



# 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

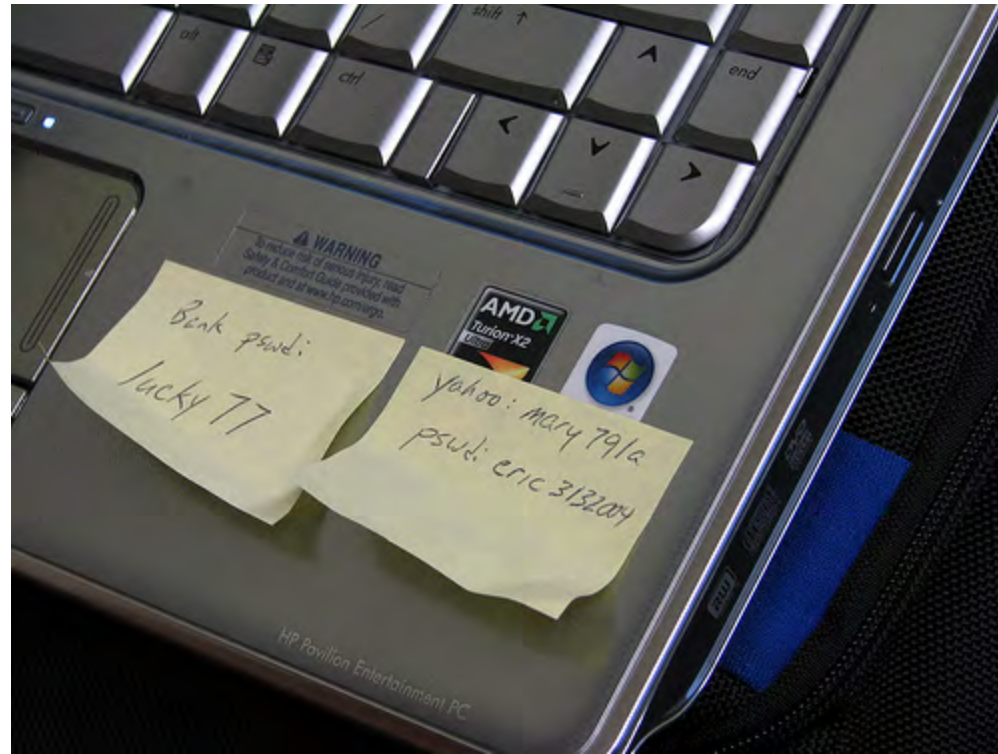
Seriously, don't do  
it.

The background is a dark blue gradient with a faint, abstract network of white lines and dots, resembling a molecular structure or a data network. The text is centered in a bold, white, sans-serif font.

**If I can touch it, it's not your  
computer/network anymore.**

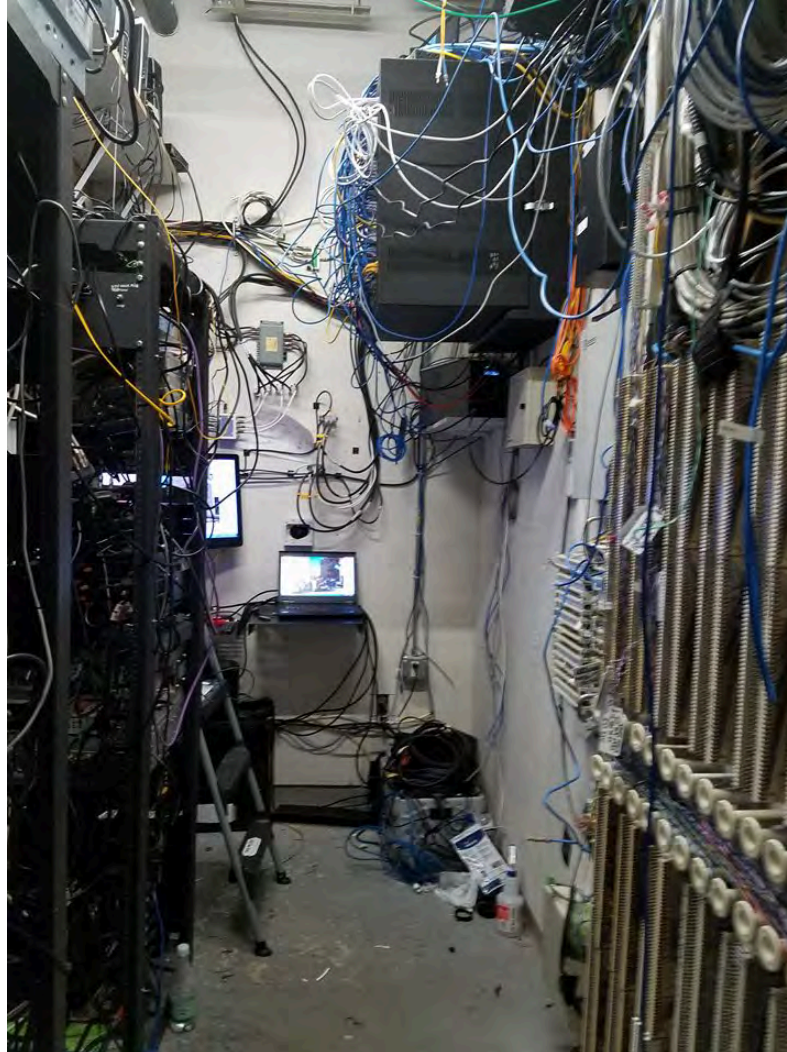
# Physical Security Matters

Ahem..



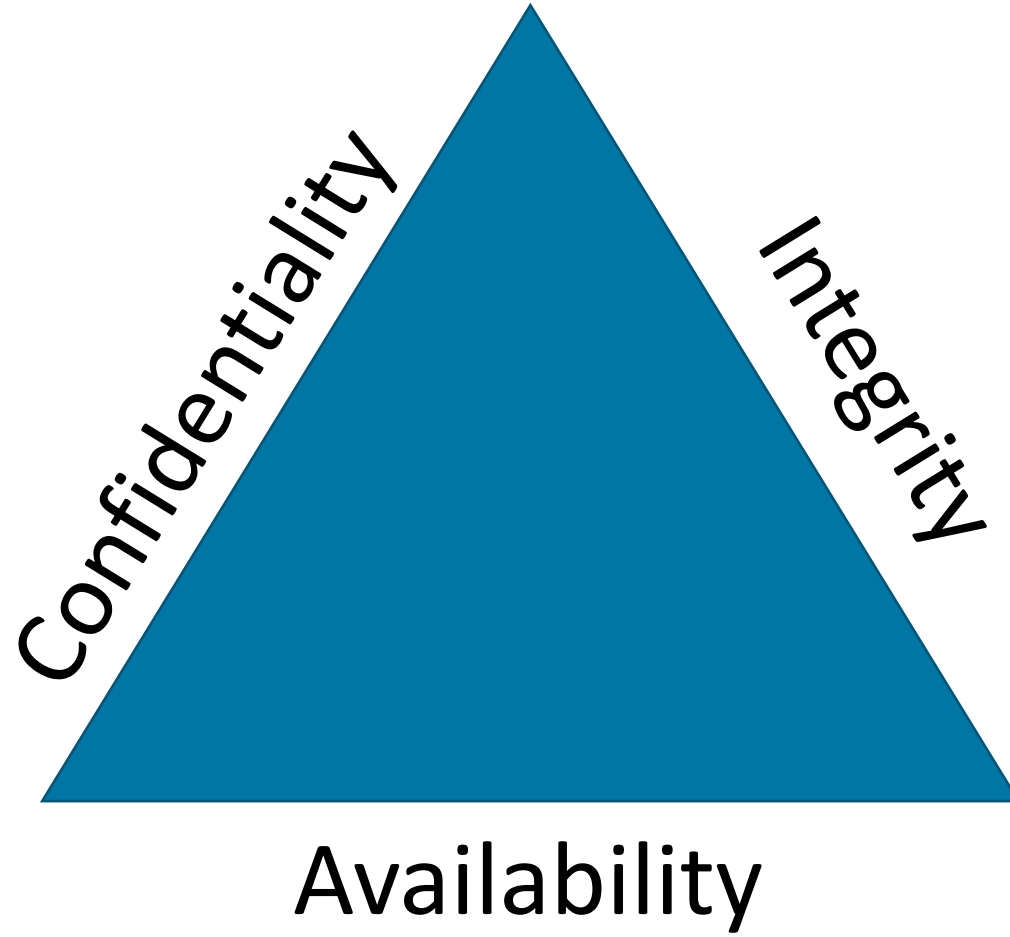


# Can you spot the RasPi with the cell modem?

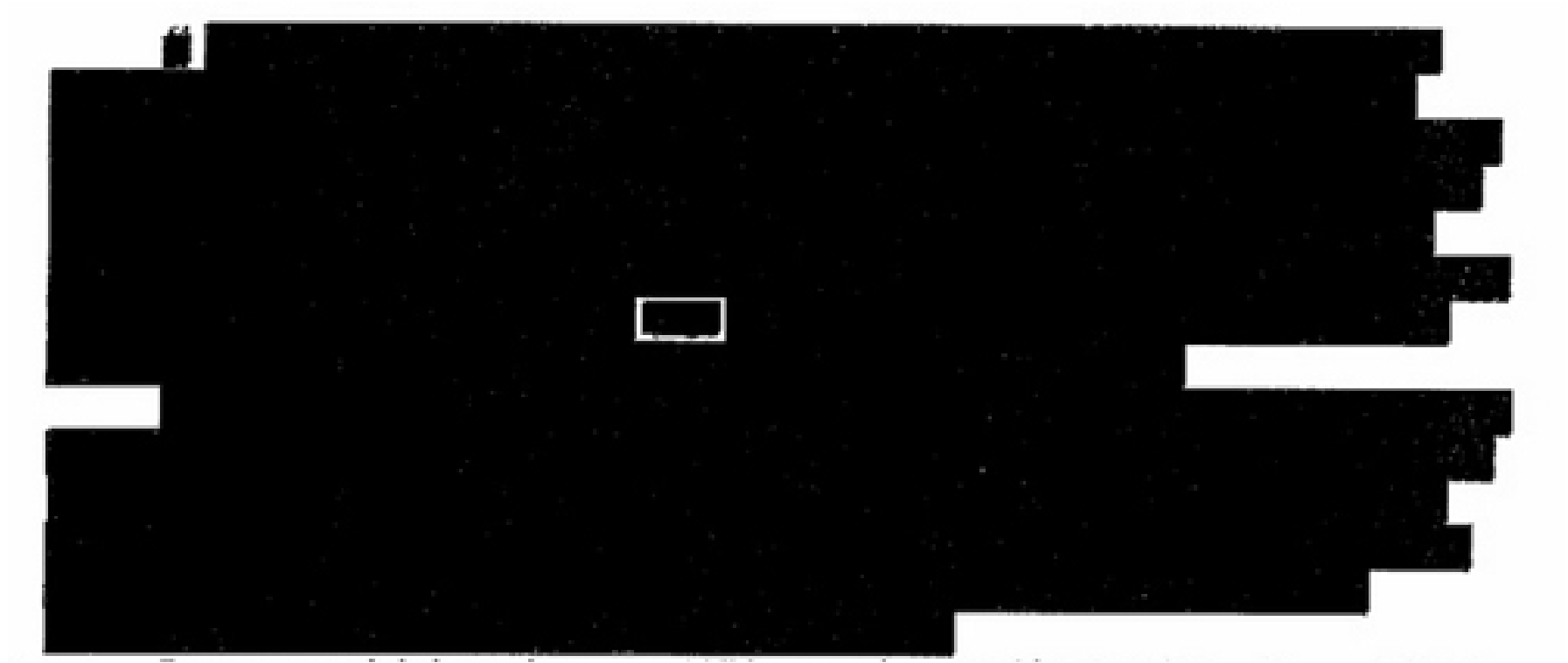


Wiring closet at Fenway Park during a game, Boston. Photo Credit: Rayanne Buchianico

# The Traditional Security Triad



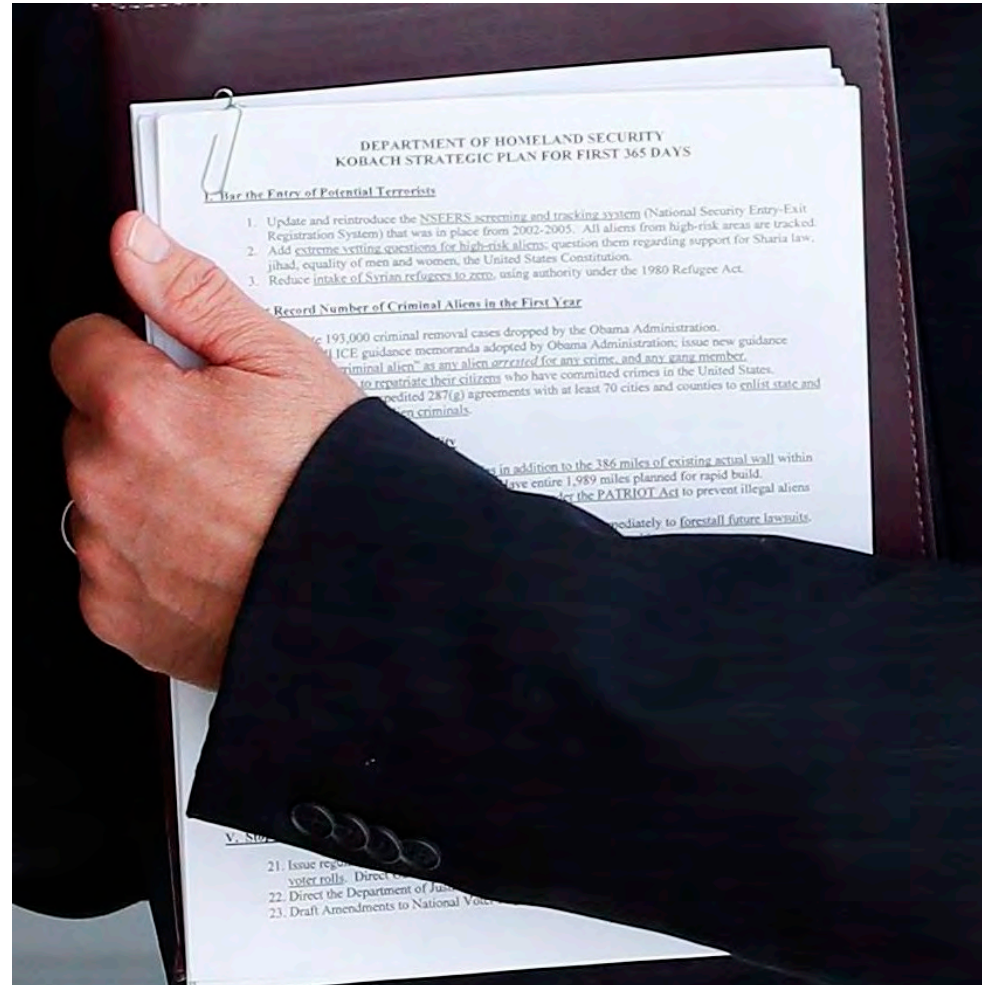
# Confidentiality



# Confidentiality



# Confidentiality





# Confidentiality

## DEPARTMENT OF HOMELAND SECURITY KOBACH STRATEGIC PLAN FOR FIRST 365 DAYS

### I. Bar the Entry of Potential Terrorists

1. Update and reintroduce the NSEERS 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.
3. Reduce intake of Syrian refugees to zero, using authority under the 1980 Refugee Act.

### Record Number of Criminal Aliens in the First Year

193,000 criminal removal cases dropped by the Obama Administration.

ICE guidance memoranda adopted by Obama Administration; issue new guidance

"criminal alien" as any alien arrested for any crime, and any gang member.

to repatriate their citizens who have committed crimes in the United States.

expedited 287(g) agreements with at least 70 cities and counties to enlist state and

alien criminals.

Security

in addition to the 386 miles of existing actual wall within

have entire 1,989 miles planned for rapid build.

under the PATRIOT Act to prevent illegal aliens

# Integrity



# Availability



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



# A Venn diagram, just because



Credit: Daniel Schatz (@Virtuity)

# Physical Security's 5 D's

- Deter
- Detect
- Deny
- Delay
- Defend



The background is a dark blue gradient with a faint, abstract network of white lines and dots, resembling a molecular structure or a data network. The text is centered in the middle of the image.

**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

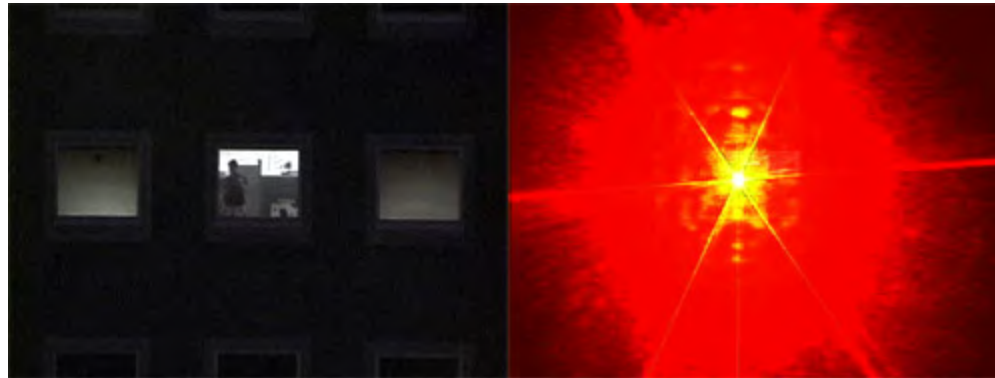


Focused on Entry and Egress Points

Rarely monitored in real time

Cost of recording retention

# Fracking Lasers!



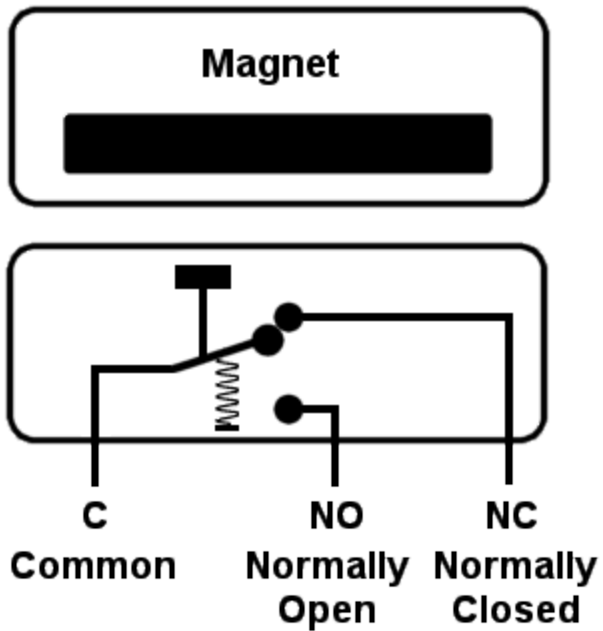
# IP Cameras

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



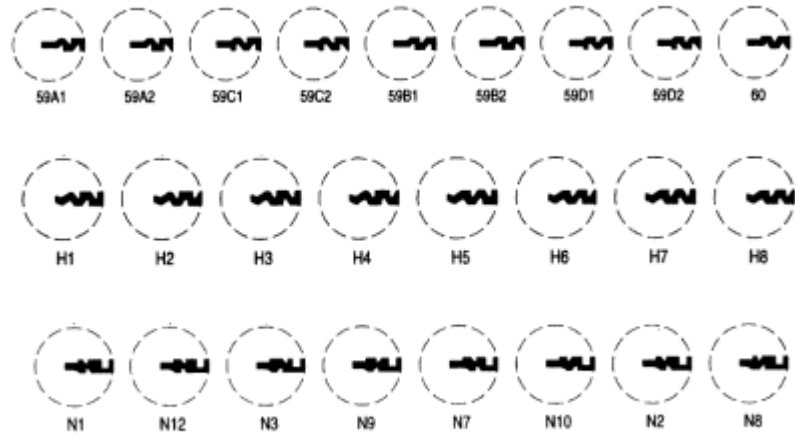
Used for Exit

Check for door gaps

# Fun with doors

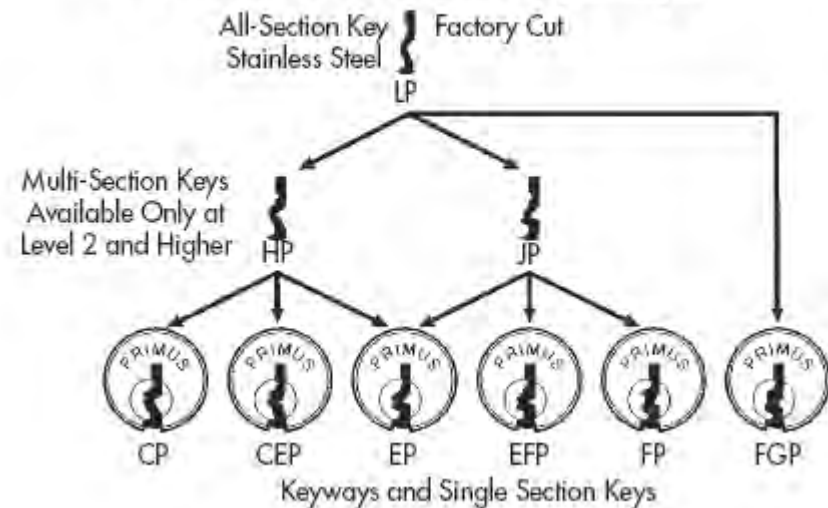


# Keys are bad



Cylinder Options					
D200WP American Lock® Edge™ Key Control	D10 Arrow® K5, K6, L6A	D01 Corbin® 59A1-A2	D29 Corbin® 60	D07 Corbin®/ Russwin® L4	D13 Falcon® (composite)
D12 Kwikset® (composite)	D08 Lockwood®	D11 Russwin® 981/852	D30 Russwin® D1	D36 Sargent® LA-LC (composite)	D70 Sargent® RA-RC (composite)
D04 Schlage® C	D34 Schlage® E	D28 Schlage® P (accepts C-L)	D13 Weiser® (composite)	D03 Yale® 8	D15 Yale® GA

## Primus Obverse Keyways





# 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



## Personnel Barriers

Cargo and freight have to  
come in somehow.

Find it.

# Elevators



WELCOME TO THE  
**LOS ANGELES FIRE DEPARTMENT**



[FIRE STATIONS](#)

[ALERTS](#)

[NEWS](#)

[RED FLAG](#)

[SAFETY](#)

[FIRE PREVENTION](#)

[FIRESTATLA](#)

[JOIN](#)

[FAQS](#)

[ABOUT](#)

## LAFD REQUIREMENT #75: KEY ACCESS BOX STANDARD

PRINT 

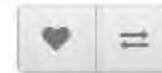
FIRE PREVENTION & PUBLIC SAFETY BUREAU



REQUIREMENT #75: KEY ACCESS BOX STANDARD



# Fire Service Keys



## Universal Fire Service Key Set

Brand: [ElevatorKeys.com](https://ElevatorKeys.com)

Product Code: KSUFS16

Availability: 2 - 3 Days

**\$124.95**

Qty

# 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>