Is Your Data Literally Walking Out the Door?

Mike Saunders

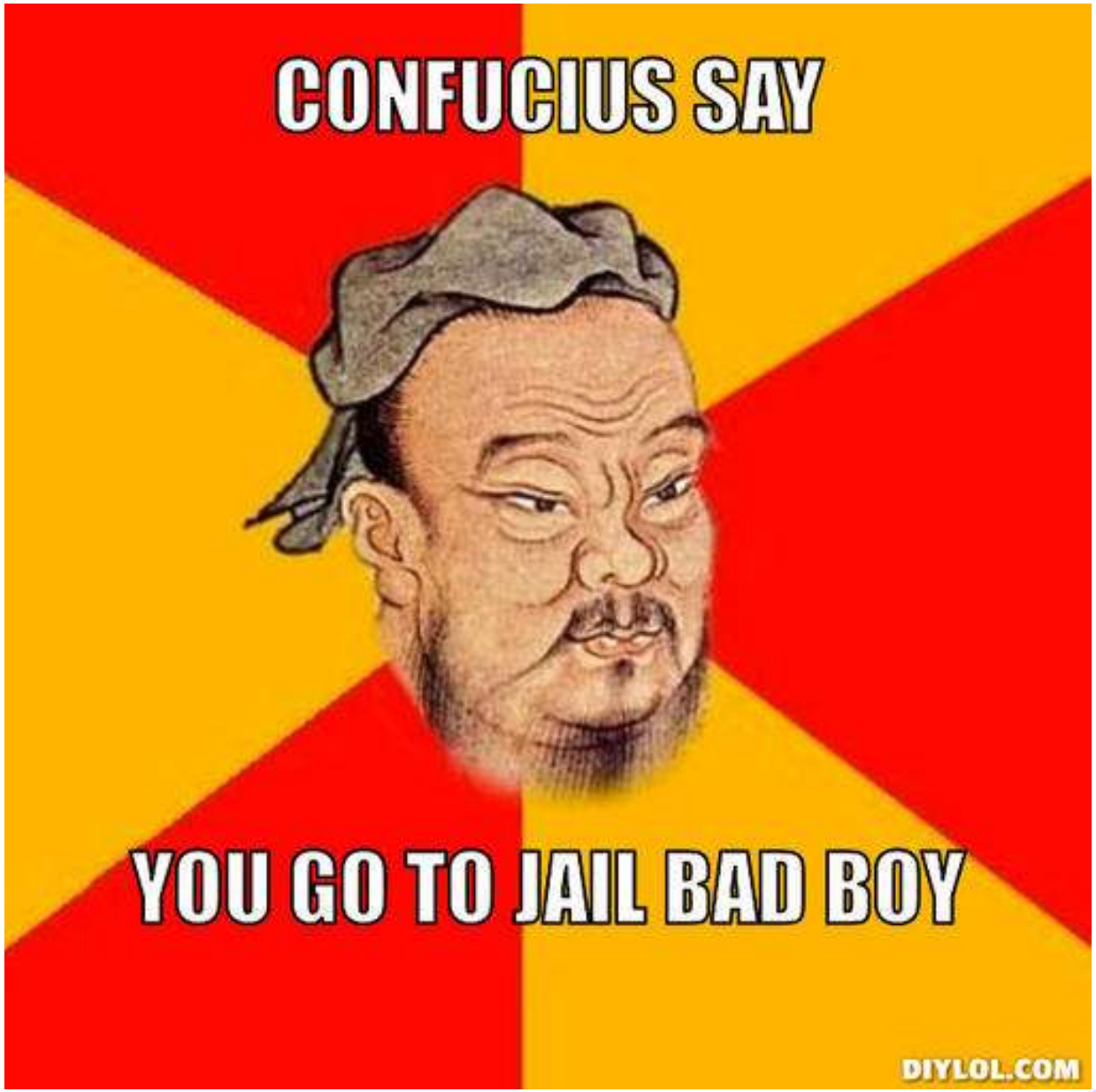
Hardwater Information Security

About Mike

- In IT full-time since 1998
- Entered IT Security in 2007
- Certifications: CISSP, GPEN, GWAPT, GCIH
- Not a professional physical security tester, just curious. And paranoid.

DISCLAIMER

- If you don’t own it or don’t have permission, don’t test it!
- Seriously! Don’t do it!
- Don’t test on your critical controls unless you have backups
- Attempting physical bypass of security mechanisms may result in damage
- Make sure you have written authorization with you if you’re attempting a physical pen test
  - Have at least two contact numbers
  - Make sure your contacts will be available in case you get caught

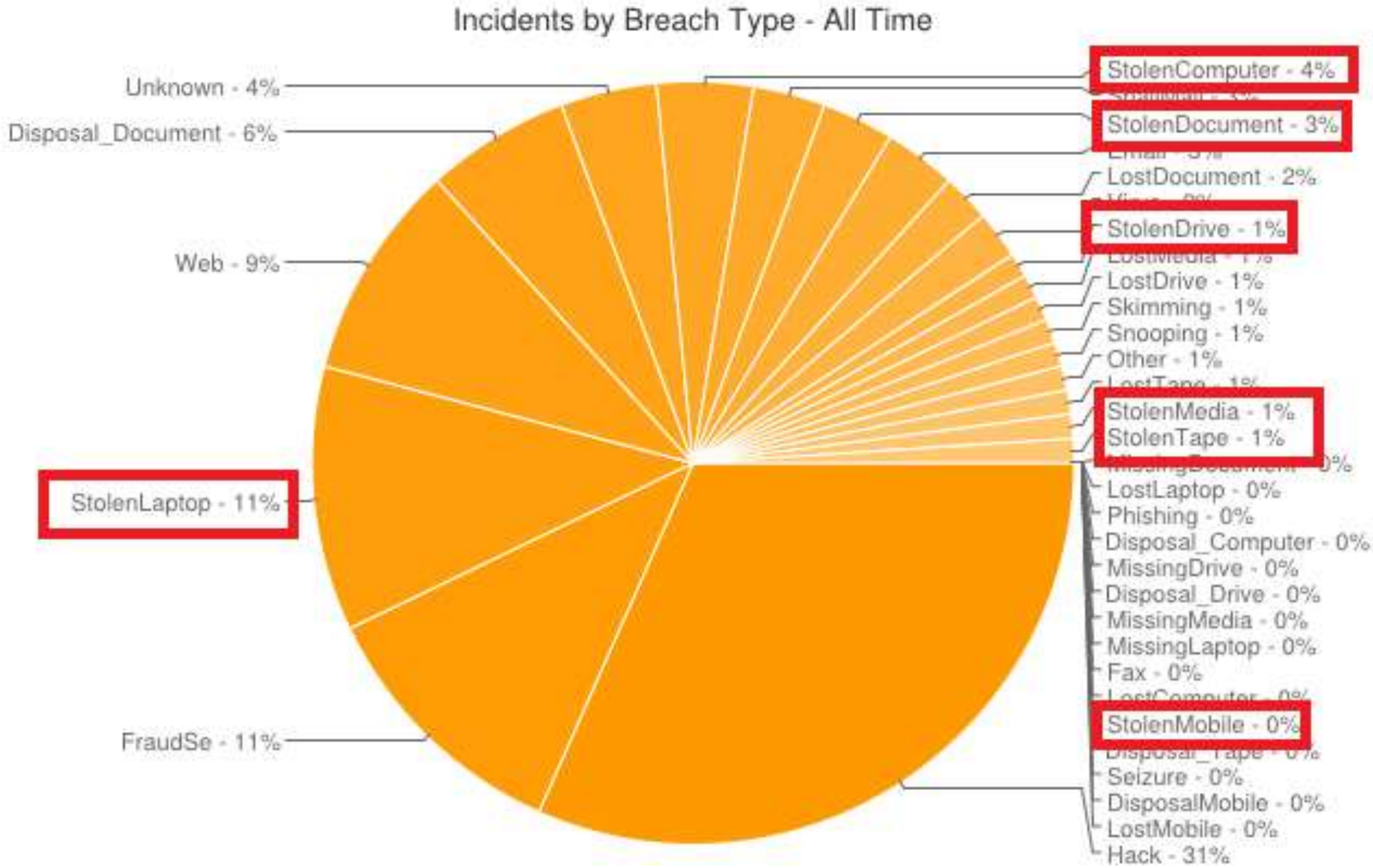

CONFUCIUS SAY
YOU GO TO JAIL BAD BOY
DIYLOL.COM

Goals

- Overview on how attackers see your physical security
- Provide information about bypassing common security mechanisms
- When you leave here, look at your infrastructure in a new way
- Talk about some defenses

Data Loss / Breach via Physical Theft

- 2009 - BCBSTN – 57 stolen hard drives = over 1M records
- datalossdb.org – ~21% of all lost records due to theft
  - 11% stolen laptop
  - 4% stolen computer
  - 3% stolen document
  - 1% stolen drive
  - 1% stolen media
  - 1% stolen tape


Incidents by Breach Type - All Time
Unknown - 4%
Disposal_Document - 6%
Web - 9%
StolenLaptop - 11%
FraudSe - 11%
StolenComputer - 4%
StolenDocument - 3%
LostDocument - 2%
StolenDrive - 1%
LostDrive - 1%
Skimming - 1%
Snooping - 1%
Other - 1%
StolenMedia - 1%
StolenTape - 1%
LostLaptop - 0%
Phishing - 0%
Disposal_Computer - 0%
MissingDrive - 0%
Disposal_Drive - 0%
MissingMedia - 0%
MissingLaptop - 0%
Fax - 0%
StolenMobile - 0%
Seizure - 0%
DisposalMobile - 0%
LostMobile - 0%
Hack - 31%

Physical security principles

- Deter
  - Lighting, fencing and gates, guards
- Deny
  - Locking mechanisms
- Detect
  - Cameras, motion sensors, glass break sensors, noise sensors, vibration sensors
- Delay
  - Locking cables, higher security locks, attack-resistant safes

Surveillance and accesibility

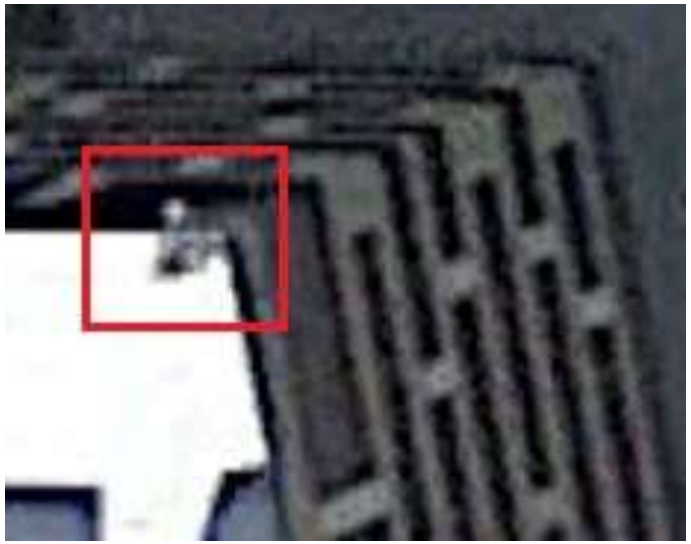
- Are there vantage points to observe your facility discretely?
  - Even if there aren't, there's always Google
- Are there doors only used for exiting?
- Hedges and trees are great for privacy for you *and* potential attackers
- 7' fences will deter most attackers
  - 8' with 3-strand barbwire on top, 45 degrees facing outward will deter all but most determined / most to gain
- Higher security areas may require multiple perimeters with gates
- Lights act as a weak deterrent, coupled with cameras they act as a detective control
- Are there gaps in the camera coverage?

Recon

Street view

Cameras

More cameras



We haz security!

O Rly?

What the? I can't even.

www.schneier.com

More fail

Other thoughts on perimeter security

- Easy wins
  - Doors propped open
  - Doors unlocked for convenience
  - Windows open for cooling
- Were you expecting that delivery?

We’ve got doors! Even Locks!

gregvan.com

Doors with External Hinges

- Just pop the hinge pins!

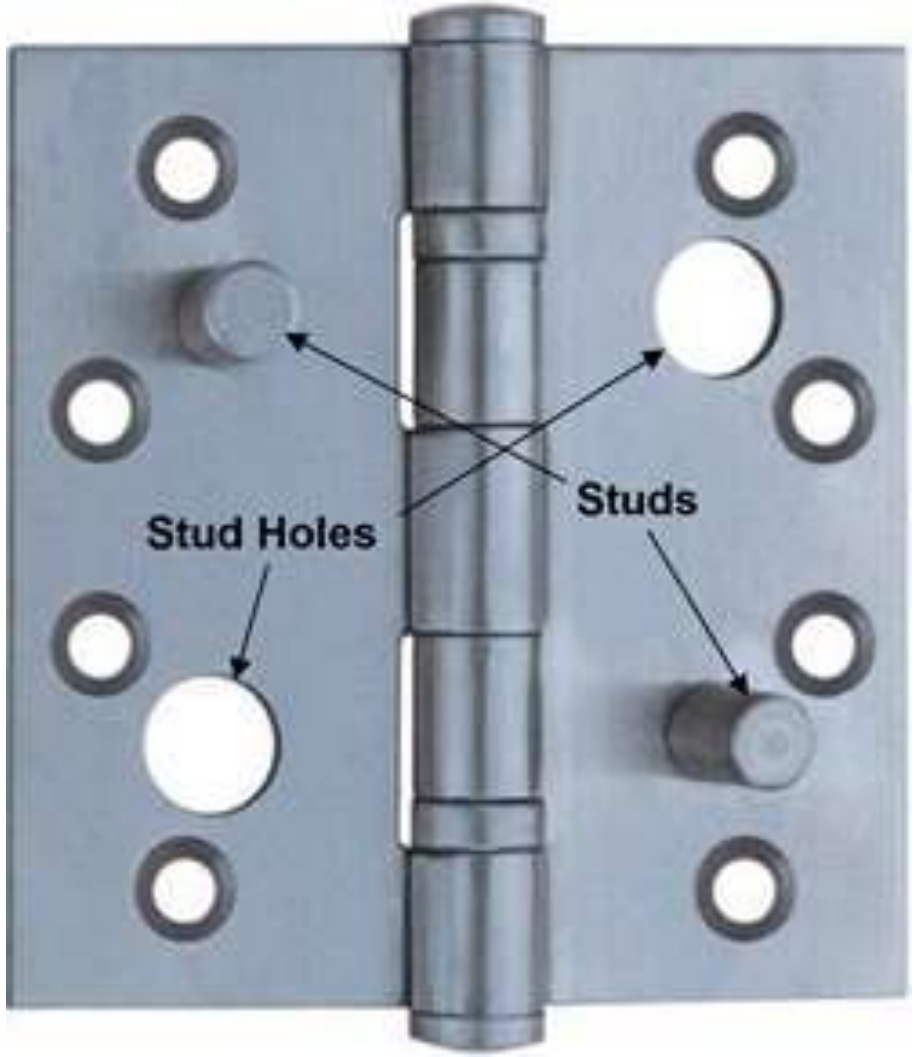
Protecting hinges

- If you must have external hinges, use a secure hinge
  - Set screw hinges
  - Stud hinges
  - Non-removable hinge pin

Set screw hinge

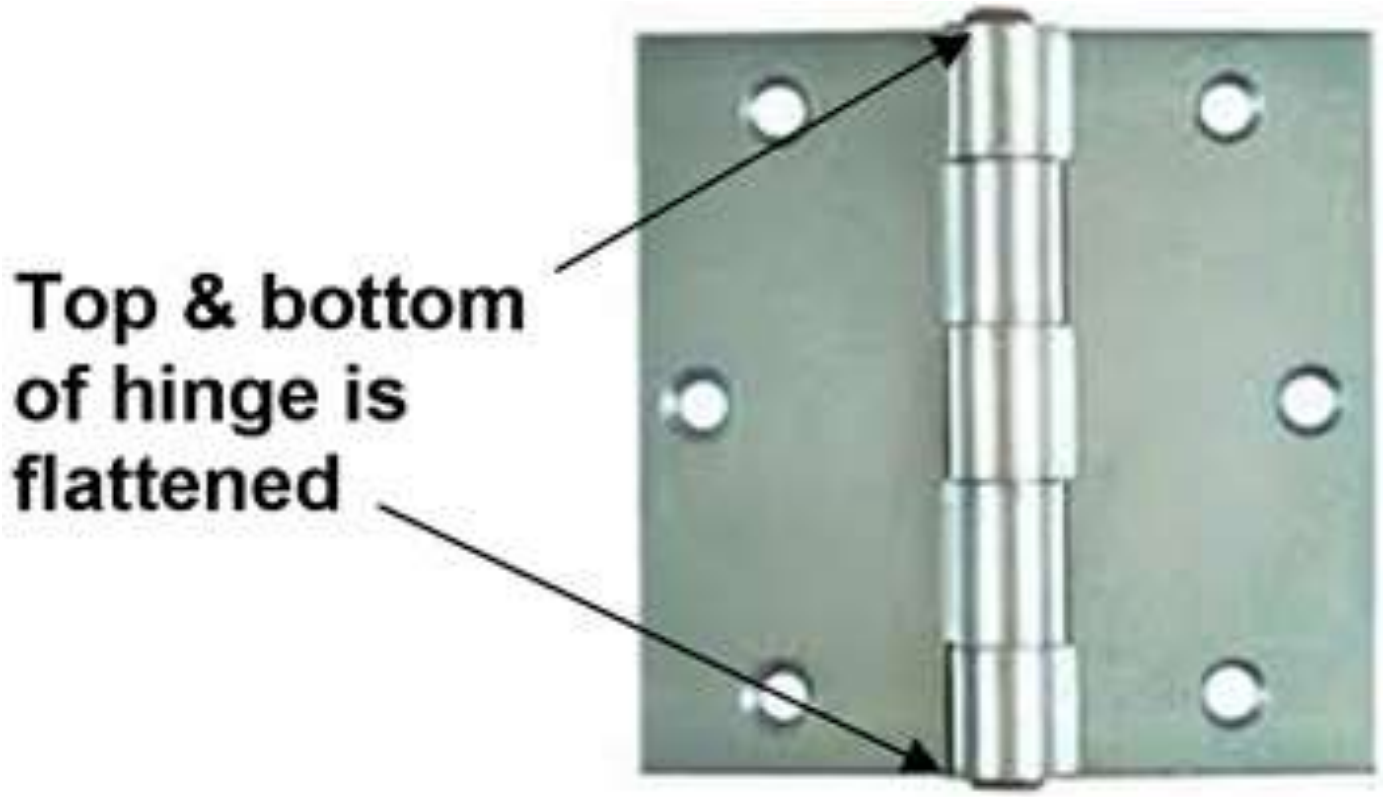
www.renovation-headquarters.com

Stud hinge



www.renovation-headquarters.com

Non-removable hinge



www.renovation-headquarters.com

Crash (panic) Bar Doors

www.leinbachservices.com

Bypass and protect a crash bar door

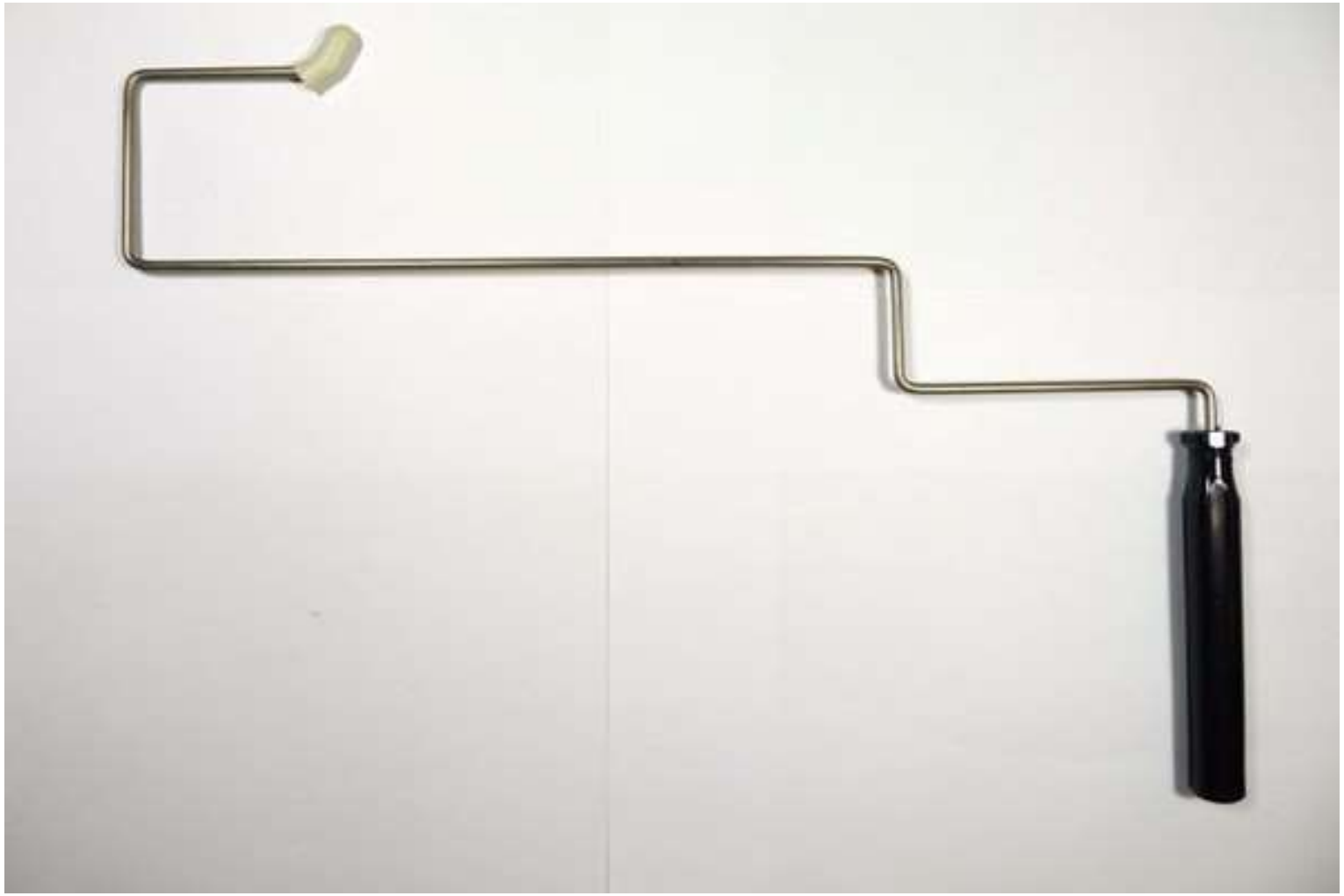
Insert a prying tool here!

A latch plate protector helps prevent prying.

Can possibly be bypassed by tying a small screw or nail to a piece of string, inserted behind protector plate, pulled through from underneath to trigger latch.

Infosecinstitute.com

J tool door bypass tool



J tool in action

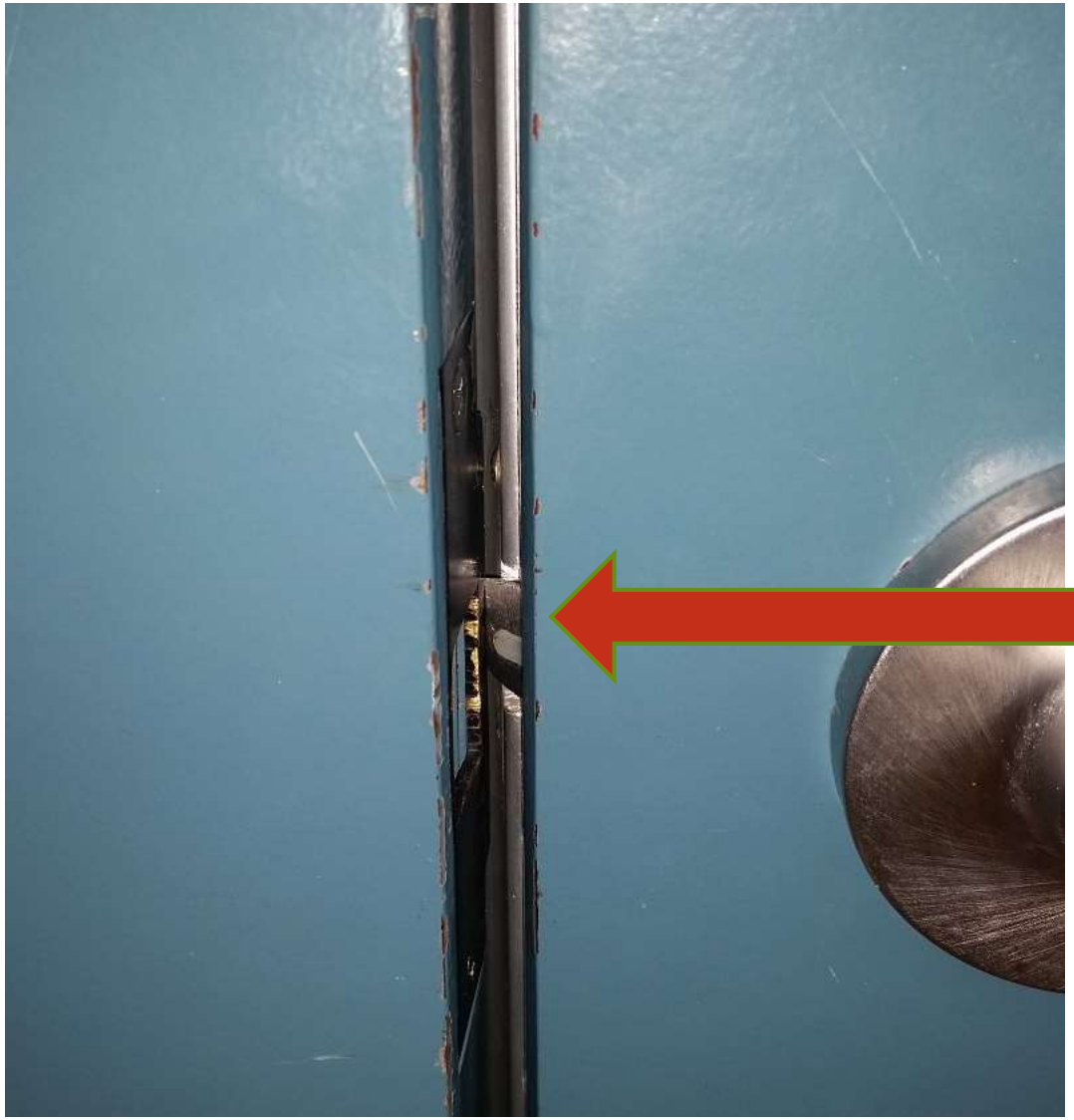
TouchSense Crash Bar Doors

If there's enough room, a piece of copper wire inserted through door frame and touched to bar will trigger sensor.

www.katzlerlocks.com

Well, what do we have here?

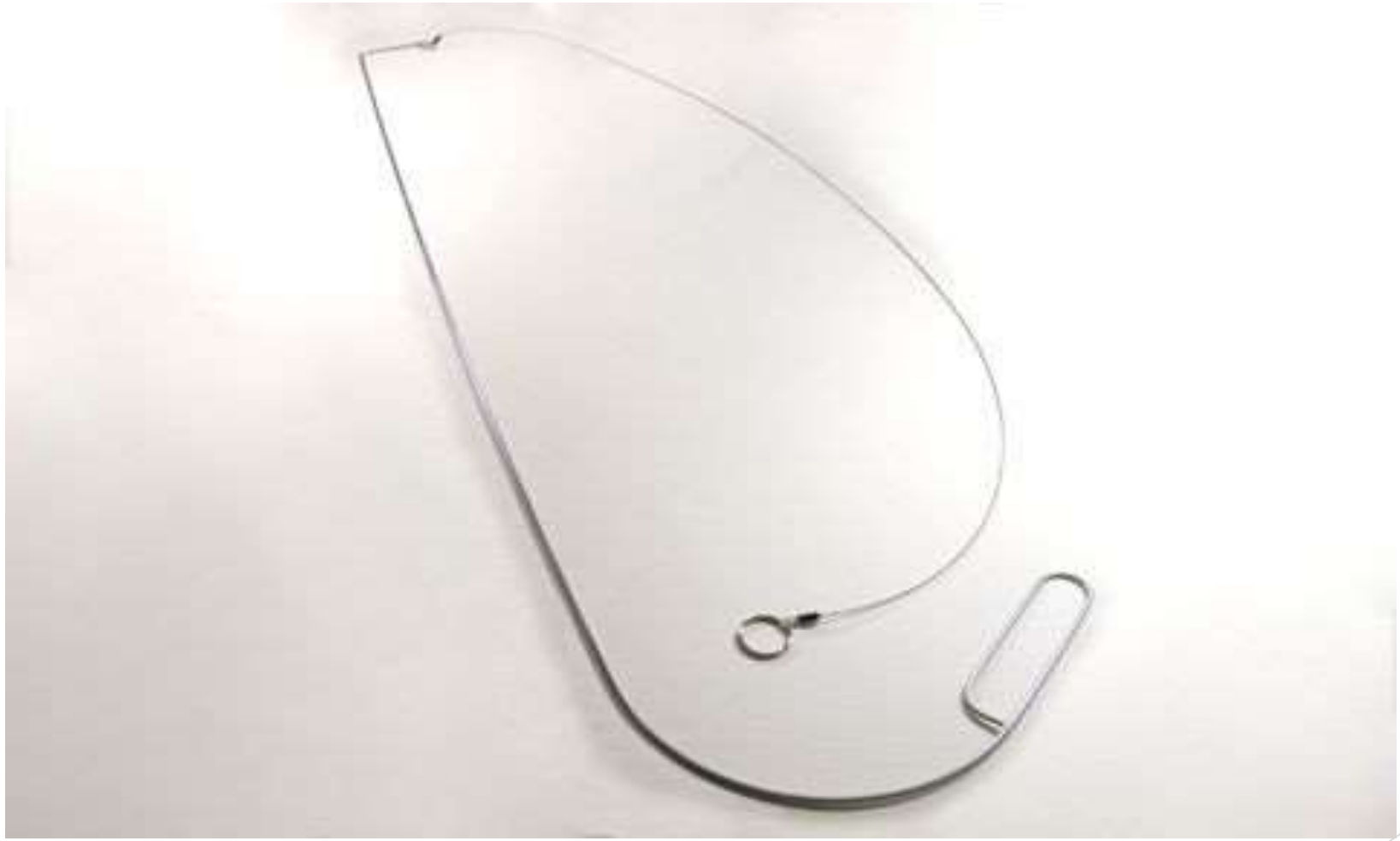
No keys? No problem!



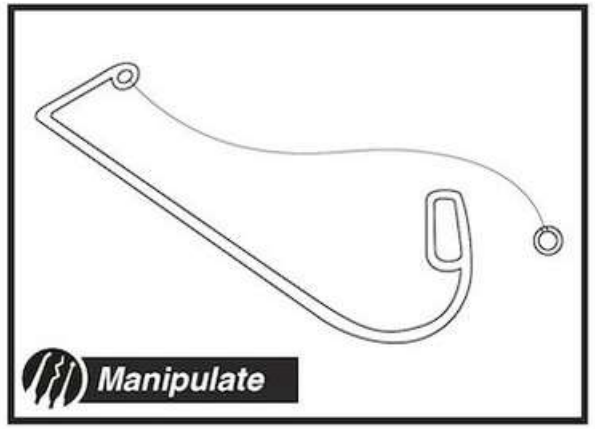
Pick a card. Any card will do!

What about lever handles?

The K-22

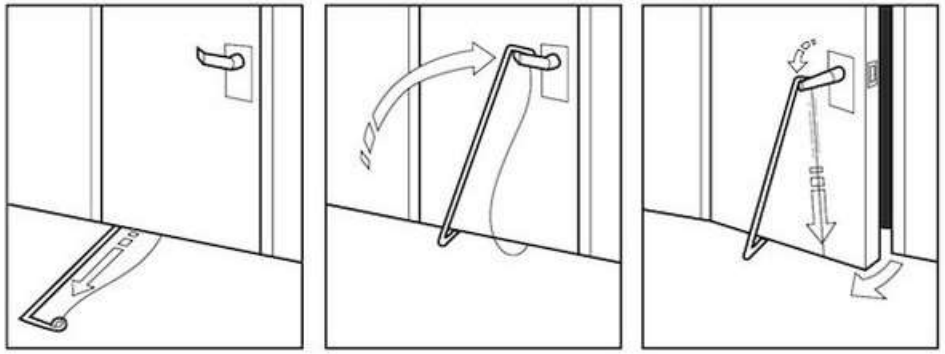


K-22 in action



Detailed Uses

This tool has one use, and it does it well. It goes underneath a door and pulls on the lever on the inside. The inside lever on many types of security hardware is left open in case of emergencies and for convenience - even when the outside lever is locked. As a note, try to not keep the tool bent all the time. Hang it up or put it on a shelf. When you are ready to go, bend the tool to fit in the bag and put it to use!



Step 1:
Insert tool under the door

Step 2:
Work tool over the latch

Step 3:
Pull down on cable to open the door

Stealth

K-22 meets crash bar

http://www.theben-jim.com/

What about the roof?

- Access to roof may be gained from adjacent building, tree, or climbing
- Rooftop openings often overlooked
  - Simple locks or no locks at all
  - May not have additional controls (RFID, cameras, etc.)
- Access to ventilation shafts

We’ve got badge readers!

And he’s cloning your badge!

RFID Badge Reader Attacks

- Badges can be cloned
- $500 buys the hardware to clone cards and brute force RFID badge reader
  - Proxbrute - http://www.mcafee.com/us/downloads/free-tools/proxbrute.aspx
- Larger antennas can be hidden in a clipboard, read from several feet away
- Newer HID iCLASS encryption key available for purchase
- Resources:
  - http://www.irongeek.com/i.php?page=videos/derbycon4/t110-advanced-red-teaming-all-your-badges-are-belong-to-us-eric-smith
  - http://www.irongeek.com/i.php?page=videos/derbycon3/3303-how-can-i-do-that-intro-to-hardware-hacking-with-an-rfid-badge-reader-kevin-bong

Where do I find badges to clone?

- Physical observation may lead to favorite lunch places or watering holes
- After-hours company events posted online
- Wait, didn’t we see something earlier?

Time to get on the bus

Or go for a walk

What about cameras?

Who’s got a wire cutter?

www.cabletiesandmore.com

www.assecurity.ca

Wireless cameras?

www.astak.com

Seek…

advanced-intelligence.com

Adjustable 7W Powerful All Wireless Bug Camera Jammer & WiFi GPS Blocker

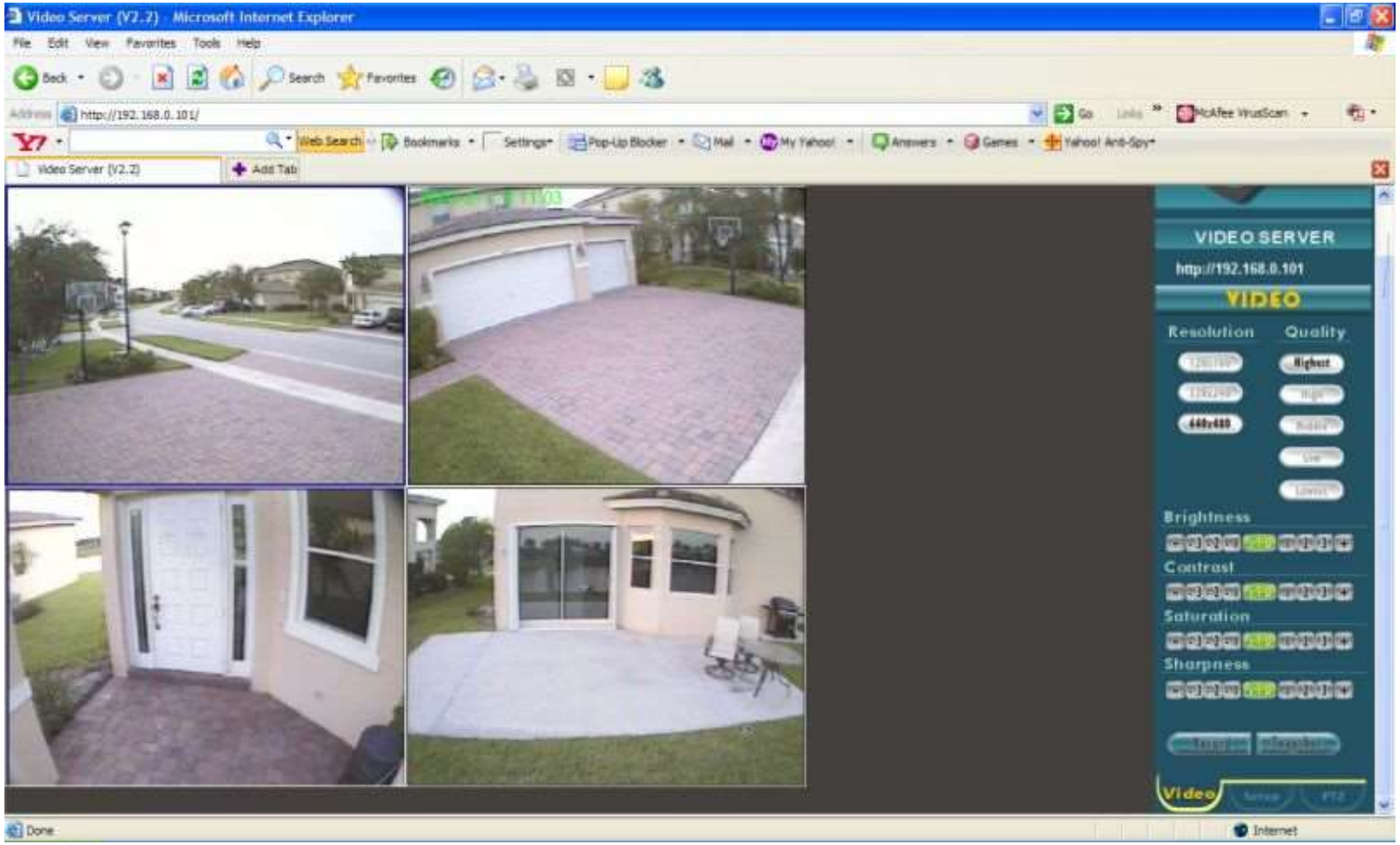
US$257.99

Compare

Add To Cart

And destroy (or at least jam)

IP cameras (and security systems)

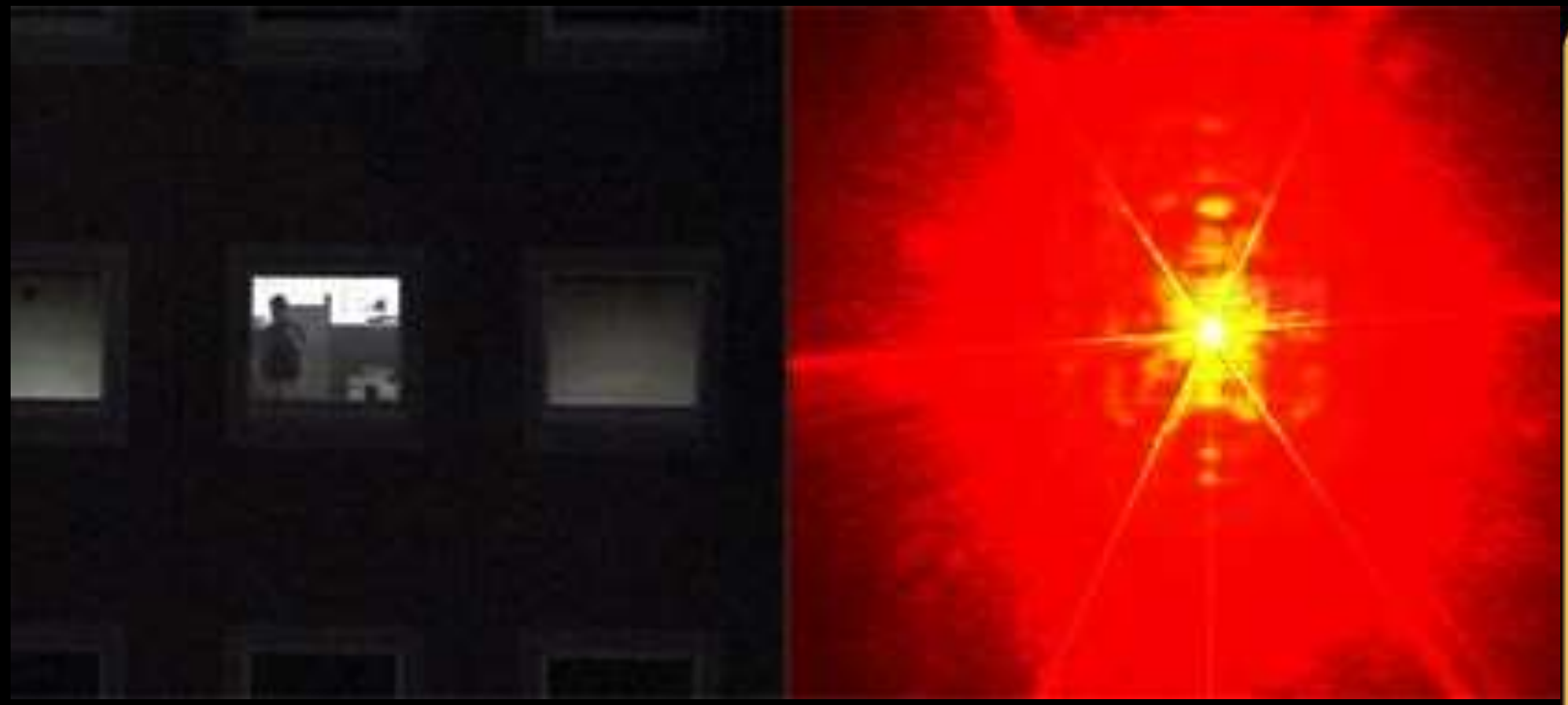


www.cctvcamerapros.com

IP cameras (and security systems) …(and the Internet)

IP Camera + Internet + Weak/Default Creds =

Blinding a security camera with a laser



www.naimark.net

You say convenience…

securestate.com

Oh hai! Come on in!

Yes, we have bypass!

- Video removed

Motion detector tricks

- Slide a notebook under the door
- Or…


I'M DETECTING
MUCH WIN
IN THIS SECTOR

More thoughts on doors and locks

- Good locks on bad doors = BAD
- Bad locks on good doors = BAD
- Master keys are great
  - Unless you rekey once in every never
- Cheap padlocks can be shimmed or picked easily

You say keypad…

- Cheaper than a badge system
- Convenient for sharing code between multiple employees
  - But you have to change the code when employees leave
- Analog keypads don’t have brute forcing detection capabilities
- But, they can leak information about the code…

www.schneier.com

Hrm… I wonder what the code is?

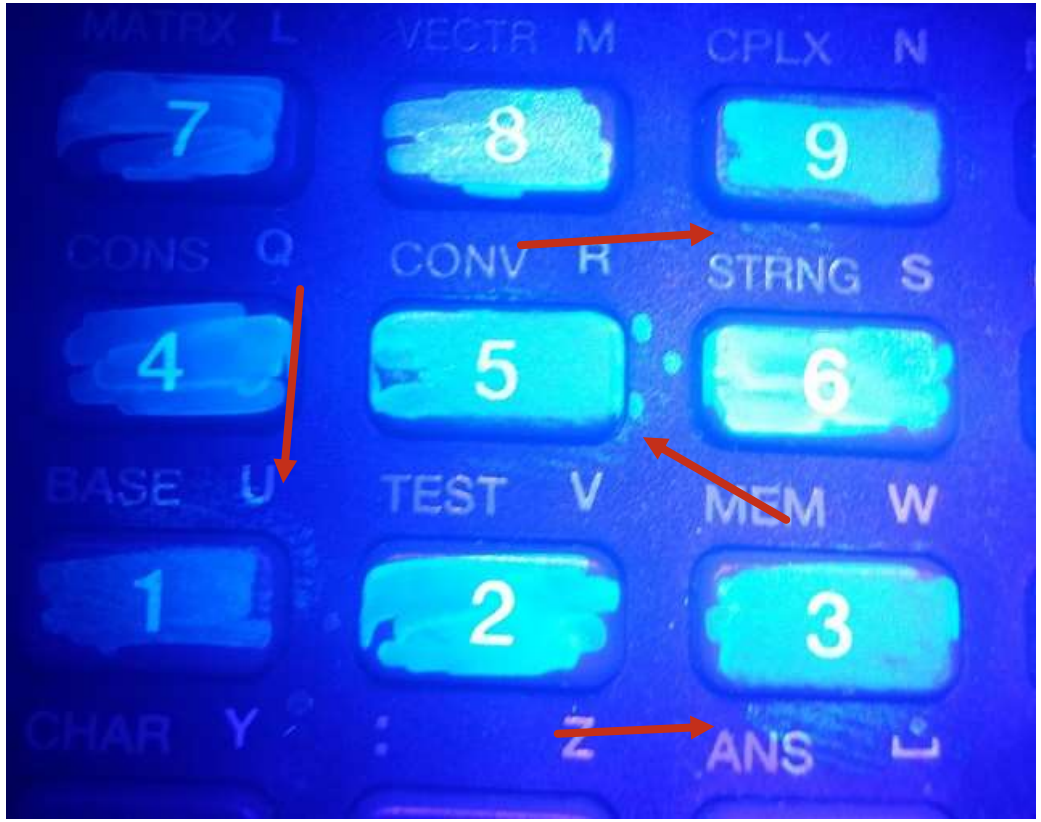

1 2 3
4 5 6
7 8 9
* 0 #

I wonder why those buttons are so shiny…

www.schneier.com

Fun with a black light

Fingerprints from UV pen ink



Fingerprints from highlighter

Attacking biometric systems

- Biometric signatures (and/or pins) are stored on your access card!
  - If I can clone your card, I can just put in my own fingerprint/pin
- Fingerprints can be duplicated

Attacking biometric systems

Defending against biometric attacks

- Live tissue verification
  - Looks for heartbeat and body heat
- Iris and retina scanners

Escalation

- Segmentation is important
  - Perimeter – fencing, gates, exterior entrances
  - DMZ – reception/receiving areas, common areas
  - Core – majority of office area
  - VLANs – higher security than core areas
    - Computer room, network closet, document storage, drug storage, trade secrets, etc.
- Moving from lower security area to higher security area
  - Controls commensurate with sensitivity of asset
- False-ceilings adjacent to higher security area
  - Walls should extend from floor to actual ceiling

Detection gives you the upper hand

- Sensors
  - Door open, glass break, motion, infrared, acoustic, vibration, pressure
- Monitor badge system for brute force attacks
- Cameras can help identify intruders and what was taken
- Test your systems regularly

Final thoughts

- Look at your facility in a new light
  - Are your doors installed properly?
  - How are you locks looking?
  - What about those keypads?
  - Don’t forget about cameras!

Other Resources

- Videos
  - http://www.irongeek.com/i.php?page=videos/derbycon4/t110-advanced-red-teaming-all-your-badges-are-belong-to-us-eric-smith
  - http://www.irongeek.com/i.php?page=videos/derbycon3/3303-how-can-i-do-that-intro-to-hardware-hacking-with-an-rfid-badge-reader-kevin-bong
  - http://www.youtube.com/watch?v=me5eKw6BP8g
  - http://www.irongeek.com/i.php?page=videos/derbycon4/t540-physical-security-from-locks-to-dox-jess-hires

- Other Resources
  - http://www.aijcrnet.com/journals/Vol_3_No_10_October_2013/12.pdf
  - http://resources.infosecinstitute.com/physical-security-managing-intruder/
  - http://www.slideshare.net/jemtallon/cissp-week-26
  - https://www.defcon.org/images/defcon-13/dc13-presentations/DC_13-Zamboni.pdf
  - https://ourarchive.otago.ac.nz/bitstream/handle/10523/1243/BiometricAttackVectors.pdf
  - https://blog.netspi.com/ada-requirements-opening-doors-for-everyone/

Credits

- Chris Nickerson, Eric Smith, Joshua Perrymon – Lares Consulting
- Dave Kennedy - TrustedSec
- SecureState
- Tim and Jem Jensen

Any questions?

- msaunders.sec@gmail.com
- @hardwaterhacker
- http://hardwatersec.blogspot.com/