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

CORE SECURITY

Hi! I’m Bobby.

CORE SECURITY

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.

CORE SECURITY

A couple of things to start with

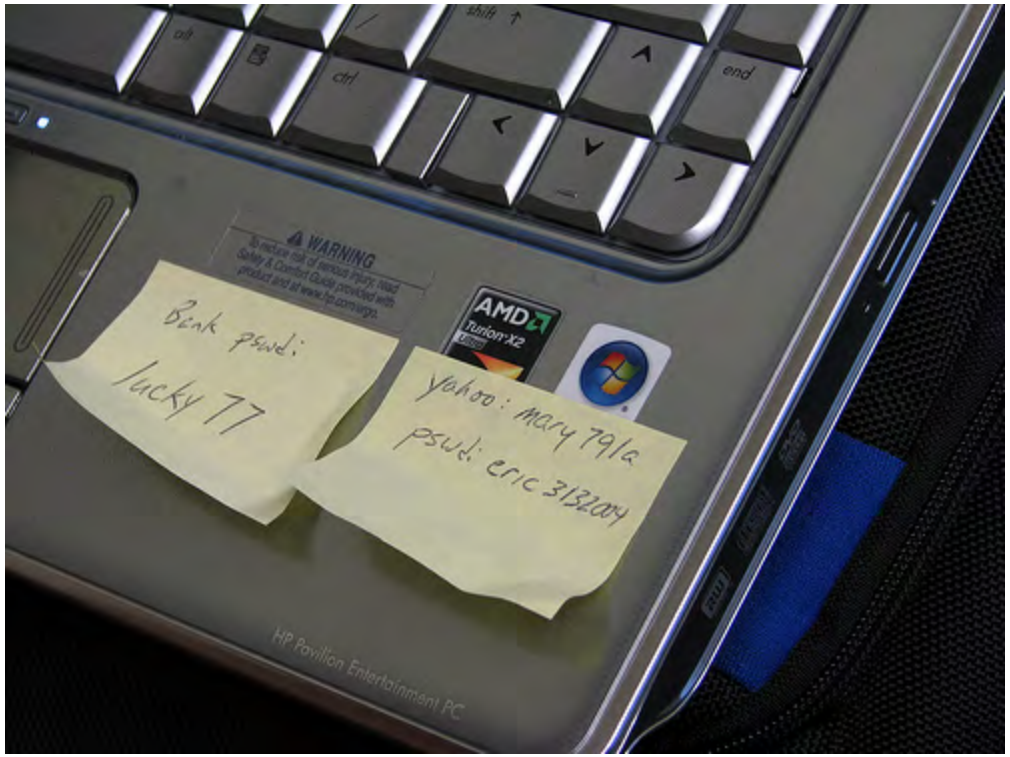
Seriously, don’t do it.

CORE SECURITY

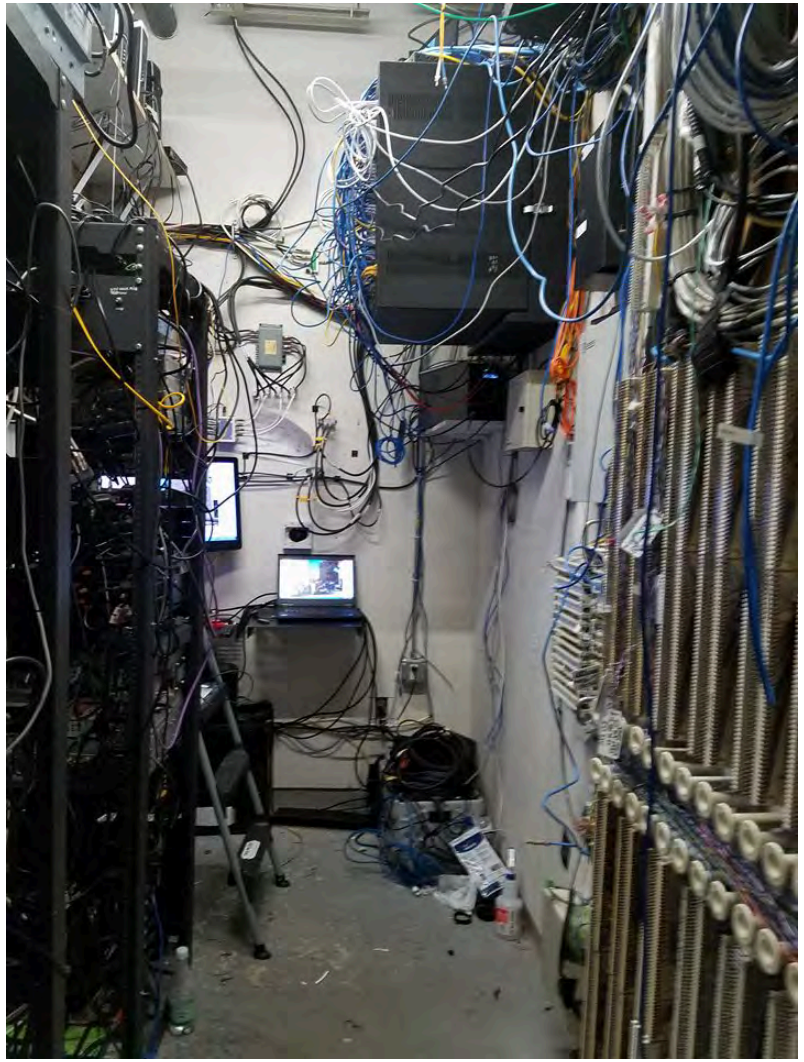
If I can touch it, it’s not your computer/network anymore.

Physical Security Matters

Ahem..

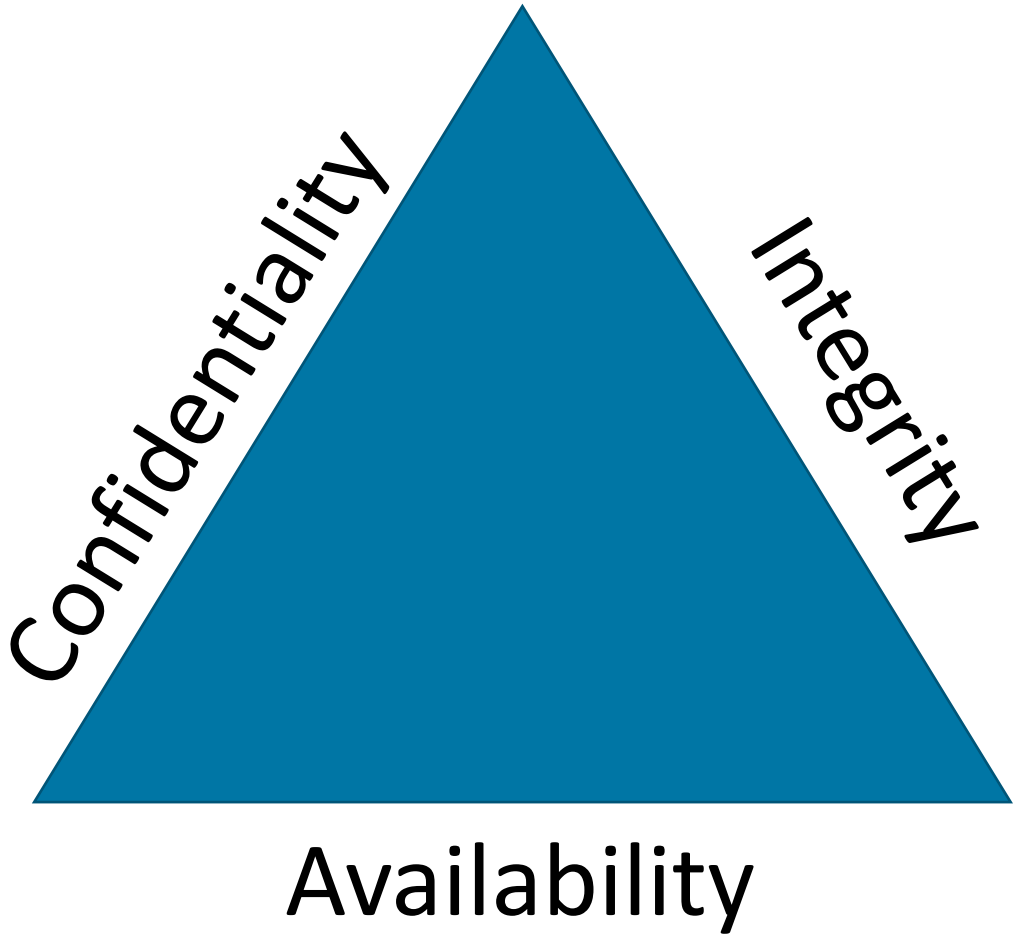


Can you spot the RasPi with the cell modem?

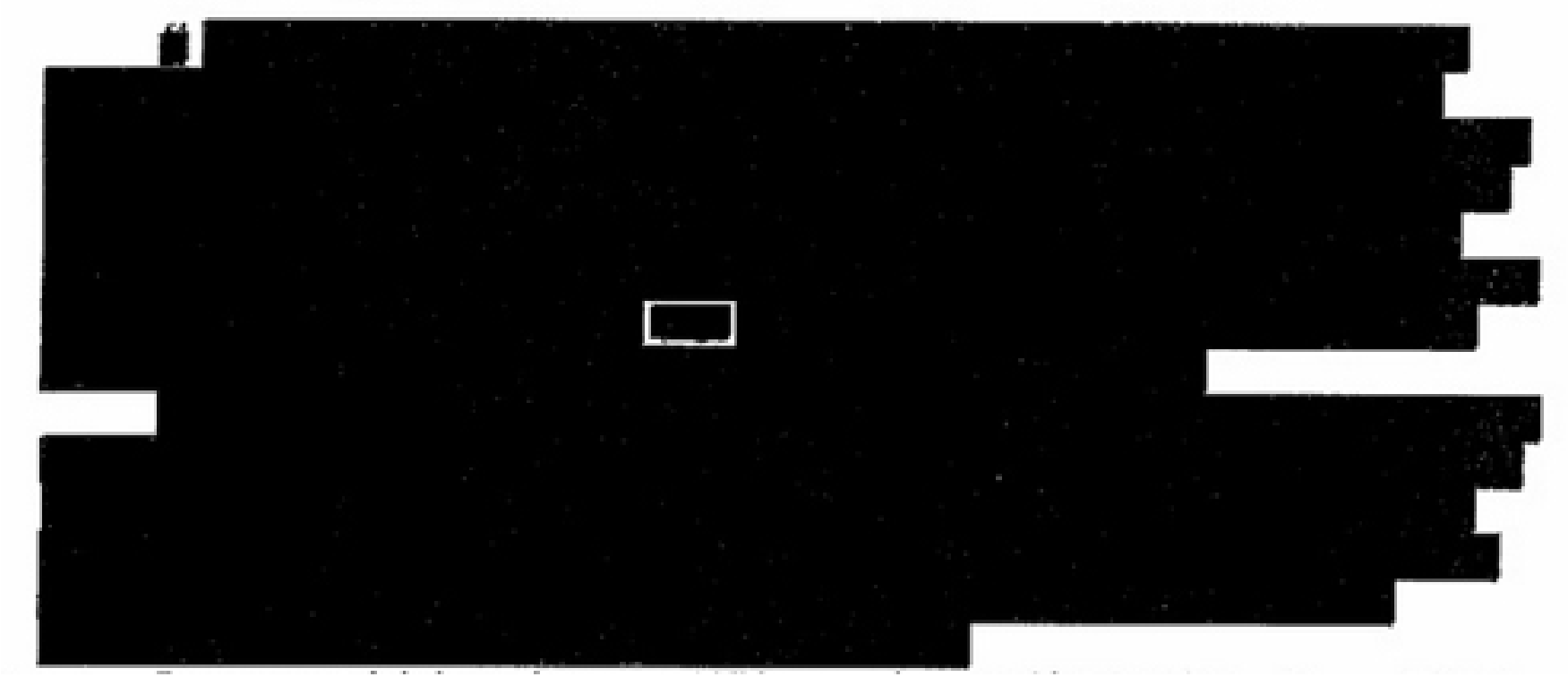


Wiring closet at Fenway Park during a game, Boston. Photo Credit: Rayanne Buchianico

The Traditional Security Triad

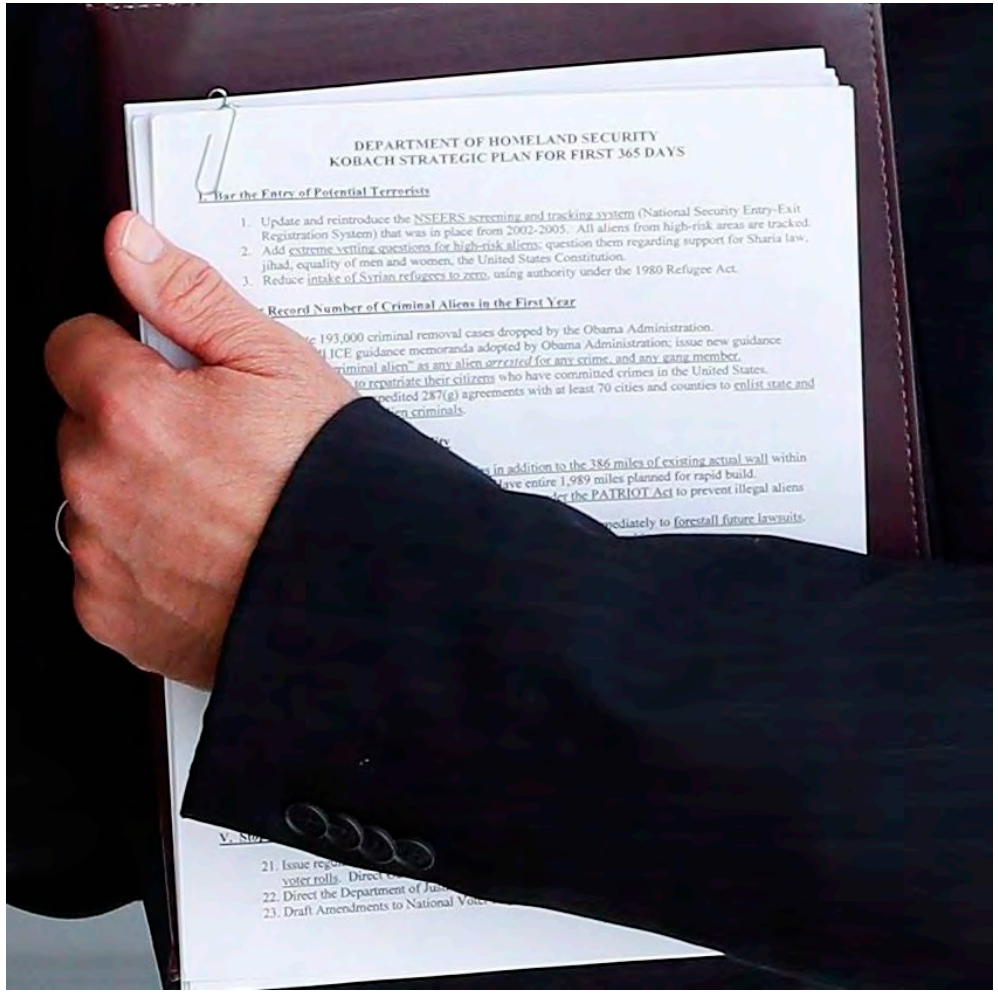


Confidentiality

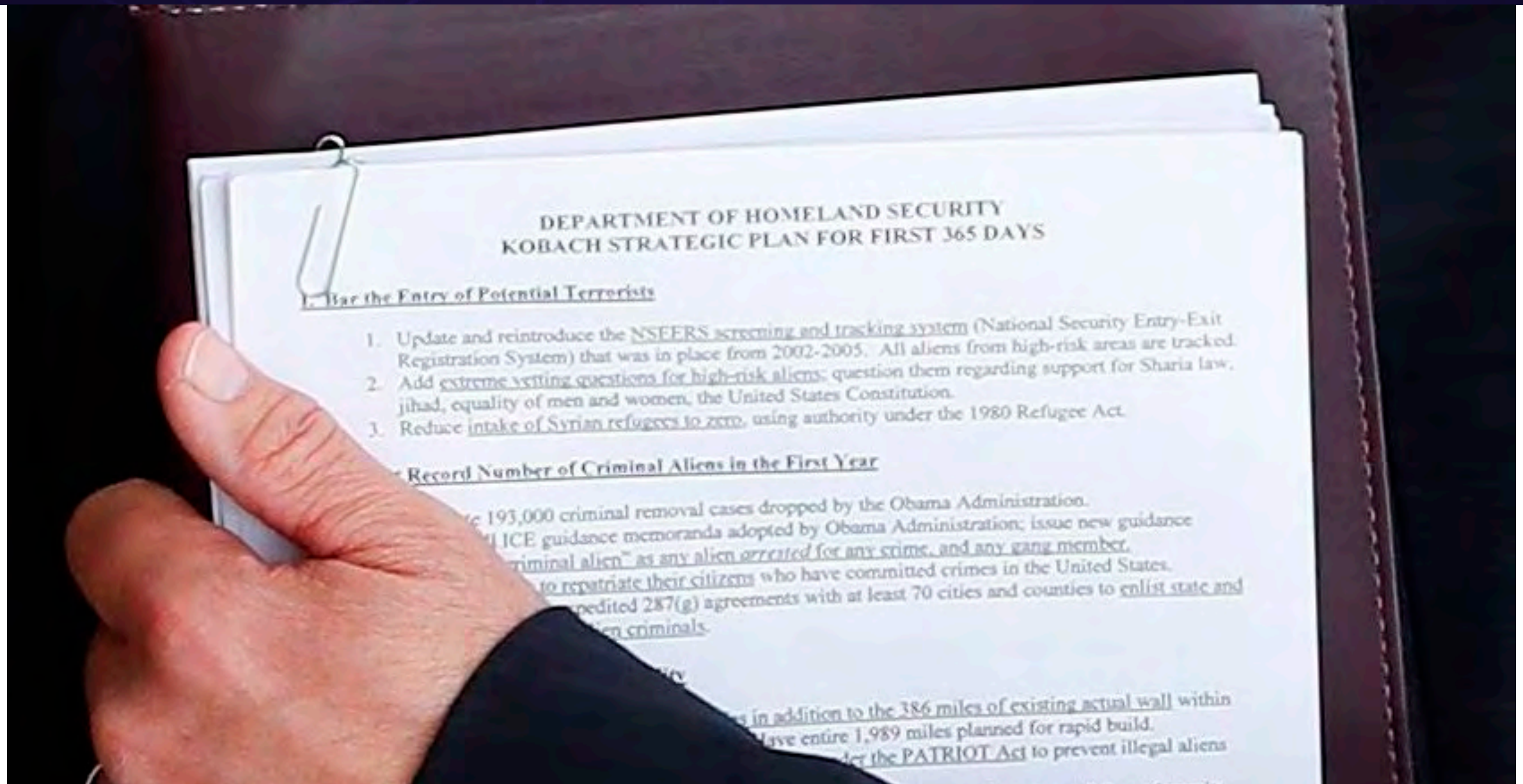


Confidentiality

Confidentiality



Confidentiality



Integrity


DEPARTMENT of INVESTIGATION
FBI
THIS CERTIFIES THAT THE SIGNATURE AND PHOTOGRAPH HEREON IS AN APPOINTED
SPECIAL AGENT
OF THE FEDERAL BUREAU OF JUSTICE, UNITED STATES DEPARTMENT OF INVESTIGATION.
For Mulder
SUCH IS CHARGED WITH THE DUTY OF INVESTIGATING VIOLATIONS OF THE LAWS OF THE UNITED STATES, COLLECTING EVIDENCE IN CASES IN WHICH THE UNITED STATES IS OR MAY BE A PARTY IN INTEREST, AND PERFORMING OTHER DUTIES IMPOSED UPON HIM BY LAW.
DIRECTOR
ORDER OF THE ATTORNEY GENERAL OF THE UNITED STATES
JUSTICE DEPARTMENT
FEDERAL BUREAU OF INVESTIGATION

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

Notice that there’s nothing about STOPPING attackers

Fences

CORE SECURITY

Fences

Story time!

CORE SECURITY

Guards

Provide real-time response

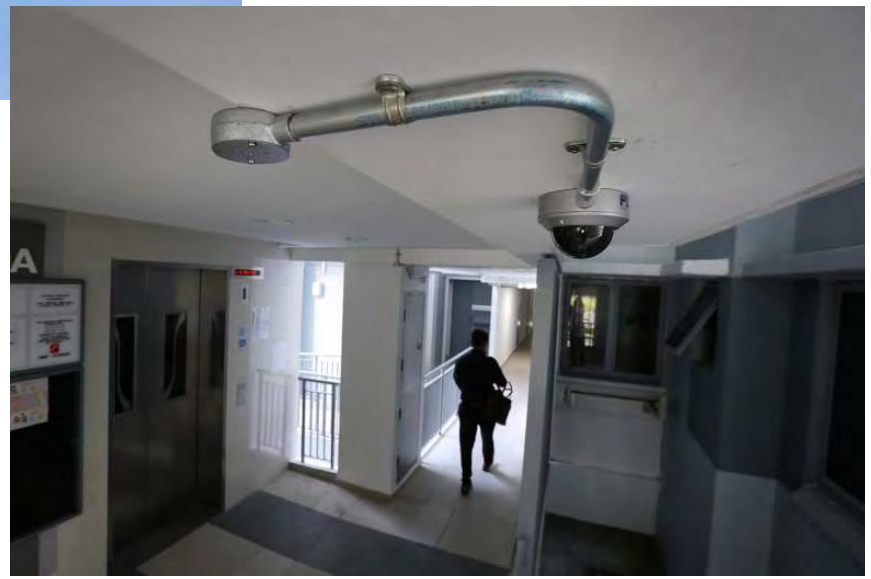
Able to improvise

Expensive

They get bored

CORE SECURITY

Cameras



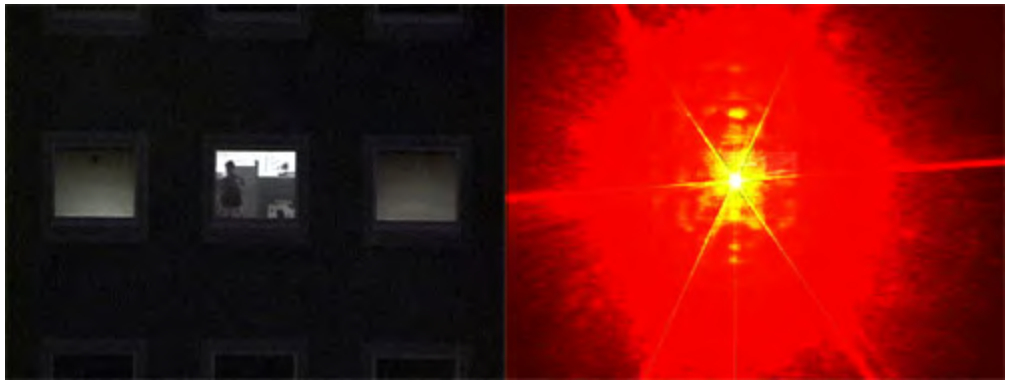
Focused on Entry and Egress Points

Rarely monitored in real time

Cost of recording retention

CORE SECURITY

Fracking Lasers!



CORE SECURITY

IP Cameras

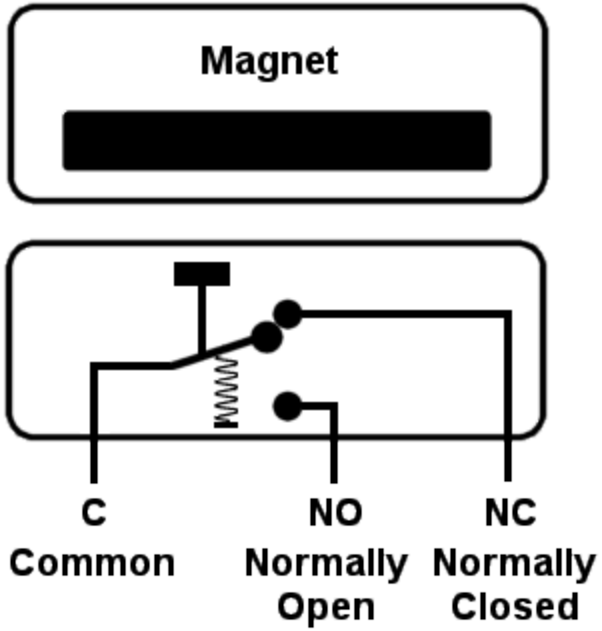
If you can get access to the Ethernet line, check out Looping Surveillance Cameras through Live Editing from DEFCON 23

CORE SECURITY

Door open/close sensors

CORE SECURITY

Operate on magnetic fields



CORE SECURITY

Motion Sensors

Some use Ultrasound

Some use Infrared

They can be tuned to increase or decrease sensitivity

CORE SECURITY

Motion Sensors

Degrades the sensitivity of sensors

Requires prior placement

CORE SECURITY

Lasers Again

Don’t use too much

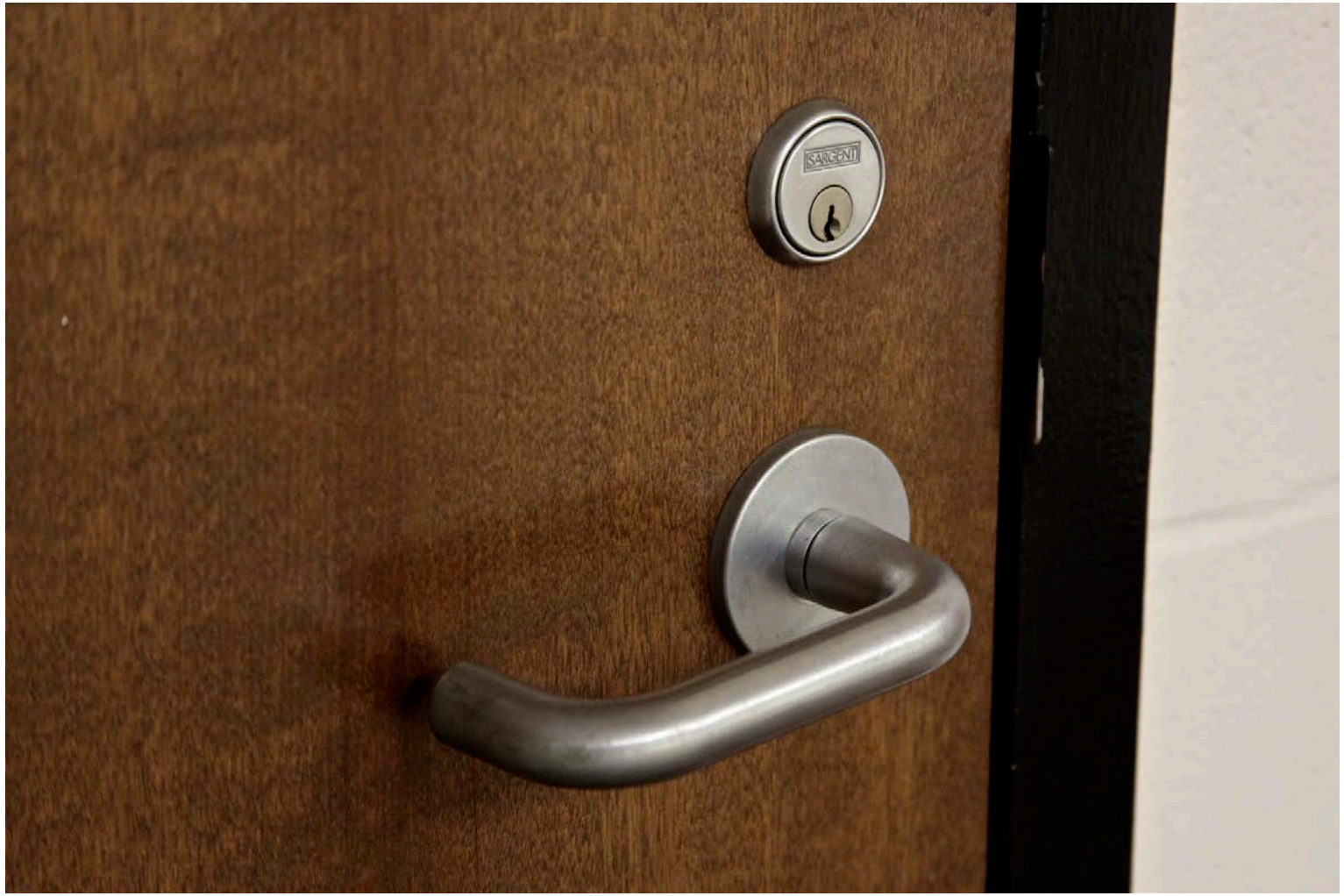
CORE SECURITY

Motion Sensors

Used for Exit

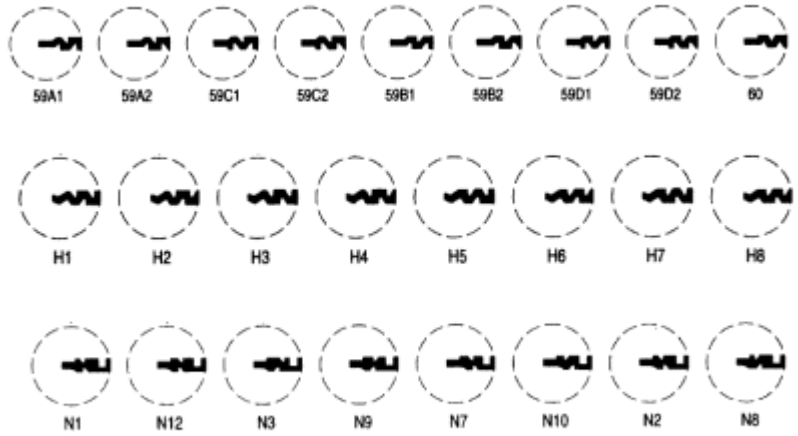
Check for door gaps

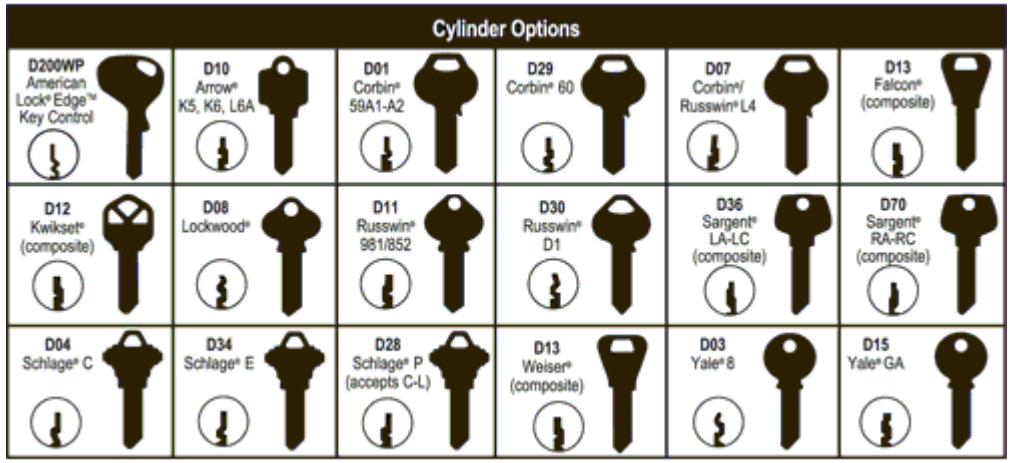
Fun with doors

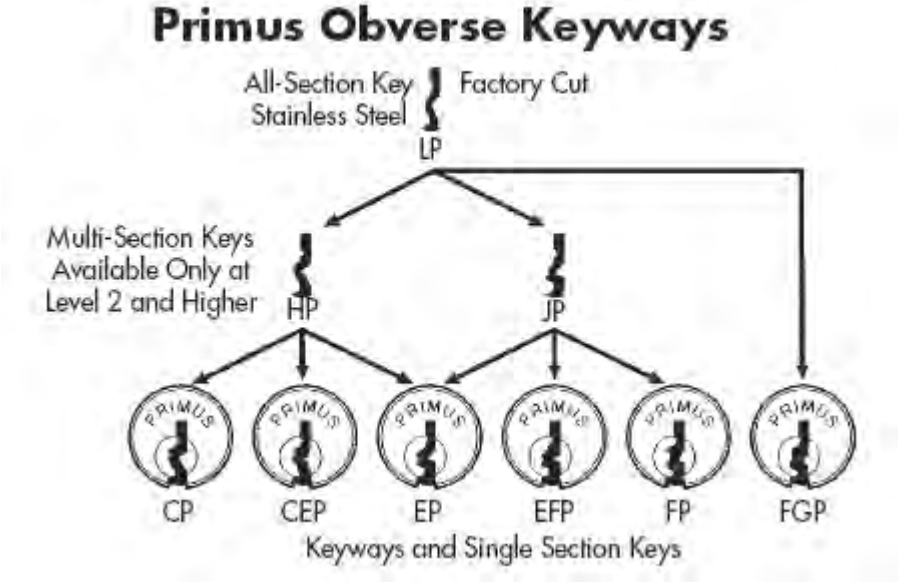


CORE SECURITY

Keys are bad







CORE SECURITY

Picks

CORE SECURITY

Guns

CORE SECURITY

Bump Keys

CORE SECURITY

Destructive bits

Do not try this at home,
work, school,
or really anywhere.

CORE SECURITY

Strikes

CORE SECURITY

Guards and Blocks

CORE SECURITY

The most versatile bypass tools

CORE SECURITY

The most versatile bypass tools

CORE SECURITY

Proximity Cards

CORE SECURITY

Prox Cards

“Short” range RFID

Authentication, but not authorization

Trivial to clone

CORE SECURITY

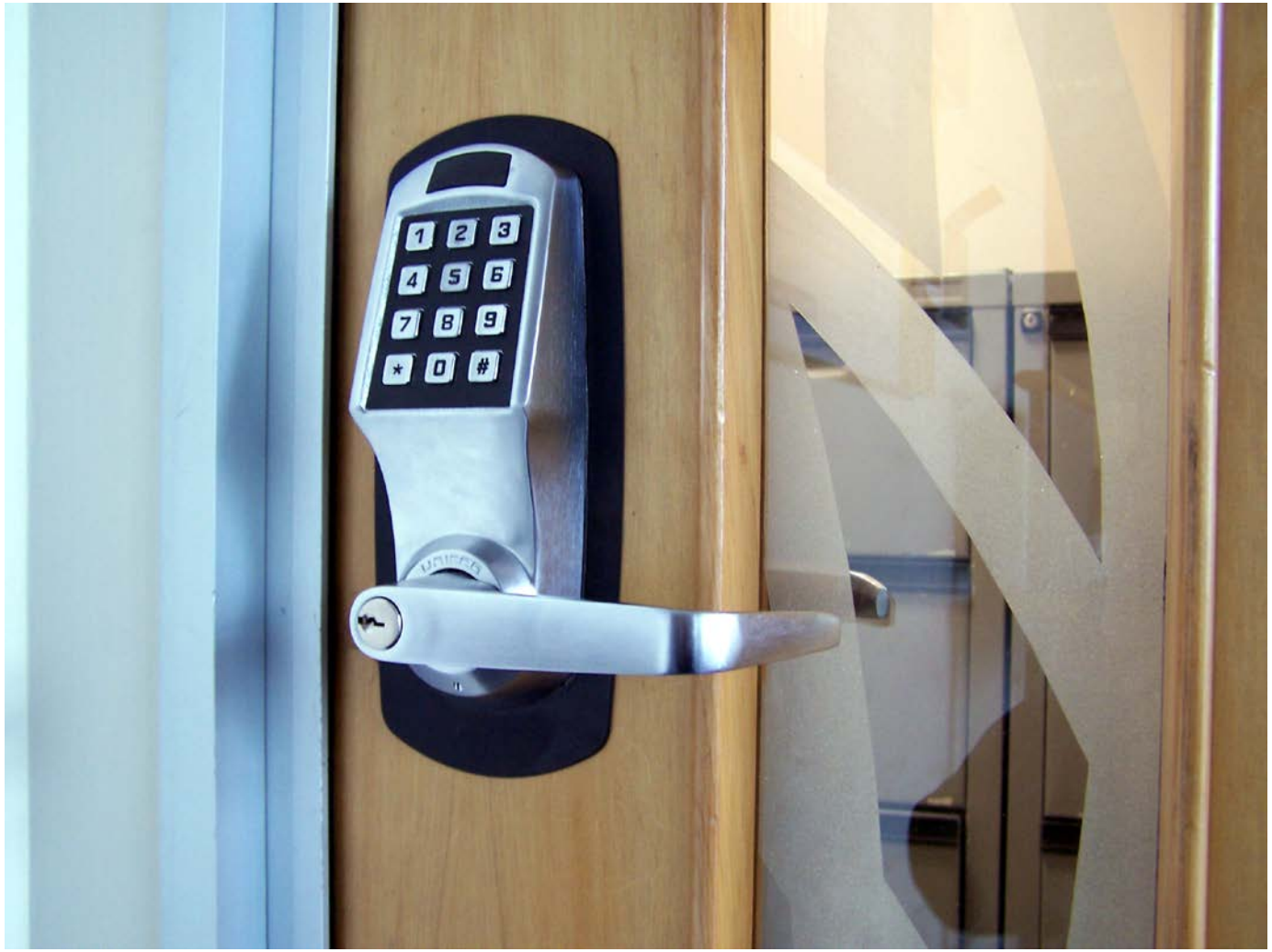
Biometrics

CORE SECURITY

Cloning fingerprints

CORE SECURITY

Electronic locks



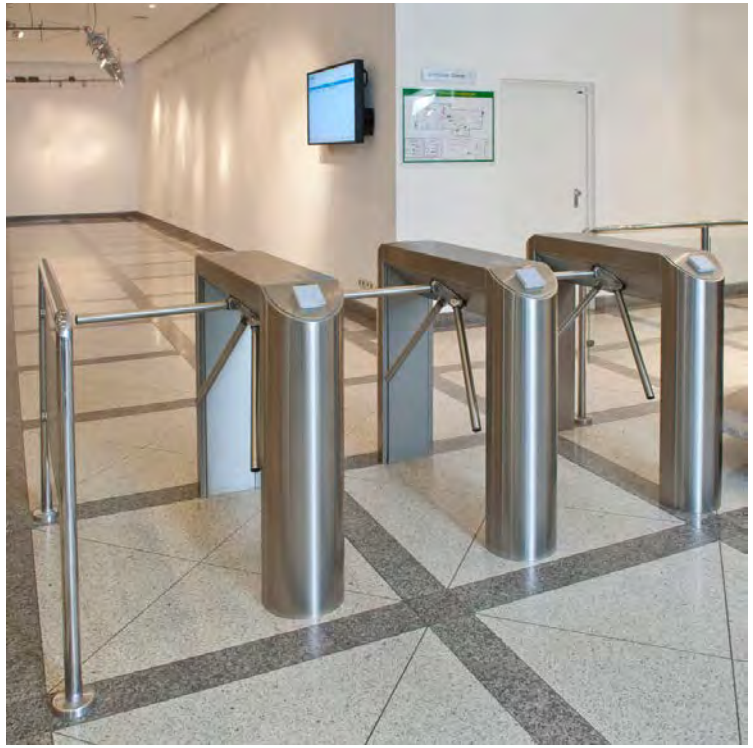
CORE SECURITY

Electronic locks

- Default codes… sometimes
- People reuse codes
- When in doubt…

CORE SECURITY

Turnstiles and Mantraps



Personnel Barriers

Cargo and freight have to come in somehow.

Find it.

Elevators

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
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