Lecture 38 – Physical Security

Ryan Cunningham
University of Illinois
ECE 422/CS 461 – Summer 2017
Security News

- Security executives leaving Uber
- US law proposed to jail executives for covering up data breaches
- Powerful new phishing tool “Mailsploit”
- Vendors starting to ship laptops with IME disabled
What Is Physical Security?

• Any physical object that creates a barrier to unauthorized access
• This includes: locks, latches, safes, alarms, guards, guard dogs, doors, windows, walls, ceilings, floors, fences, door strikes, door frames and door closers
Destructive vs. Nondestructive Entry

• Destructive entry
  – Involves using force to defeat physical security
  – Methods involve crowbars, bolt cutters and sledge hammers
  – Negative impact on IT resources is apparent
  – Remediation steps also obvious

• Nondestructive entry
  – Compromises security without leaving signs of a breach
  – Defeats intrusion detection
  – Greater and long-term threat
Is Physical Security An IT Concern?

• You have been working hard to secure your network from cyber attacks
  – Redundant layers of authentication, firewalls, and intrusion detection systems should protect against electronic methods of entry

• But what if an attacker gains access to the server room or network wiring closet ...
  – Is you network still safe?
Type of Threats to Physical Environment

- **Natural / Environmental**
  - Earthquakes, floods, storms, hurricanes, fires, snow/ice
  - Consequence of natural phenomena

- **Man made / Political Events**
  - Explosives, disgruntled employees, unauthorized access, employee errors, espionage, arson/fires, sabotage, hazardous/toxic spills, chemical contamination, malicious code, vandalism and theft
  - Acts of commission or omission
Lessons-Learned for U.S.

- Major Domestic Events:
  - 2005 Hurricane Katrina (1,836)
  - 1995 Federal Office Building, Oklahoma City (168)

- Major International Events:
  - 1998 U.S. Embassy, Kenya (237)
  - 1983 Beirut Barracks, Lebanon (309)
Categories of Security Controls

• **Management (Administrative) Controls**
  – Policies, Standards, Processes, Procedures, & Guidelines
    • Administrative Entities: Executive-Level, Mid.-Level Management

• **Physical Controls**
  – Physical Security (Facility or Infrastructure Protection)
    • Locks, Doors, Walls, Fence, Curtain, etc.
    • Service Providers: FSO, Security Guards, Dogs

• **Technical (Logical) Controls**
    • CCTV & Camera, IDS, Moisture detection system, Fire/Smoke detection system, Fire suppression, Environmental control system, UPS, etc.
    • Service Providers: Building Architect, Critical Infrastructure Protection (CIP) Engineer, Operations Center.
Strategic Approach to Physical Security

Source: Global Crossing website
Physical Controls – Facility Construction

- **Structured barriers:** Perimeter structure
- **Walls & Fencing**
  - Specific gauge and fabrication specifications (e.g. No. 11 gauge galvanized chain-link fencing material.)
  - Specify height, or need for “top guard” (e.g. 8-ft in height, 6-in. under ground with top guard.)

<table>
<thead>
<tr>
<th>Height</th>
<th>Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 meter / 3 – 4 ft</td>
<td>Deters casual trespassers</td>
</tr>
<tr>
<td>2 meter / 6 – 7 ft</td>
<td>Too high to climb easily</td>
</tr>
<tr>
<td>2.4 meter / 8 ft with top guard</td>
<td>Deters determined intruder</td>
</tr>
</tbody>
</table>

*Source: Official (ISC)² Guide to The CISSP Exam*
Physical Controls – Facility Construction

• Structured barriers: Entry points
  – Gates, bollards, roadways.
  – Doors, windows, ventilation airways, manhole covers, etc.
  – Department of State and DoD Anti-Ram Vehicle Barrier Certification Criteria (SD-STD-02.01):

<table>
<thead>
<tr>
<th>Speed Rating</th>
<th>Speed at Impact</th>
<th>Penetration Rating</th>
<th>Penetration Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>K4</td>
<td>30 mph</td>
<td>L3</td>
<td>&lt; 3 ft</td>
</tr>
<tr>
<td>K8</td>
<td>40 mph</td>
<td>L2</td>
<td>3 – 20 ft</td>
</tr>
<tr>
<td>K12</td>
<td>50 mph</td>
<td>L1</td>
<td>20 – 50 ft</td>
</tr>
</tbody>
</table>

Vehicle Weight: 15,000 lb.

Technical Controls – Entrance Protection

Entry access control systems

• **Turnstiles**
  – Revolving doors that can be activated to “lock” and not allow unauthorized individuals to enter or leave facility
  – To prevent “piggybacking”.

• **Mantraps**
  – Routing people through two stationary doorways

• **Fail-safe**
  – Door defaults to being **unlocked**.

• **Fail-secure**
  – Door defaults to being **locked**.
Technical Controls

Entry access control systems – |

• **Mechanical** locks:
  – Key
  – Combination locks
  – Magnetic locks

• **Electronic** locks:
  – Combination lock
  – Proximity / RFID badge
  – Bio-metric
How to evade?

• Just like any other attack:
  1. Understand how the system works
  2. Find the weakest link
  3. Look for design assumptions
Locks and Keys
Legal Notice

• Laws regarding lock picking vary significantly state-by-state
• In most states purchase and possession of dedicated lock picking tools is legal
  – Penalties are raised significantly if you get caught using them in the commission of a crime

Public domain image from http://commons.wikimedia.org/wiki/File:Madame_Restell_in_jail.jpg
http://toool.us/laws.html
Lock Picking in Movies

• Genuine lock picking in movies used to be prohibited
• Before 1967, the Hays code (Motion Picture Production Code) required censorship of Hollywood movies
  – “All detailed (that is, imitable) depiction of crime must be removed, such as lock picking or mixing of chemicals to make explosives”

Public domain image from http://commons.wikimedia.org/wiki/File:Motion_Picture_Production_Code.gif
Pin Tumbler Lock
\[ 8^7 = 2,097,152 \]
Compromising Locks

• For centuries, the lock has been one of the cornerstones of physical security
  – We rely on dozens of them every day to protect people and assets

• The trust most people place in locks is unwarranted
  – Most locks can be easily compromised with nondestructive methods
  – Sometimes within seconds and with readily available tools

• “Locks keep honest people honest”
Feeler Picking

- Apply light tension
- Lift one pin at a time
  - Identify binding pin
- Lift binding pin until it reaches the shear line
- Setting the binding pin will rotate the lock slightly
- Find next pin and repeat the process
Scrubbing / Raking

• Apply light tension
• Work over pins back to front in a circular motion
  – attempting to pop them into the shear line with the combination of tension
• Good for beginners
• Usually employ snake pick or half diamond

Photo by Jennie Rogers included with permission.
Bump Keys

• Driver pins “jump” higher than the cylinder just for an instant
• If a light rotational force is applied, the cylinder will turn
• Lock bumping is a very fast method for opening the lock
• The lock is not damaged
• Defense: different weighted pins

Photo by Jennie Rogers included with permission.
How many of you have your keys sitting out?
Copy your house keys with your phone

No time for the hardware store? Get your keys delivered to you

Get Started
ACCUVOTE-TS

The votes are in and Diebold supplies take the lead for accuracy and simplicity of use with this dependable touch-screen technology. //

Replacement Access Keys
+ 2 keys that allow easy service access to the Tally Printer and replacement battery compartment

GS-567311-1000 $5.90 USD per set
$6.90 CAD per set

Enter a quantity

add to your order

ORDER BY PHONE 800.769.3246
Why is physical security an IT concern?
physical access == total access?
What about Encryption?
Proximity
Signal Emissions

• Computer screens emit radio frequencies that can be used to detect what is being displayed.

• Visible light reflections can also be used to reconstruct a display from its reflection on a wall, coffee mug, or eyeglasses.

• Both of these require the attacker to have a receiver close enough to detect the signal.
Faraday Cages

• To block electromagnetic emanations in the air, we can surround sensitive equipment with metallic conductive shielding or a mesh of such material, where the holes in the mesh are smaller than the wavelengths of the electromagnetic radiation we wish to block.

• Such an enclosure is known as a Faraday cage.
Acoustic Emissions

- Dmitri Asonov and Rakesh Agrawal published a paper in 2004 detailing how an attacker could use an audio recording of a user typing on a keyboard to reconstruct what was typed.
Electromagnetic Radiation from Video Display Units: An Eavesdropping Risk?

Wim van Eck
PIT Dr. Niker Laboratories, 5. Paulstraat 4, 2641 XI
Leiden, The Netherlands

This paper describes the results of research into the possibility of eavesdropping on video display units. By picking up and decoding the electromagnetic interference produced by the display, the eavesdropper can obtain information that would otherwise be impossible to obtain. During the research project, the video output of a display was monitored. It became more and more clear that this type of equipment can be eavesdropped upon, even by an unaware eavesdropper. The research has implications for the security of electronic communication systems.
High speed video
(actual video playing here)