Physical Security: An Overview from Deadbolts to Deathtraps

By: Cody L. Hofstetter
Disclaimer

• This presentation is for educational purposes only.

• I am not a lawyer even if I sound like one. Seek legal advice from someone who is.
Overview

• Introduction
• Basic Security
• Breaking/Fixing Basic Security
• RFID
• Closing Points to Remember
About Cody Hofstetter

From Software Pirate to Freedom Advocate
Death of the Dino
Explicitly NOT covered by the CC-BY-SA in this presentation:

- All logos, trademarks, taglines, et al associated with any company.
Red Eye Audience Participation
How Basic Locks Work
How Basic Locks Work
How Basic Locks Work

Opening With a Key
How Basic Locks Work

Opening *Without a Key*
Deadbolts
Deadbolts
Deadbolts
Fail-Safe Vs Fail-Secure

- **Fail-Safe (aka Fail-Open)**
  - A device will not endanger lives or property when it fails

- **Fail-Secure (aka Fail-Closed)**
  - Access or data will not enter an adversary’s hands in a failure
Fail-Safe Vs Fail-Secure

E.g. a building catches fire
- Fail-Safe systems unlock doors to allow firefighters and quick escape
- Fail-Secure systems lock doors to prevent unauthorized access
Dead Latch
Strike Plate
Dead Latch Engaging
Lockpicking

• Not at all how it happens in the movies
• **NOT** illegal to own tools or practice
• A single lock can take anywhere from seconds to hours depending upon its complexity (visit TOOOL)
• Any real engagement will likely involve the use of bypass tools
Lockpicking

• Bypass tools:
  - Bump keys
  - Snap gun
  - Crash bar
  - Mouth

D.D.T

Odds are if you don't know what this is .... you shouldn't have one
Hinge Removal
Jamb Pins

MAJOR MFG.

JAMM PINS FOR RESIDENTIAL DOORS

⭐⭐⭐⭐⭐

3

product reviews

YOUR PRICE:

$3.95

SKU:

MS-JP-10

SHIPPING:
Calculated at checkout

CURRENT STOCK:
Out of stock

SCI
Jamb Pins
Crash Bars
Request to Exit
Modern Door Handles
Under Door Attacks
Under Door Prevention

Under Door Attack Prevention — Security Door Bottom

Under Door Attack Prevention — Blocking Clips
Padlocks
Padlocks
Padlock Shims
Padlock Shims - DIY
Padlocks
Padlock Shims - DIY

• Do NOT practice on locks you depend on
• Do NOT practice on locks you can’t open
• Your shims WILL break. If you cannot open it, you may render the lock inoperable
High Security Padlocks

• Use techniques that make shimming impossible
• Most common is ball bearings instead of spring loaded catch
• Indentation on shackle is round instead of wedge-shaped
Electronic Credentials

Attacking Electronic Credentials
Proxmark 3
Proxmark 3

• Open Source Design
• Operates in:
  – Low Frequency (LF) 125KHz
  – High Frequency (HF) 13.56MHz
• Reader AND Tag
Garage Openers

• Started as simple transmitter and receiver design (but opened neighbors as well)
• Second iteration used approx 4,096 codes
  – Small enough that unsophisticated attackers could go through a neighborhood and check
Garage Openers

• Iteration 2.5
  – Remotes preprogrammed to roughly 3.5 billion unique codes

• Third iteration uses frequency spectrum between 300-400MHz and rolling code (code hopping)
  – Also transmits a unique identifier for the remote control, sequence number, and sometimes an encrypted message
Garage Openers

• Standards used by Chamberlain, LiftMaster, and Craftsman

<table>
<thead>
<tr>
<th>Dates</th>
<th>System</th>
</tr>
</thead>
<tbody>
<tr>
<td>1984-1993</td>
<td>8-12 DIP switch on 300-400 MHz</td>
</tr>
<tr>
<td>1993-1997</td>
<td>Billion Code on 390 MHz</td>
</tr>
<tr>
<td>1997-2005</td>
<td>Security+ (rolling code) on 390 MHz</td>
</tr>
<tr>
<td>2005-present</td>
<td>Security+ (rolling code) on 315 MHz</td>
</tr>
<tr>
<td>2011-present</td>
<td>Security+ 2.0 (rolling code) on 310, 315, and 390 MHz</td>
</tr>
</tbody>
</table>
Car Security

• First remote keyless system introduced on...

• 1984 Renault Fuego
Car Security

• Smart Key
  – Introduced by Mercedes-Benz as "Key-less Go" in 1998 on W220 S-Class

• Vulnerable to “Replay” attacks
Hacker Tools

- HackRF One - $300
- UberTooth One - $120
- Raspberry Pi 3 B+ - $35
- Kali Linux - $0
Faraday Cage

- Enclosure used to prevent electromagnetic fields
- Formed by a continuous (or mesh) conductive material
- External field causes electric charges within the conducting material to be distributed, canceling the field's effect in the cage's interior (and vice versa)
Faraday Bags

- Used by Law Enforcement to prevent signals (such as dead man switches) from reaching a device (i.e. a remote wipe)
CIA Op-Sec Fail

- Italy convicts 23 Americans for 2003 CIA rendition (practice of abducting and transferring individuals to third countries for detention and “interrogation”)
- UN considers these as “crimes against humanity”
- Metadata examination revealed relationship between multiple operatives
CIA Op-Sec Fail

- How was the relationship established?
- Operatives were supposed to use lined bags to prevent cell signals when not in use.
Signal

- Wickr/Telegram/WhatsApp
- Secure Messaging App
- Encrypted communications (end to end and perfect forward secrecy)
- Disappearing messages
Want to hire me?

- Pentest your organization
- Give talks
- Teach how to enhance your privacy
- Train your staff to make your company more secure
Thank you

Closing points to remember:

Just because you’re paranoid doesn’t mean they aren’t after you

Use FOSS & tell everybody

Email:

Slides@SovereignCyberIndustries.com