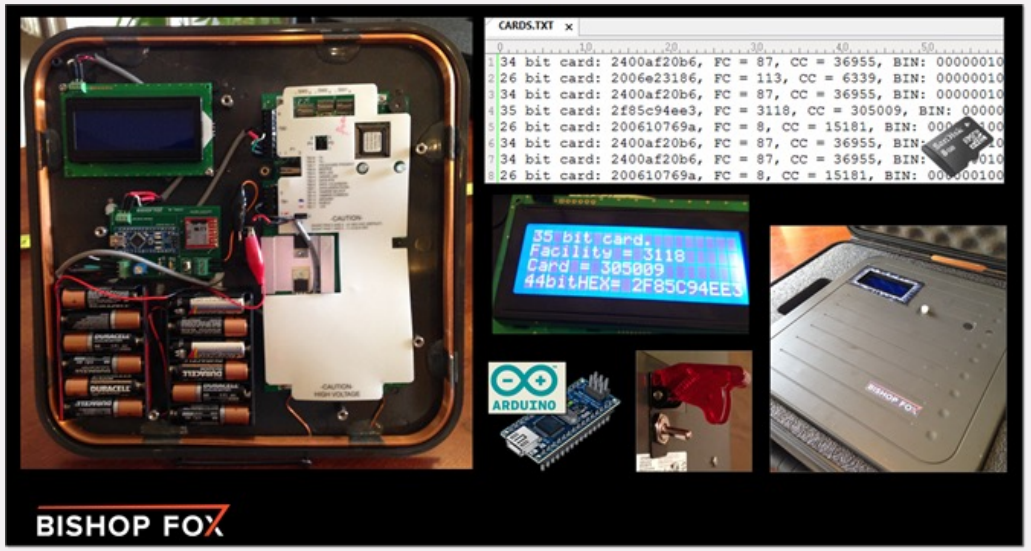
- How you ask? With one of these!
  - Fun little all-purpose RFID toolkit
    - Reads and writes just about every smartcard



Proxmark RDV

Hacks From Hollywood Coming to a Facility Near You!

- LF Cards can be read from a much further distance.
- This hack can be done for just under $200
  - A nifty tool called the Hunt Pad
  - Grabs all that is needed to clone a Hid Proxcard
  - Some social engineering required

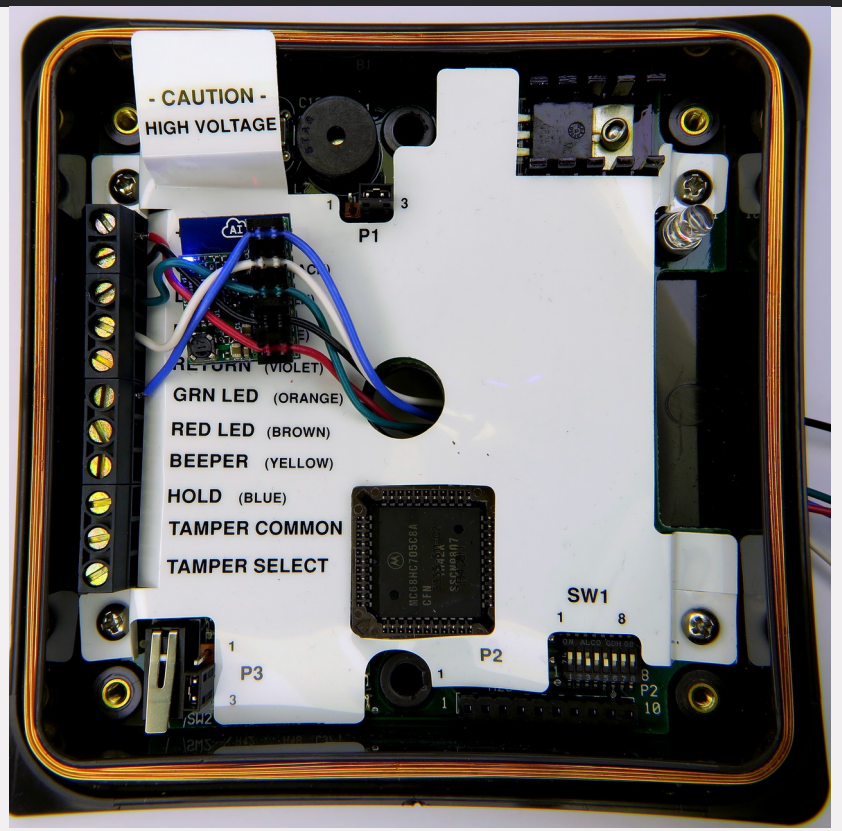


[Creds: RFID Reader Snoops Cards From 3 Feet Away | Hackaday]

But Wait, There's More!

- Cut out the middleman with the ESP Key ($75)
  - Step 1: Deploy
  - Step 2: Wait
  - Step 3: Profit
- Reads the data meant for the door controller
  - Man in the middle Attack
  - Further Intelligence gathering

ESP Key

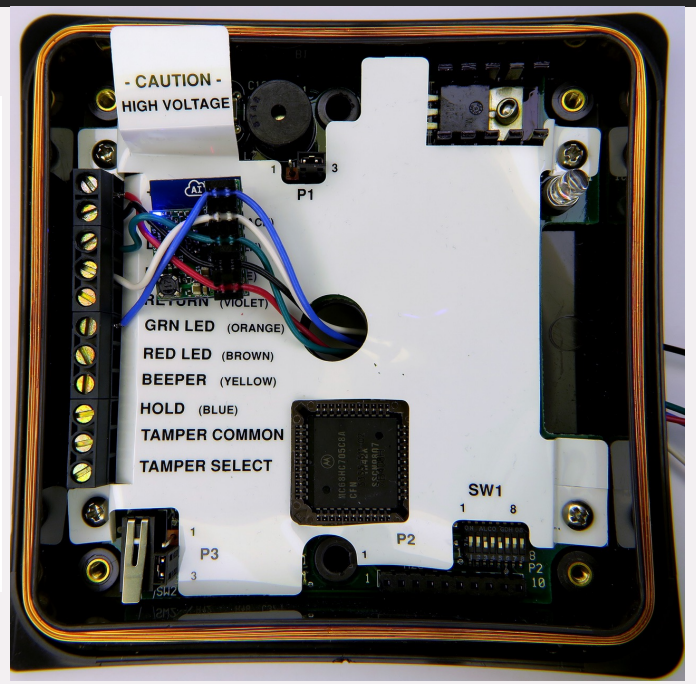


Bugged Reader

[Creds: ESPKey Wiegand Interception Tool (redteamtools.com)]

Tampering Defenses

- These systems have tamper alarms
  - They're rare
  - It's an electromagnet
  - Very easy to detect
    - With this thing →
- Counterattack to tamper alarms
  - Super Top-secret tool (Neodymium Magnet)
  - You can find good ones in old hard drives



Reader

Creds magnet search tool https://www.redteamtools.com/magneticsearchpole

Hacks From Hollywood Coming to a Facility Near You!

- HID Proxcard and Mifare cards are both vulnerable.
  - Weigand Protocol is Everywhere
  - Attack Possible because of cleartext data TX
    - Serial Encryption modules exist
    - Deployed separately from reader

  - Counterattack
    - Place the bug <u>before</u> the module

- Anyone catch something else?

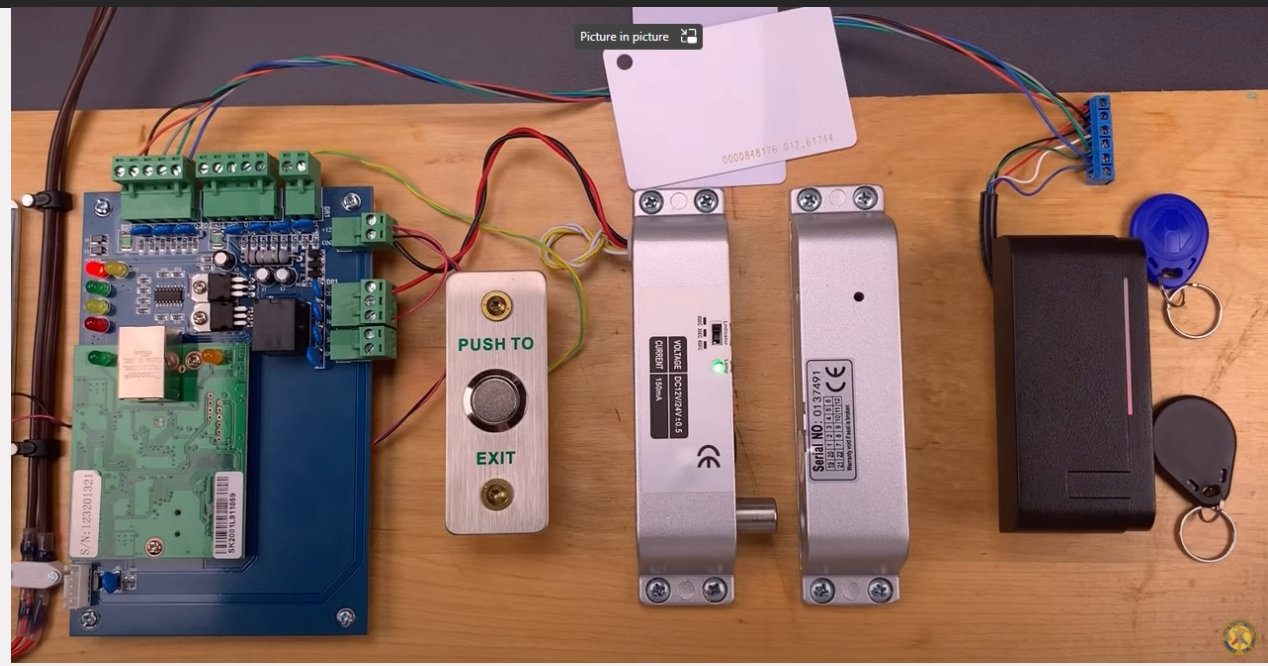


Photo Excerpt from [(60) [1052] Defeating a RFID System With The ESPKey - YouTube]

Hacks From Hollywood Coming to a Facility Near You!

- HID Proxcard and Mifare cards are both vulnerable.
  - Weigand Protocol is Everywhere
  - Attack Possible because of cleartext data TX
    - Serial Encryption modules exist
    - Deployed separately from reader

  - Counterattack
    - Place the bug before the module

- Anyone catch something else?
  - There's an Ethernet Port.
  - Door controller has a networking stack
    - Hacking at scale now feasible

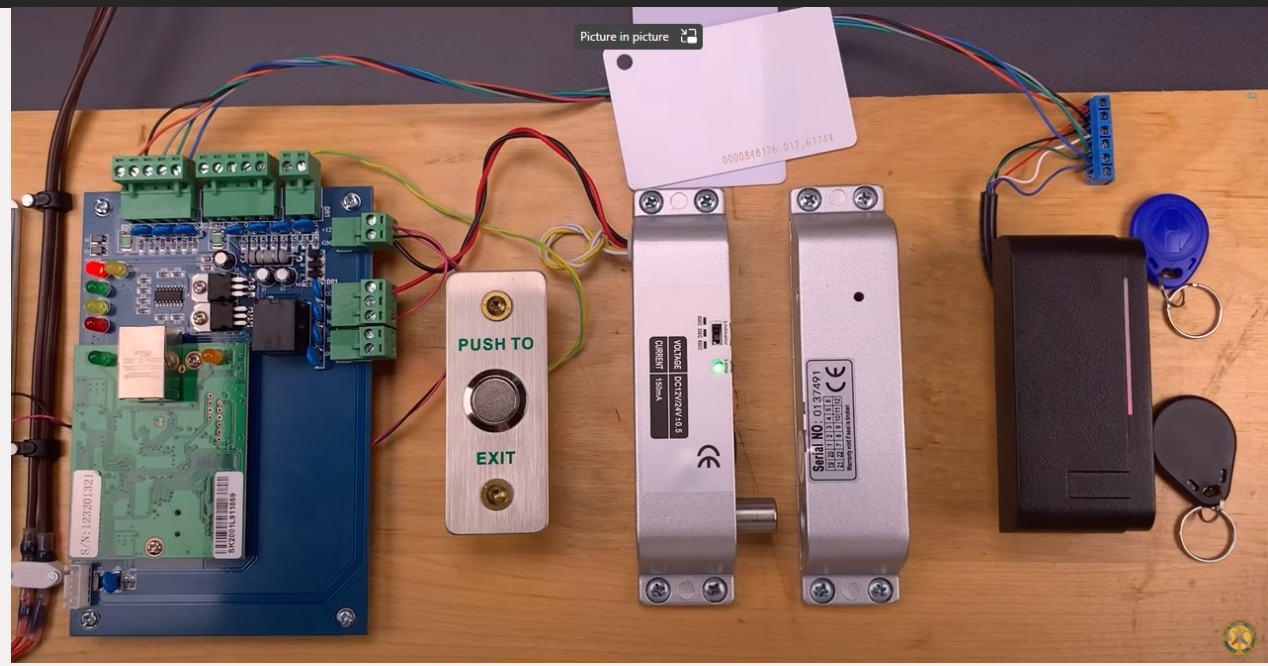


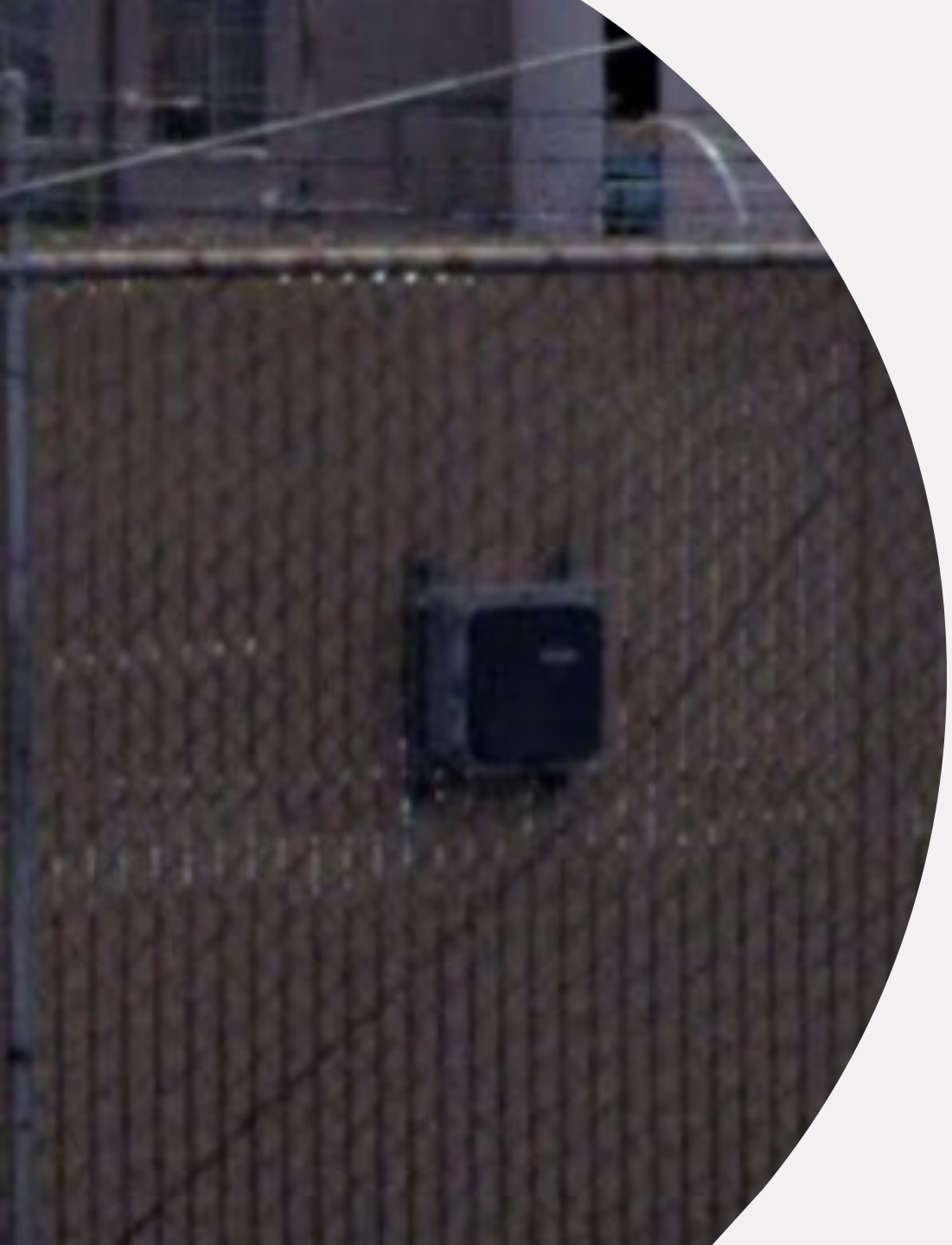
Photo Excerpt from (60) [1052] Defeating a RFID System With The ESPKey - YouTube

But Whatever You Do, Don't Do This

- Pictured is a tamper resistant card reader (redacted)
  - It is secured to a steel plate
    - Who would want to cut through that.
  - Notice anything interesting?

But Whatever You Do, Don't Do This

- Pictured is a tamper resistant card reader (redacted)
  - It is secured to a steel plate
    - Who would want to cut through that.
  - Notice anything interesting?
    - Philips head screwdriver? Probably…
    - A $3 tool can take this one off…
    - The screws in the stalls of bathrooms are higher security
  - What if it's equipped with a tamper alarm?
    - Use a magnet

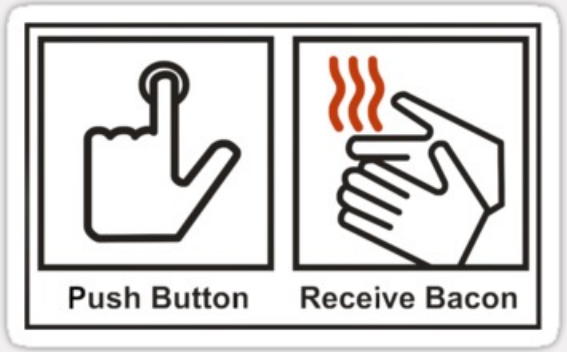


If That Wasn't Bad Enough

- You can see these from orbit
- Not subtle
- Plain as day
- This and more Found on Google Street-view (OSINT)

Hak5 Tools

Attack Platforms



Hot Plug Attacks

- Executable deployment
- Host scanning
- Keyboard injection

Hardware Keyloggers

- Remote key injection and logging

LAN taps

- Passive and Active attacks
- Surveillance
- Data Exfil

O.M.G Cable

- Code Injection Via USB
- Any mobile OS

Much more

- So much more

Tools of the trade

- Tools like these are the tip of the Iceberg
- A whole kit costs ~$500
  - Easy to use
  - Hardware can be used in abstraction
    - User can build scarier things with it
    - Check Github, new payloads every day
- Variety of toolset
- Very Effective in CQB
- But once deployed, the computer is likely compromised

Mitigation

- Just for starters
  - Avoid using proprietary cryptographic schemes
  - Train Staff
    - Make it fun
    - Morale
  - Background Checks
    - Contractors
    - Employees
  - Routine Penetration Testing
    - Physical
    - Remote
  - Network Segmentation
- IDS and Firewalls for internal and external traffic

Questions?