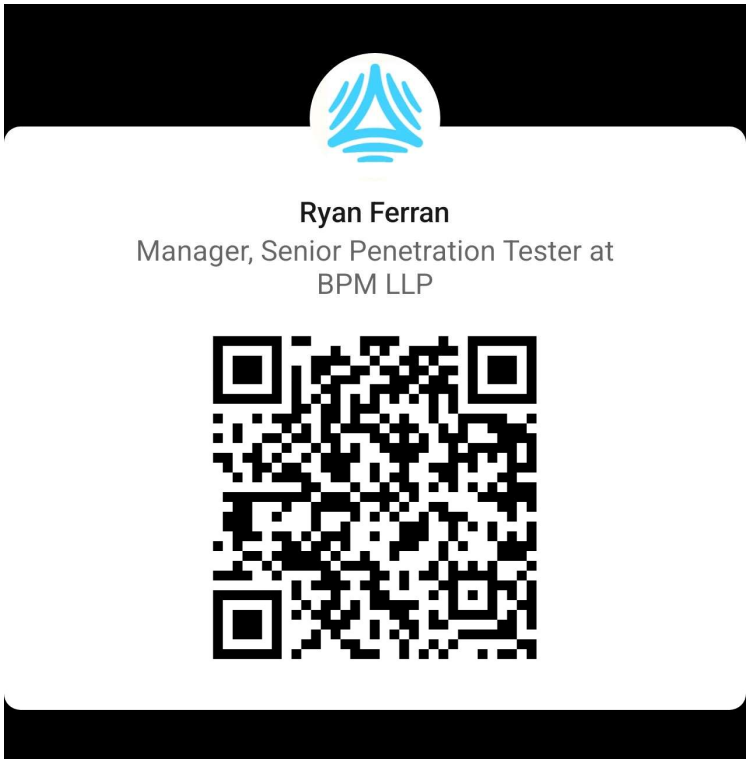

WELCOME TO THE 11TH ANNUAL HACKING CONFERENCE
How Red Teams Break Into Buildings and How You Can Stop Us
The Institute of Internal Auditors Chicago
ISACA Chicago Chapter 50

Ryan Ferran

Senior Manager, Cyber Security Assessment Services

- 20+ years in IT
  - Eight years offensive security
  - Twelve years system administration
- Technical Penetration Testing and Red Teaming
- Physical Security Team Lead
- Social Engineering
  - In-person social engineering
  - Phone-based
  - Email phishing



rferran@bpm.com

https://www.linkedin.com/in/ryan-ferran/

ryanf@bpmsec:~$ whoami

Ryan Ferran

Operational Technology Assessment Team Lead

- Power: distribution, transmission, generation on the BES
- Water Treatment, Waste Water
- Municipalities:
  - Police, Fire, Public Works
  - Airports, public services, etc, etc
- Industrial Manufacturing

Contents

- Why physical security?
- How does physical security relate to Cyber Security
- What are your publicly accessible areas and assets
- Physical vulnerabilities and exploits
- In-person social engineering
- Strategies and success stories

Questions/comments are encouraged!

Why Physical Security?

Physical security and cyber security are a two way street

- **Every Cyber event has a Physical manifestation**
- Each one protects the other
- It is still true that physical security subsumes cyber security
- Who holds the box owns the box
- Disk Encryption!
- How easy is it to physically access your internal network?

Technology is used to protect organizations physically

Technology is used to attack organizations physically

Physical Security Is More Than Fence or a Locked Door

- **In-person social engineering**
  - Lying to employees faces
  - Presenting as a vendor: SCADA, contractor, IT
  - Pretending to be an actual employee
  - Delivery, cleaning, shredding service etc.

- **Physical security assessment**
  - Analogue doors and locks
  - Physical layout vulnerabilities
  - Electronic locks
  - RFID Badge systems
  - Physical Network Access
  - Cameras
  - Alarms
  - Unlocked unattended workstations
  - Wireless peripheral devices
  - WiFi Access Points

Attacker’s Toolkit - An old version

Poll 1 — Threat Perception

"Which do you think poses a greater risk to your organization?"

1. **Physical security threats**
2. **Cyber threats**
3. **They're equally dangerous**
4. **I'm not sure**

How Does Physical Security Relate to Cyber Security?

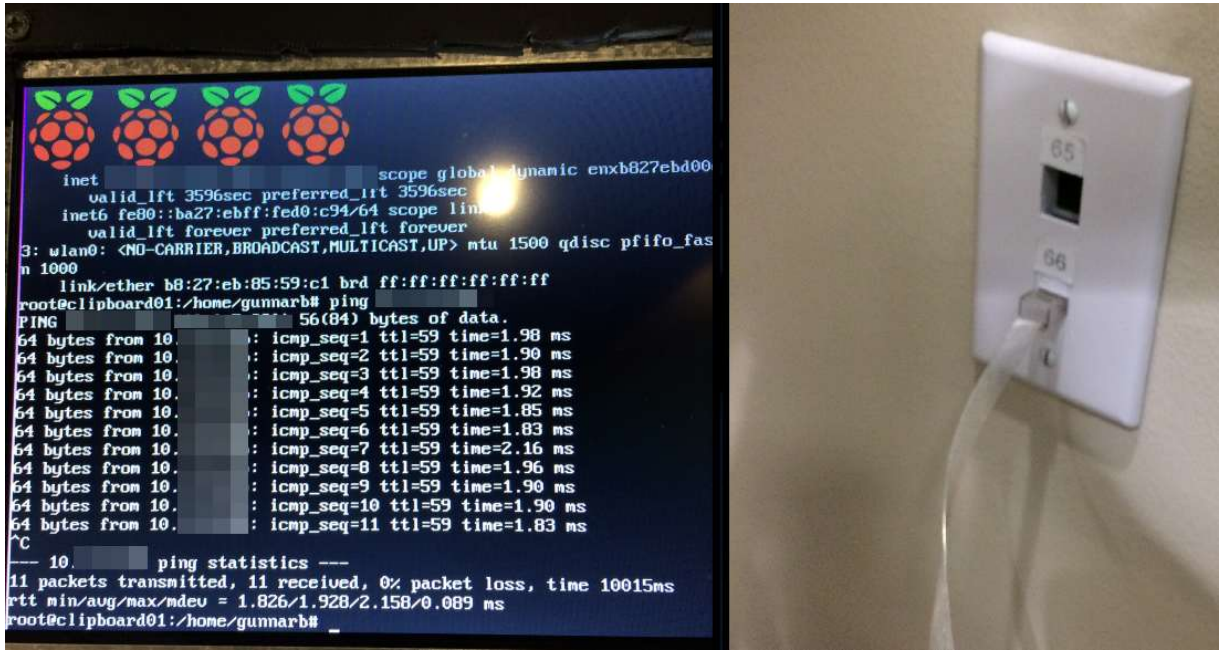
I'll Take One Order of Network Access Please

- The primary goal of a physical attack is to gain network access when remote vectors fail: **ROGUE HOST DEPLOYMENT**

- Theft of sensitive information

- Denial of service

- Common Vectors:
  - Public lobbies
  - Printers
  - Digital signage
  - VOIP phones
  - IP cameras
  - Conference rooms
  - Microwave point-to-point systems ……



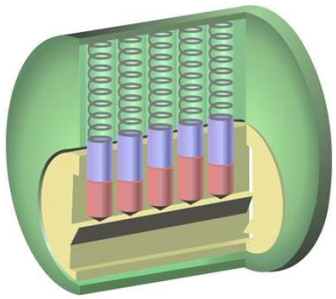
Locks

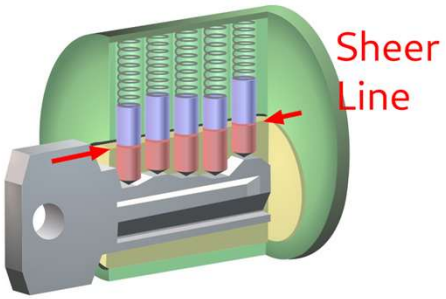
Standard Pin-Tumbler

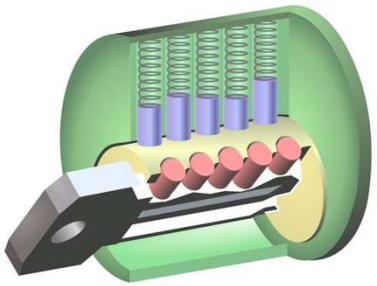
- By far the most commonly used lock design across the world

Pros:
- Cheap
- Accessible

Cons:
- Pick-able, Bump-able, force-able
- Delicate mechanism
- Well known





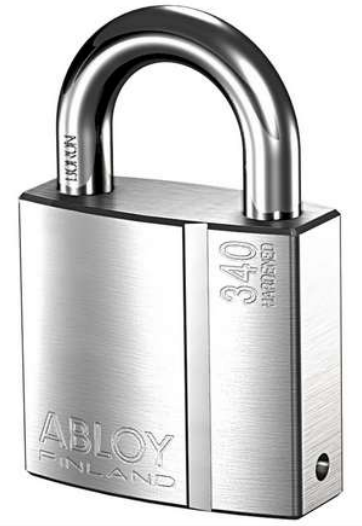


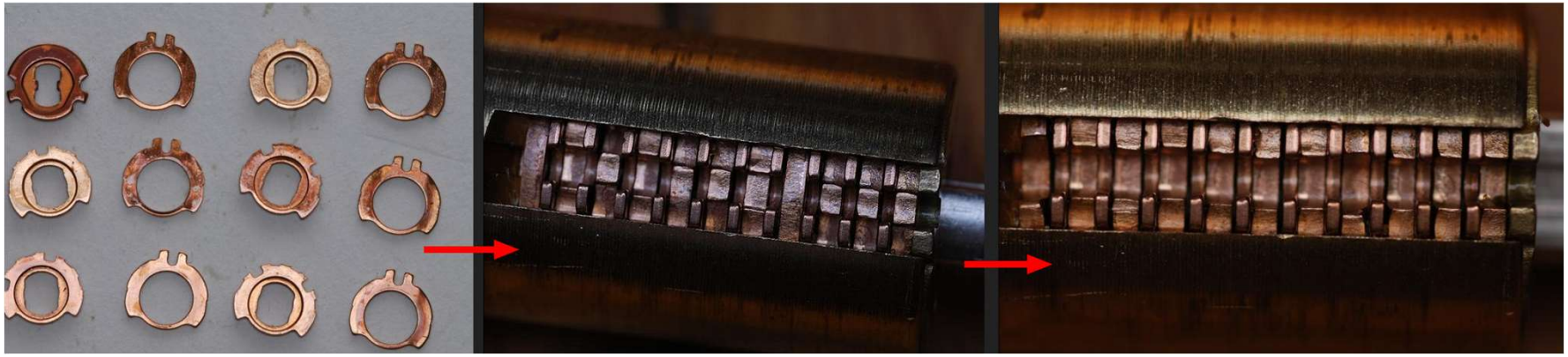
Disc Detainer

- Mostly found outside of the USA

Pros:
- Very difficult to pick
- Sturdy mechanism

Cons:
- More Expensive
- Less accessible





Wafer

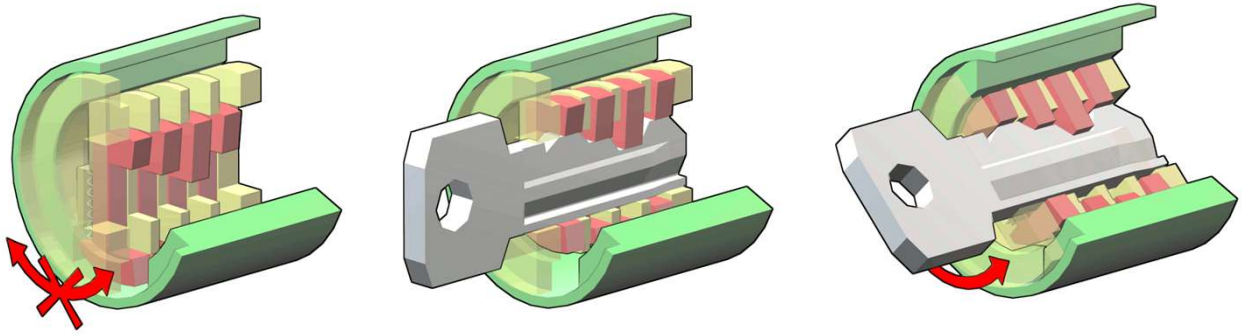
- Found in low security cabinets, desk drawers,
- and automobiles

Pros:

- Extremely cheap
- Crush-able wafers

Cons:

- Very easy to pick
- Simple -> Common keys



Modern Lock Design

Adding Layers of Security

Physical ⇔ Cyber


Crown
Jewels

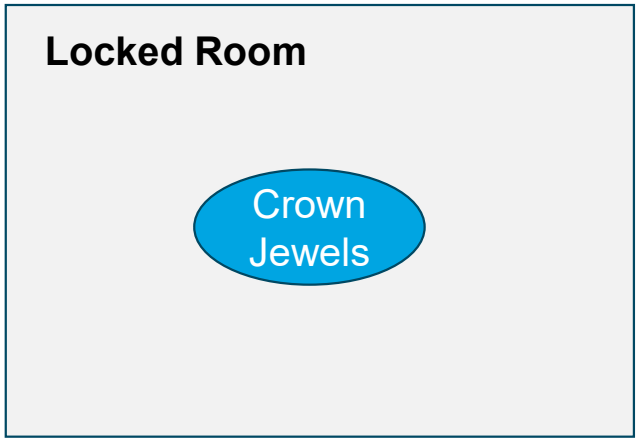
- Money / Valuable
- Sensitive information
  - Passwords
  - Financial data
  - PII
- SCADA

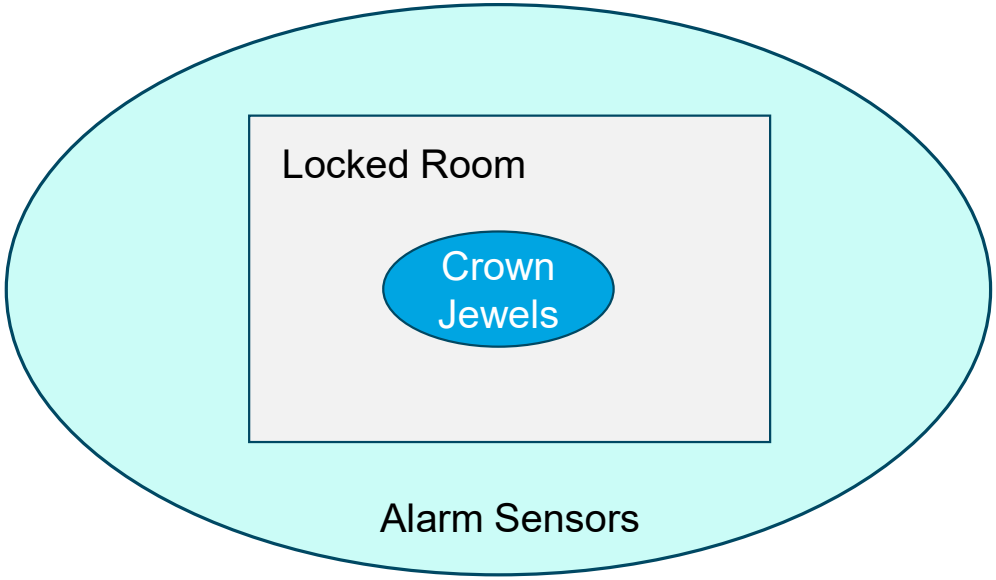
Crown Jewels

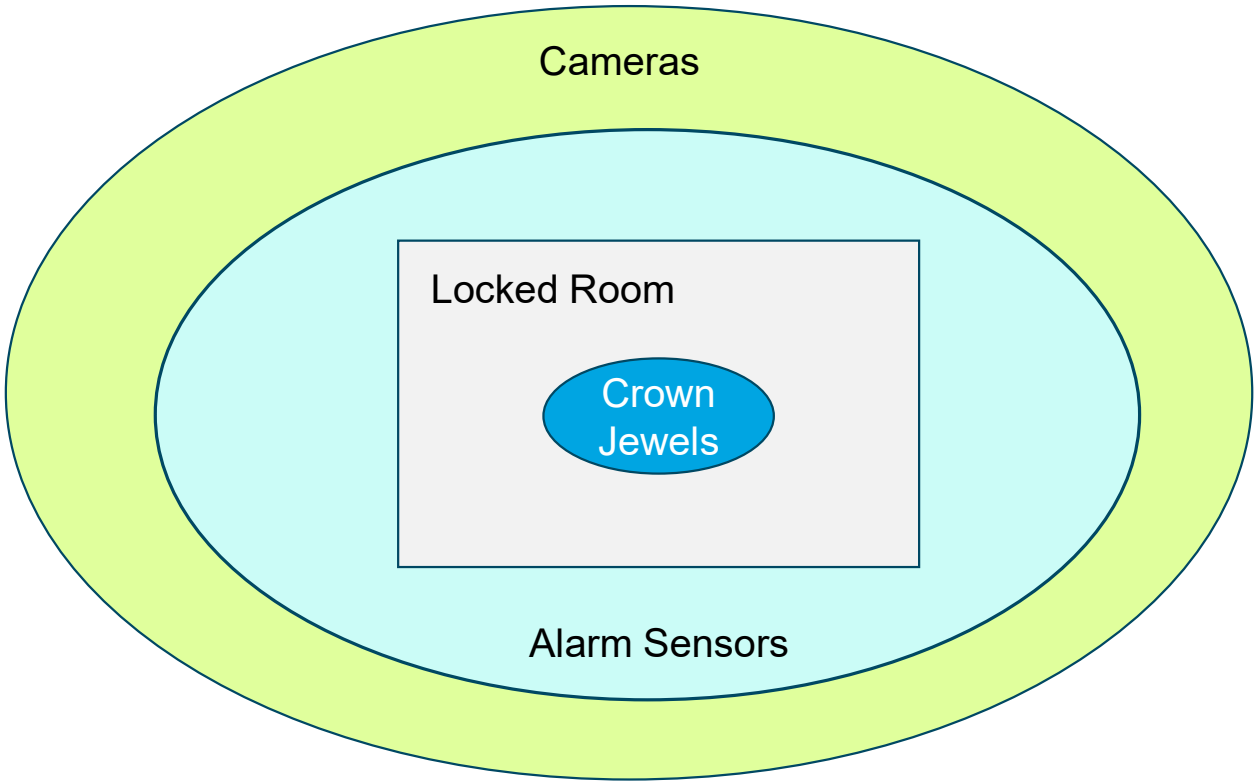
Power grid recloser

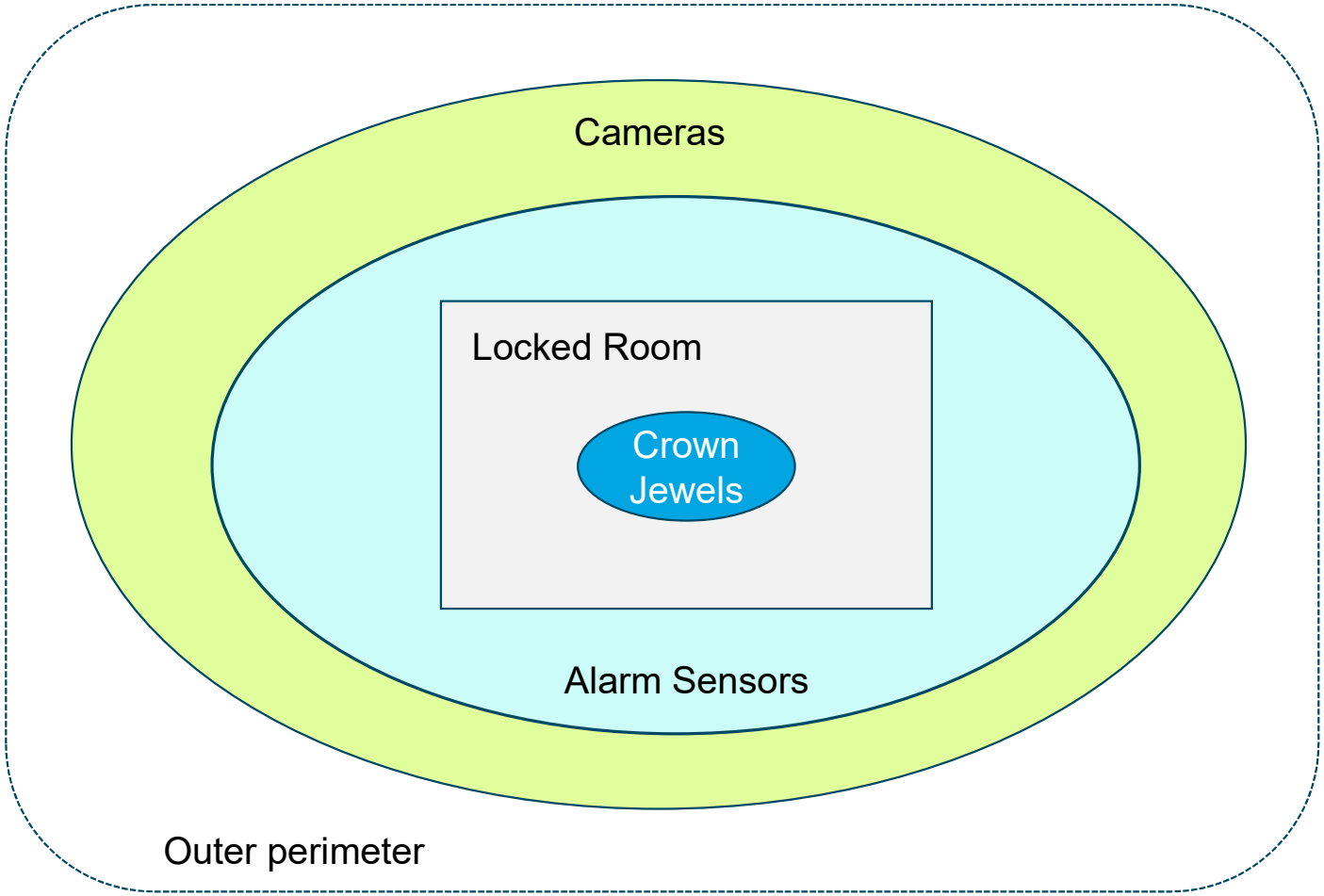
Microfilament Water Treatment

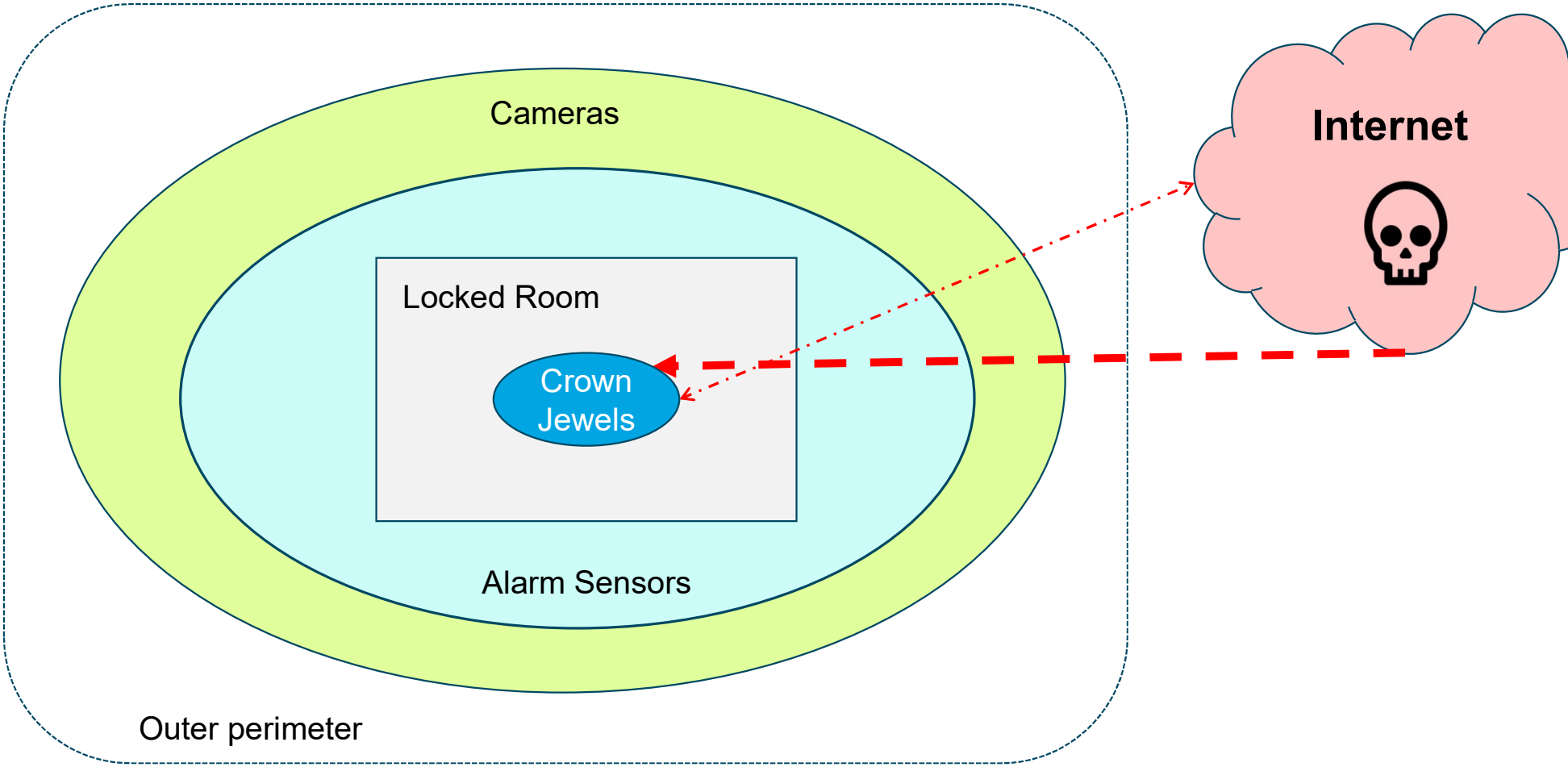

Crown
Jewels

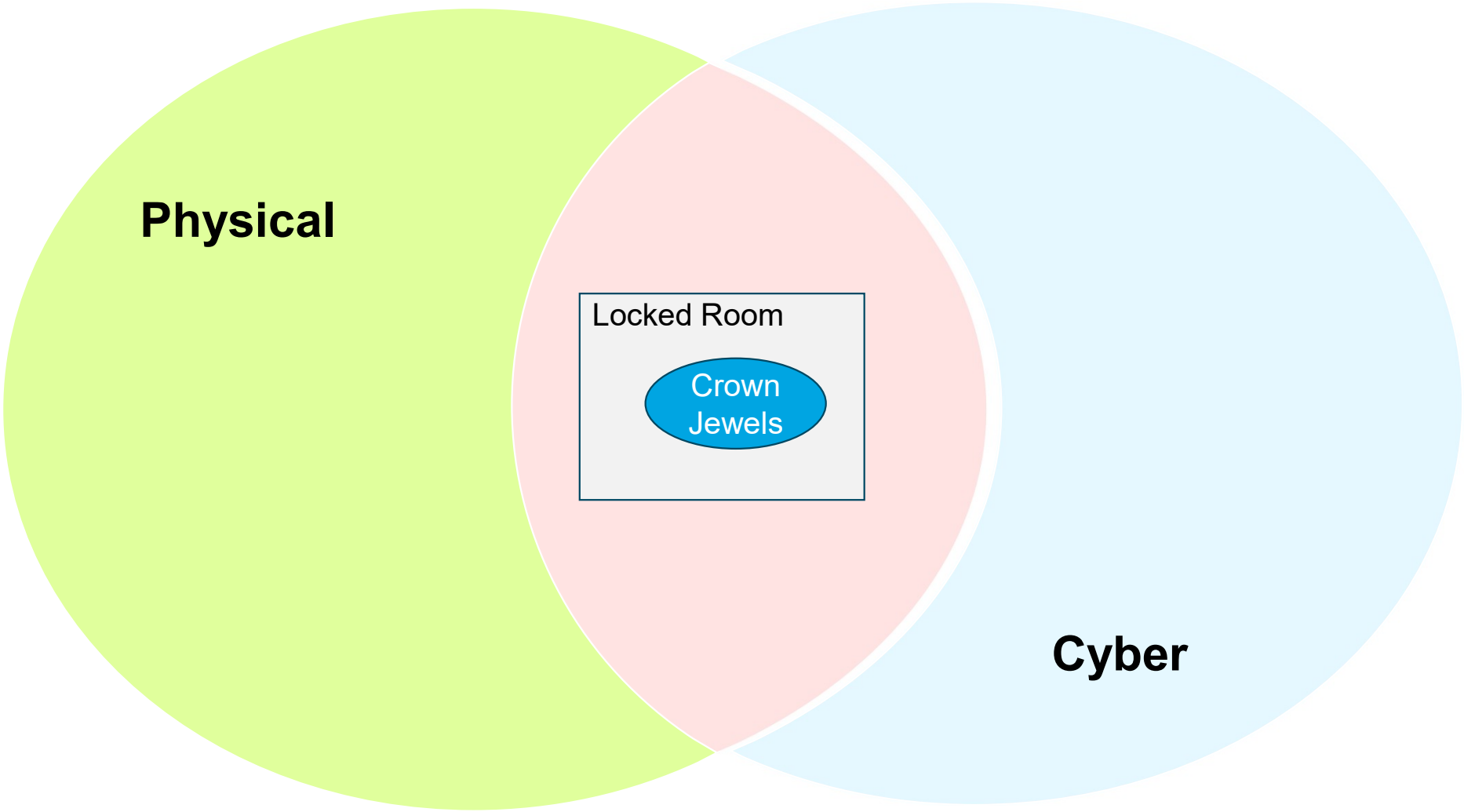

Locked Room
Crown Jewels

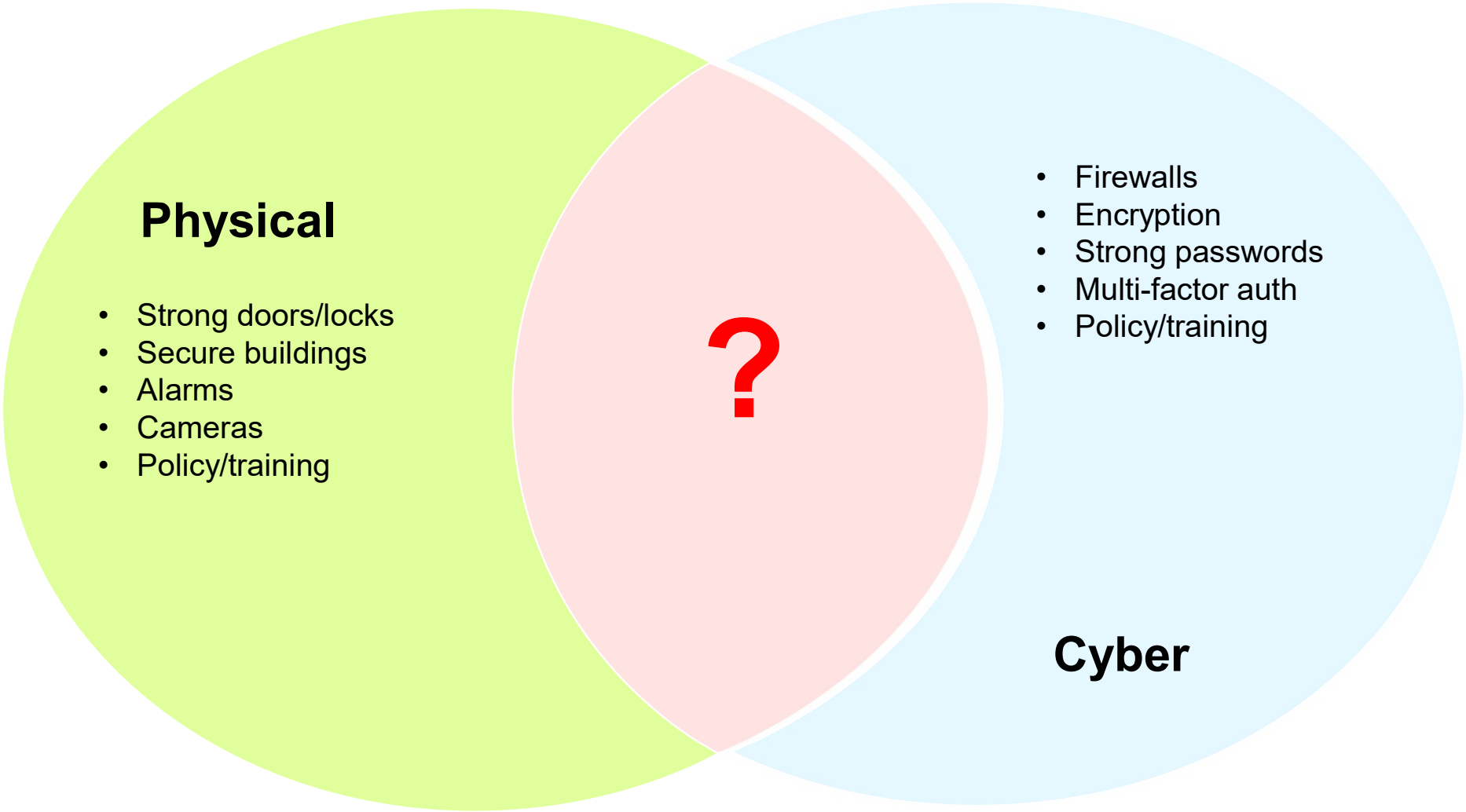

Locked Room
Crown Jewels
Alarm Sensors


Cameras
Locked Room
Crown Jewels
Alarm Sensors


Cameras
Locked Room
Crown Jewels
Alarm Sensors
Outer perimeter


Cameras
Internet
Locked Room
Crown Jewels
Alarm Sensors
Outer perimeter


Physical
Locked Room
Crown Jewels
Cyber


Physical
• Strong doors/locks
• Secure buildings
• Alarms
• Cameras
• Policy/training
?
• Firewalls
• Encryption
• Strong passwords
• Multi-factor auth
• Policy/training
Cyber

Physical

- Assume the vendor/third-party is meeting your security standards
- IT / OT Divide
- IT is unaware of changes in the real world
- OT is not informed about IT challenges
- Each side assumes the other will provide the necessary protections
- Unknown unknowns

?

Cyber

Poll 2 — Workstation Habits

"What do you do when you step away from your workstation?"

1. Lock it every time
2. It locks automatically
3. Lock it if I'll be gone a while
4. I rarely/never lock it
5. I didn't know I was supposed to lock it

What Are Your Publicly Accessible Areas?

Physical Proximity Network Access Vectors

- Live network ports in publicly accessible areas
  - Lobby ports
  - Kiosk ports
  - Printer ports
- Wireless peripherals
  - Human Interface Devices (HID)
- WiFi access points
  - Physically accessible and secured
  - Guest WiFi access
  - WiFi vulnerabilities
- Dumpsters, Shred Bins, Electronic Waste
- Community accessible conference rooms
- Vehicles and portable devices in the field ?

Live Network Ports Publicly Accessible

It is very hard to secure a publicly accessible network

Potential Solutions:

- Static IP addressing
- Sticky MACs
- Port Security
- Network Access Controls (NACs)
- 802.1x (PNAC) aka “EAP over LAN”

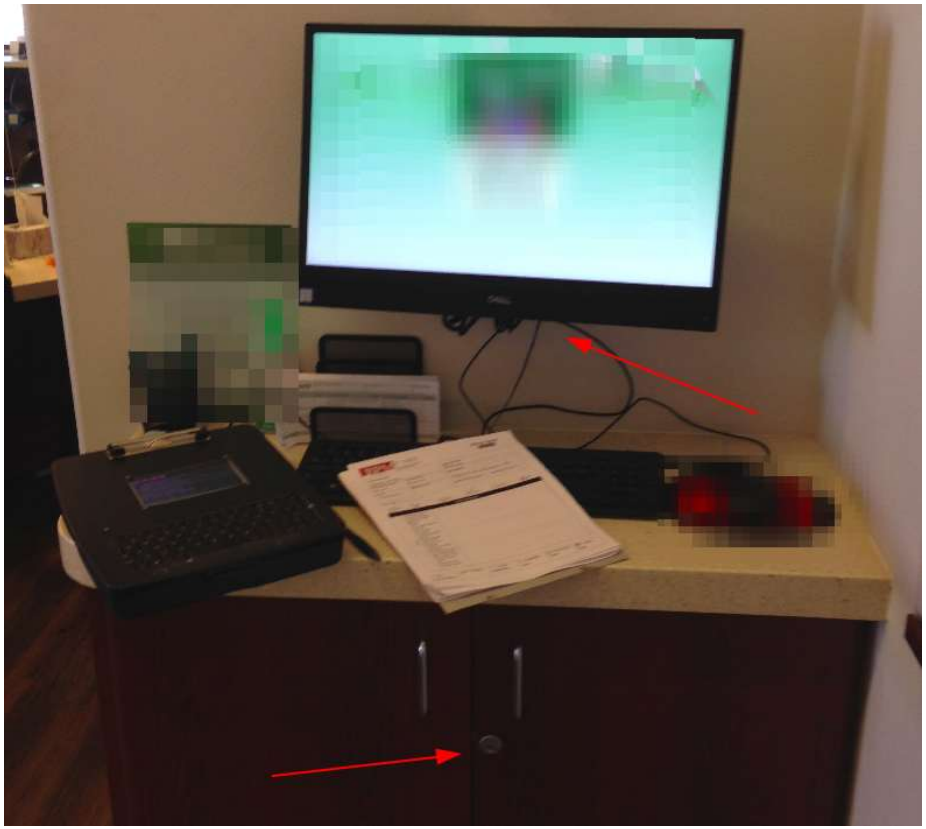
Example rogue host: Packet Squirrel

Image reference: https://cdn.shopify.com/s/files/1/0068/2142/products/Packet_Squirrel_800x.jpg?v=1508535547

Do Not Allow Physical Access to Network Ports

- Physically remove network ports
- Disconnect wires at the patch panel

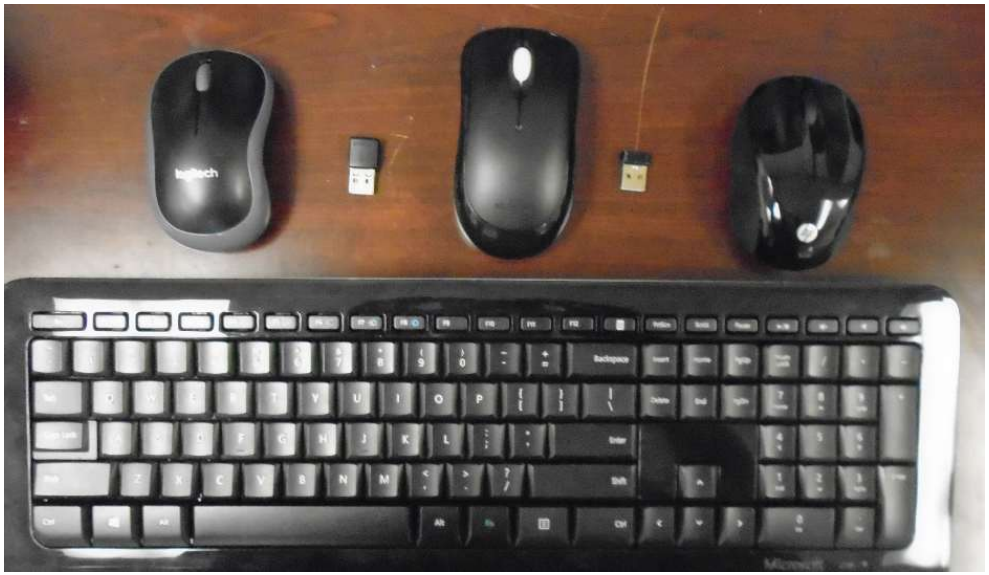
- Construct mechanisms to block physical access
  - Printers
  - Kiosks
  - Payment systems

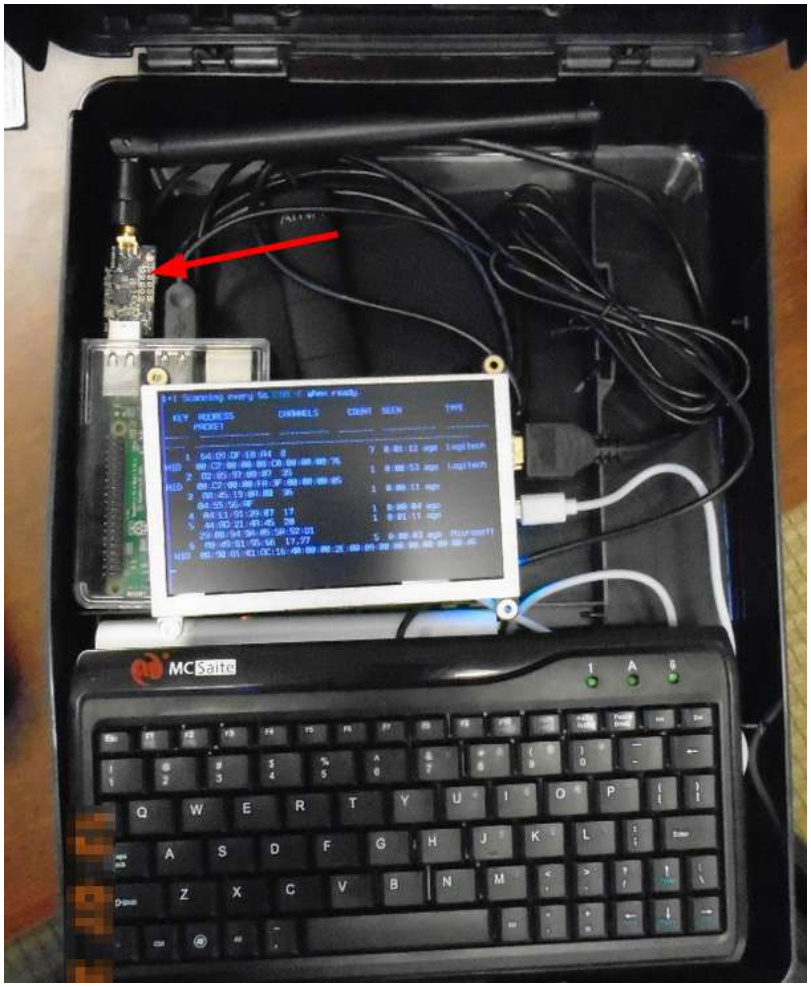


Wireless Peripherals

MouseJack Attack and the CrazyRadio PA

- Wireless keystroke injection
- Potential for long range attack 100 meters





WiFi Can Be Scary But Doesn’t Need to Sink The Ship

- The range of WiFi attacks can extend beyond a few hundred meters
- There are many WiFi vulnerabilities and attacks
- E.g. Printers enabling WiFi that are also connected to the internal network

- Critical Strategies:
- Physically secure WiFi access points
- Air-gap Guest WiFi networks to dedicated ISPs

Image reference: https://www.adsdigital.co.uk/blog/wireless-access-point-work

Remaining Public Access to Physical Assets

- **Dumpsters, Shred Bins, Electronic Waste**
  - Where does your data go to die?
- **Community accessible conference rooms**
  - Network access is typically a requirement
  - Unmonitored access to unknown persons
- **Vehicles and portable devices in the field**
  - Device encryption
  - Policy

Avoiding Humans: Physical Exploits

Physical Ingress

How can an attacker gain unauthorized access to secure locations?

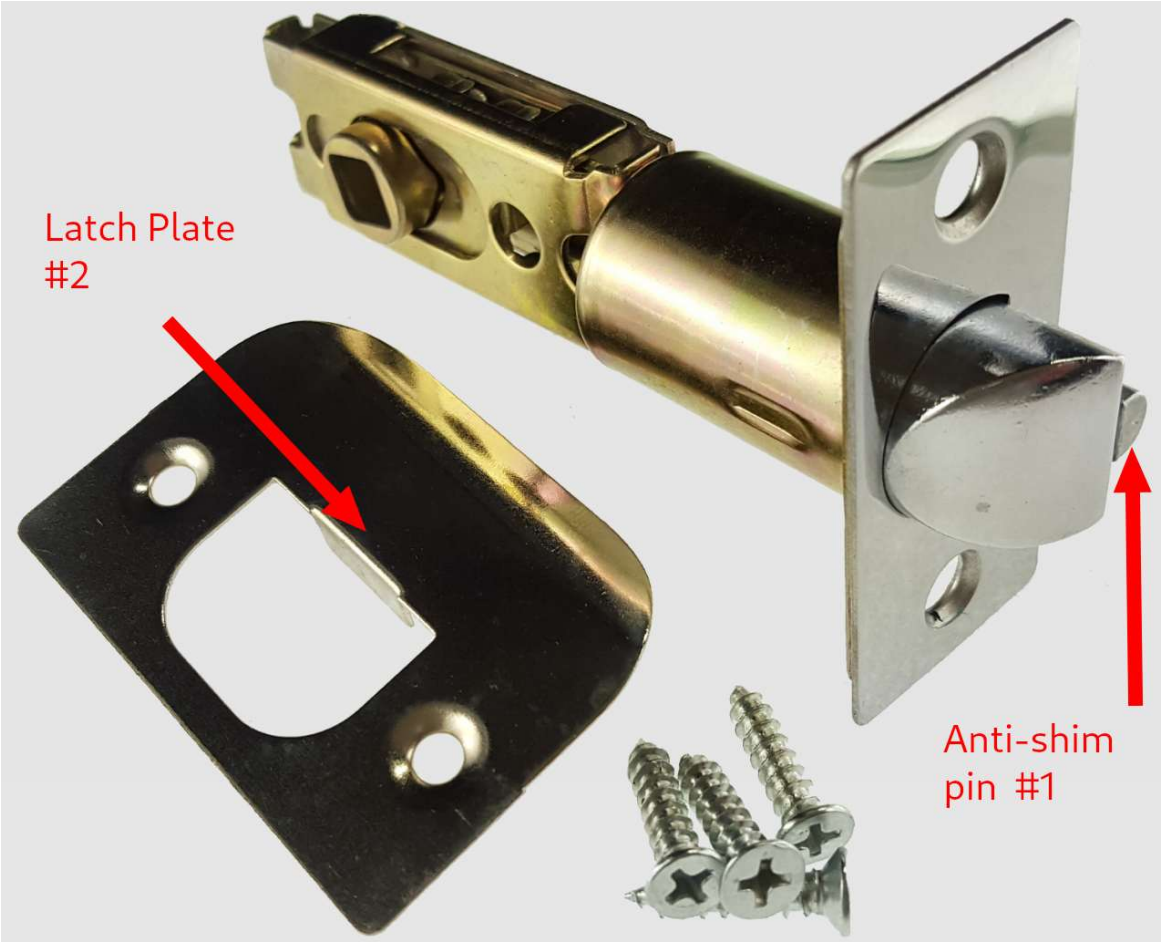
- Physical ingress is often obtained due to faulty door implementation
- Even new and expensive doors can be vulnerable
- The time to bypass a door/lock can be just a few seconds
- Doors and locks change with the weather, time, and use
- **Pro tip:** Examine doors and locks for new buildings during the construction phase!

Analogue Locks and Doors: Loiding

- An **anti-shim pin** is the primary mechanism that secures a lock latch from manipulation
- **Anti-shim pin failure is by far the most frequent vulnerability exploited when doors are physically bypassed**

Analogue Locks and Doors: Loiding … Continued

- **Anti-shim pin** failure is common:
- #1 has to sit perfectly on #2 and if the shim pin falls into the void, the lock can be easily bypassed
- Shim pins experience mechanical failure
- Doors can be moved (lean or push) to create shim pin vulnerabilities



https://www.topclasscarpentry.com/images/door-latches/adjustable-60-70-mm-backset-door-latch-polished-chrome.png

Shimming Doors

Even if the latch is not externally exposed, anti-shim pin failure can be exploited

Exploiting Motion Sensors

Double Doors: One example the J-Tool

The List Goes On ...

The list of door/lock vulnerabilities is endless, and an experienced assessor will continue to find new ways to defeat more doors/locks

- Under-the-door attack
- Shove-knife attacks
- Vulnerable hinges
- Removable door windows
- Pushing/leaning attacks
- Etc.

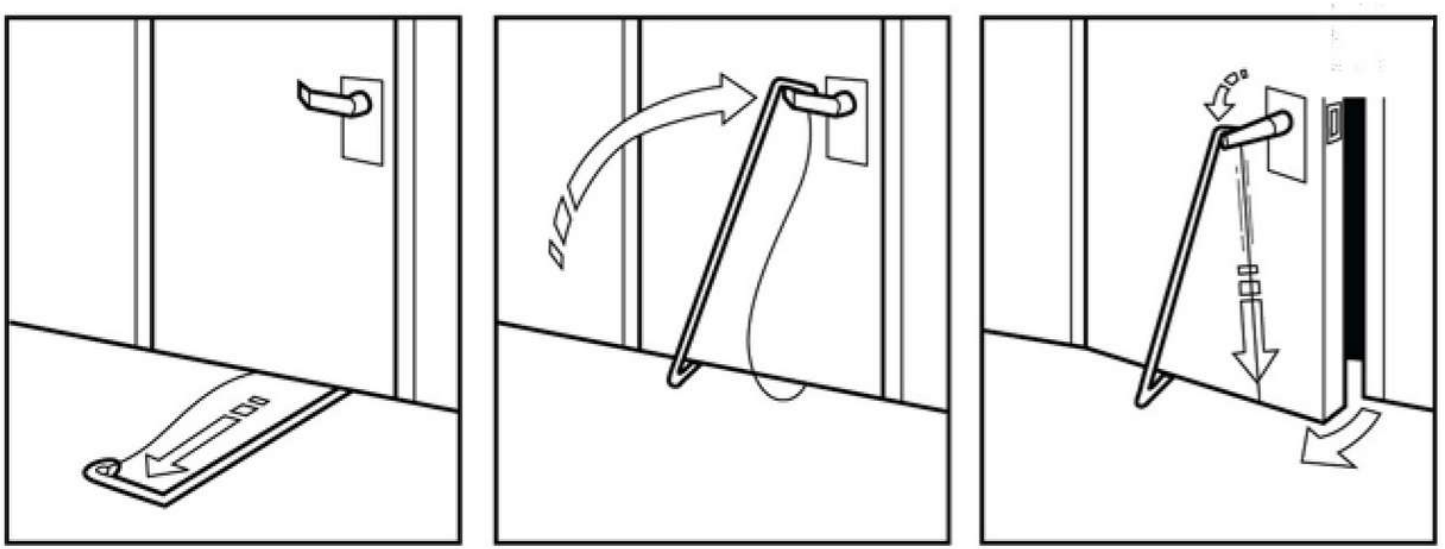


Image reference: http://www.hardcasesurvival.com/content/UndertheDoortool.jpg

Mortise Locks Rule!

Mortise locks *can potentially* provide a much more secure and durable door

1) The mortise style latch and anti-shim pin are superior in that the anti-shim pin sets on different plane that the latch

1) Dead-bolts work VERY well

2) Rounded door knob avoids under the door attacks

Image reference: https://www.grainger.com/product/YALE-Mortise-Lockset-1-34F869

Electronic Ingress

RFID badges are very common in modern facilities, but can be vulnerable to cloning attacks

```
33 bit card: 2255a800XX, FC = 42, CC = 13893652, BIN: 000000100010010101011010100000000000xxxxxxxxx
26 bit card: 20062cd8XX, FC = 22, CC = 27768, BIN: 00000010000000000110001011001101100001xxxxxxx
26 bit card: 20062cd8XX, FC = 22, CC = 27768, BIN:  00000010000000000110001011001101100001xxxxxxx
```

Cloning RFID Badges Can Be Easy or Not Currently Possible

- There are many types of RFID badges in use across the world
- North America tends to use a select few brands and types of badges
- The most common is HID Prox2, which is very easy to clone
- Cloning can occur “offline” in some cases allowing an attacker to read a badge covertly and then clone the badge later
- The myriad of types of badges can make selecting, and implementing an RFID badge system difficult
  - Example 1: Downgrade attacks
  - Example 2: iClass

Image reference: https://hackerwarehouse.com/product/icopy-xs/

Securing Electronic Ingress Vulnerabilities

Current secure RFID badge systems:

- iCLASS ER
- iCLASS SE (potentially)
- iCLASS SEOS (potentially)
- SHOWA
- SECURAKEY
- MIFARE DESFIRE

Additional remediation strategies:

- RFID badge dampeners
- RFID wallets
- Multi-factor authentication
  - Pin-code
  - Biometric
  - Physical key

Image reference: https://www.id-enhancements.com/hid-rk40-iclass-se-standard-profile-keypad-reader-terminal-strip-921ntnnek00000/

Poll 3 — Awareness Check

"Have you ever tailgated (or been tailgated) into a secured area without badging in?"

1. Yes, I've done it / seen it happen
2. No, never
3. I'm not sure what tailgating is

Let’s Get Malicious: In-person Social Engineering

An Unknown Person Presents With A Purpose

Lie, lie, and lie some more:

“My name is Ryan Ferran and I am here to perform ...

- “... a WiFi audit, checking signal levels”
- “… a server inventory”
- “… a network firmware upgrade”
- Something specific to the organization or current event
- The list goes on

Third-party Access

- Custodial services
- Shredding services
- Security services
  - Security guards can be the weakest link

- Vendors vs *Vendors*
  - SCADA and OT vendors
  - IT vendors

- **Strategies for Success**
  - Set rigorous contractual expectations
  - Build and test policies
  - Train employees
  - Remove access

How Do I Teach My Organization to Defend Against Social Engineering Attacks?

Build a set playbook for employees to follow when facing unknown persons

If an employee has a simple set of instructions to follow when they encounter an unknown person, the potential for social engineering *approaches* zero.

- Challenge unknown persons
- Escort unknown persons at all times
- Make a verification call to vet the reason for unknown person's visit
- Verify government issued identification
- Do not allow workstation access
- Do not provide credentials, keys, badges
- Rely on policies to inform employees of vendor access

Final Physical Security Considerations

What Is Left Out In the Open?

- Keys
- Badges
- Sensitive papers
- Unlocked unattended workstations
- Mobile devices

- **Keys left in fleet vehicles**

- Externally visible monitors
- Unlocked shred bins
- Unlocked server rooms, network closets, etc

Wrap Up

Securing the Physical World Takes Layers and Layers

- Physically secure your network
  - Disconnect wires
  - Securely lock up publicly accessible devices
- Train employees
  - And train them again
- Periodically review your physical world
  - Doors and locks shift/degrade over time
  - Implement layers, such as MFA, on doors protecting critical assets
- Monitor access to critical areas
  - Alarms
  - Cameras
- Build and test physical incident response plans
- Review your employee exit process and remove all physical / logical access

Takeaways

- Security is what you make of it even with zero budget
- Formal policies and procedures are the foundation of successful security controls
- Segmentation of the OT network is paramount
- Testing an OT network requires additional consideration and planning, but is essential in understanding, and mitigating, exploitable vulnerabilities
- The most successful OT penetration tests start with collaboration with stakeholders from IT and OT teams

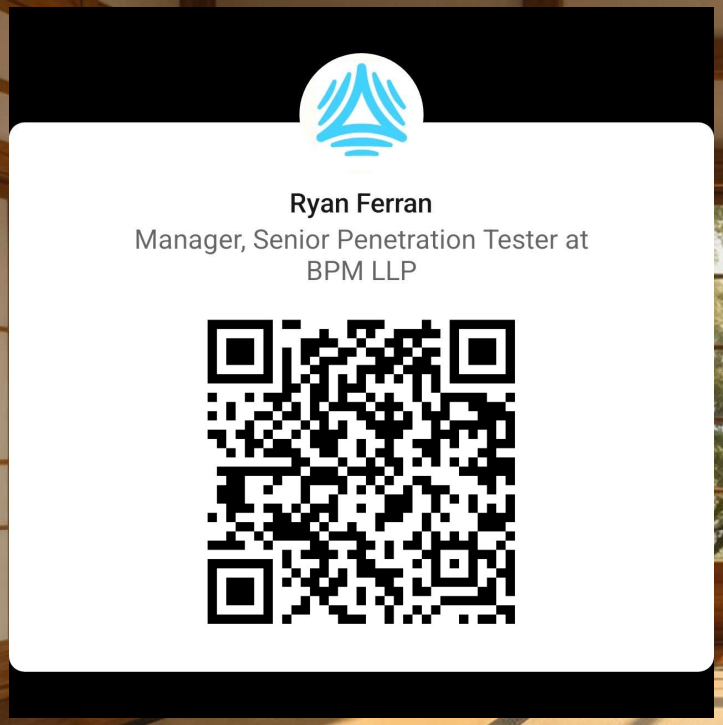
Closing Thoughts

- The threat landscape is changing, but so are the resources available as a result of CyberSecurity being on the forefront of national security
- The tooling and frameworks to support organizations enforcing least privilege have matured. Despite this high accessibility and maturity, organizations struggle with resources to implement meaningful improvement
- Even though threat actors are more sophisticated, employee action (as well as inaction) remains among the largest factors negatively impacting security
- The top issues impacting organizational security are not new, they are well understood but take resources and dedication to address

References

1. “NIST SP 800-115.” NIST. March 16, 2023. https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack“
2. “Hak5 Packet Squirrel.” May 9, 2023. https://shop.hak5.org/products/packet-squirrel
3. “Ukraine Power Grid Hack. Wikipedia. February 10, 2023. https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack
4. “A Hacker Tried to Poison a Florida City's Water Supply, Officials Say.” January 19, 2023. https://www.wired.com/story/oldsmar-florida-water-utility-hack/
5. Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions. McGraw Hill. Kyle Wilholt, Stephen Hilt. September 13, 2016
6. "Cost of a Data Breach Report 2021." IBM Security. August 5, 2021. https://www.ibm.com/downloads/cas/OJDVQGRY

WELCOME TO THE 11TH ANNUAL HACKING CONFERENCE



Ryan Ferran:
rferran@bpm.com

CPE Code:
Org = BPM
Code = johnny

The Institute of Internal Auditors Chicago

https://www.linkedin.com/in/ryan-ferran/

bpm

ISACA Chicago Chapter 50 YEARS