Physical Security for Infosec Pros
(Breaking and Entering 101)

Bobby Kuzma
Security Researcher and Evangelist

November 15, 2017
About this talk

This talk is:
- An entry level discussion of physical security

This talk is not:
- How to pick locks
- How to break into places without permission
- Approved by Marketing
Hi! I’m Bobby.
Hi! I’m Bobby.

Please say “Hi Bobby”
A couple of things to start with

Disclaimer

- This presentation does not represent the views of Core Security
- Do not attempt any of the bypass techniques anywhere you do not own, or have written permission in advance.
A couple of things to start with

Seriously, don’t do it.
If I can touch it, it’s not your computer/network anymore.
Physical Security Matters

Ahem..
Can you spot the RasPi with the cell modem?

Wiring closet at Fenway Park during a game, Boston. Photo Credit: Rayanne Buchianico
The Traditional Security Triad

Confidentiality

Availability

Integrity
Confidentiality
DEPARTMENT OF HOMELAND SECURITY
KOBACH STRATEGIC PLAN FOR FIRST 365 DAYS

1. Bar the Entry of Potential Terrorists

1. Update and reintroduce the NSFERS screening and tracking system (National Security Entry-Exit Registration System) that was in place from 2002-2005. All aliens from high-risk areas are tracked.
2. Add extreme vetting questions for high-risk aliens: question them regarding support for Sharia law, jihad, equality of men and women, the United States Constitution.

Record Number of Criminal Aliens in the First Year

3. 193,000 criminal removal cases dropped by the Obama Administration.
4. All ICE guidance memoranda adopted by Obama Administration; issue new guidance defining "criminal alien" as any alien arrested for any crime, and any gang member.
5. Repatriate their citizens who have committed crimes in the United States.
6. Increased 287(g) agreements with at least 70 cities and counties to enlist state and local criminal law enforcement agencies.

Security

7. Security at the border is increased in addition to the 386 miles of existing actual wall within Arizona. Have entire 1,989 miles planned for rapid build.
8. Use the PATRIOT Act to prevent illegal aliens from entering the country.
Integrity
Incoming MIT President finds his office does not exist.
October 15, 1990
What does Physical Security do?

Attempt to control access to a restricted area
What does Physical Security do?

Buy time for detection or response
Physical Security’s 5 D’s

- Deter
- Detect
- Deny
- Delay
- Defend
Notice that there’s nothing about STOPPING attackers
Fences
Fences

Story time!
Guards

- Provide real-time response
- Able to improvise
- Expensive
- They get bored
Cameras

Focused on Entry and Egress Points

Rarely monitored in real time

Cost of recording retention
IP Cameras

If you can get access to the Ethernet line, check out Looping Surveillance Cameras through Live Editing from DEFCON 23
Door open/close sensors
Operate on magnetic fields
Motion Sensors

Some use Ultrasound

Some use Infrared

They can be tuned to increase or decrease sensitivity
Motion Sensors

Degrades the sensitivity of sensors

Requires prior placement
Lasers Again

Don’t use too much
Motion Sensors

Used for Exit

Check for door gaps
Fun with doors
Keys are bad
Picks
Guns
Bump Keys
Destructive bits

Do not try this at home, work, school, or really anywhere.
Strikes
Guards and Blocks
The most versatile bypass tools
The most versatile bypass tools
Proximity Cards
Prox Cards

“Short” range RFID

Authentication, but not authorization

Trivial to clone
Biometrics
Cloning fingerprints
Electronic locks
Electronic locks

- Default codes… sometimes
- People reuse codes
- When in doubt…
Turnstiles and Mantraps
Cargo and freight have to come in somehow.

Find it.
Elevators
LAFD REQUIREMENT #75: KEY ACCESS BOX STANDARD

FIRE PREVENTION & PUBLIC SAFETY BUREAU
Universal Fire Service Key Set

Brand: ElevatorKeys.com
Product Code: KSUF516
Availability: 2 - 3 Days

$124.95
Fire Codes are your friend

- All buildings must comply
- Exit doors must be operable
- Bitings for fire service keys may be specified
- Or Knox Boxes

Note: Don’t post pictures of your keys online.

← New Berlin, Wisconsin Knox Box key
Social Engineering and OSINT

Receptionists are your friend. Until they aren’t.
Collect OSint for SE

- LinkedIn to mine employees
- Link to “personal” social profiles
- Look for ID badges and keys
Acting like you belong

Service Provider Uniforms = Invisible
Alarm Systems

Can be spoofed and disrupted

Multiple false alarms in a night = Disabled

Cellular connected systems can be jammed or MitM’d with an IMEI catcher
Let’s keep this going!

bkuzma@coresecurity.com
@BobbyAtCore
https://www.linkedin.com/in/bobbykuzma