Mason Competitive Cyber

Physical Security, Lockpicking, and RFID

News since last meeting

- Indiana hospital paid $55k for ransomware despite having backups
  - Didn’t want to go through effort
  - SamSam
  - Open RDP

Olympic Destroyer Malware

- Malware at 2018 Olympics opening ceremony
  - Crashed internal servers and WiFi
  - Don’t know how patient 0 compromised yet

1) Steals browser credentials. Steals system credentials with technique similar to mimikatz.
    i) mimikatz gets plaintext passwords from memory
    ii) procdump lsass.exe + mimikatz
2) Checks ARP table + uses WMI to find hosts
    a) PsExec w/ harvested credentials

3) Destroys Stuff
    a) Deletes backups, shares, event logs
    b) Disables all windows services, no recovery console
    c) Shuts down

Upcoming Competitions & Events

- Cyber Fusion
  - Feb 23rd-24th
  - VMI (registration locked)

- BSides NOVA CTF
  - Feb 24th 8:30am-4pm
  - In-person
  - Herndon

- Cryptoparty (cryptography workshop + CTF)
  - The HUB
  - March 3rd 10:30am - 6:00pm

Physical Security, Lockpicking, and NFC

- How is this related to cyber security?
  - Similar thought process
  - Lockpicking villages

- Legal Disclaimer
  - Don’t do anything illegal
  - If you do, you didn’t learn it from me

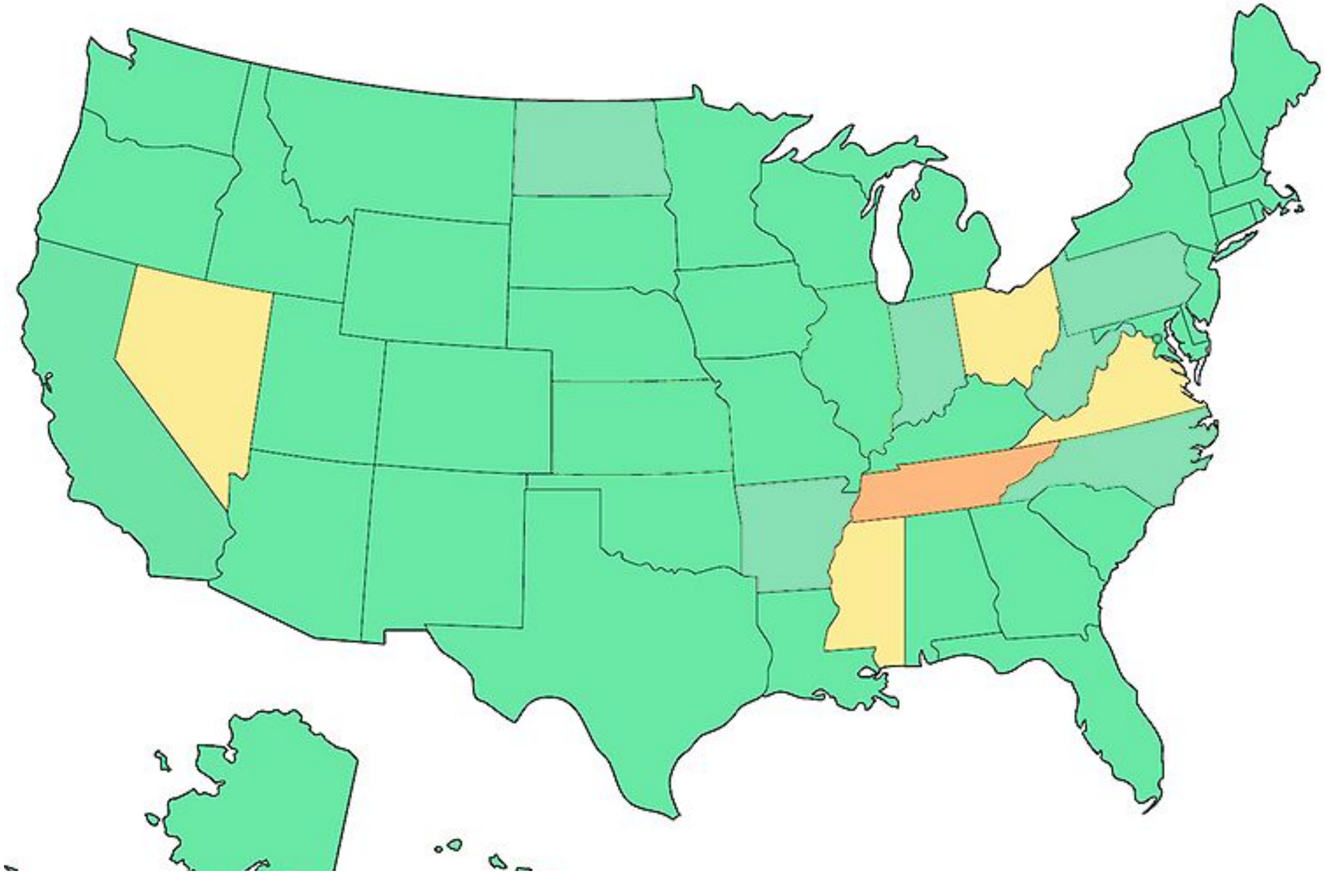
- Legit Reasons for learning this
  - Pen testing
  - Locksmithing
  - Securing RFID

Out of Scope

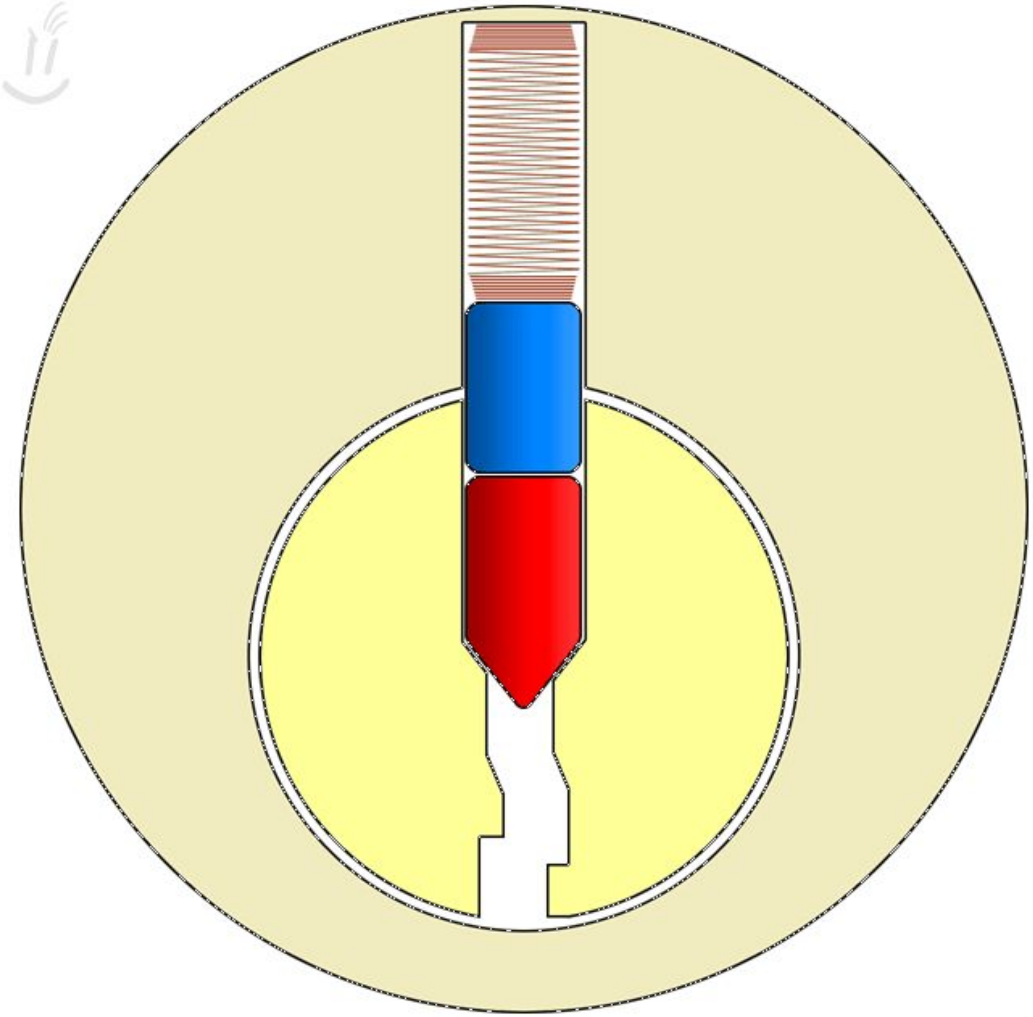
- Parkour/ninjas climbing buildings
- Mission Impossible $500,000 lock picking devices

Is it legal to lockpick?

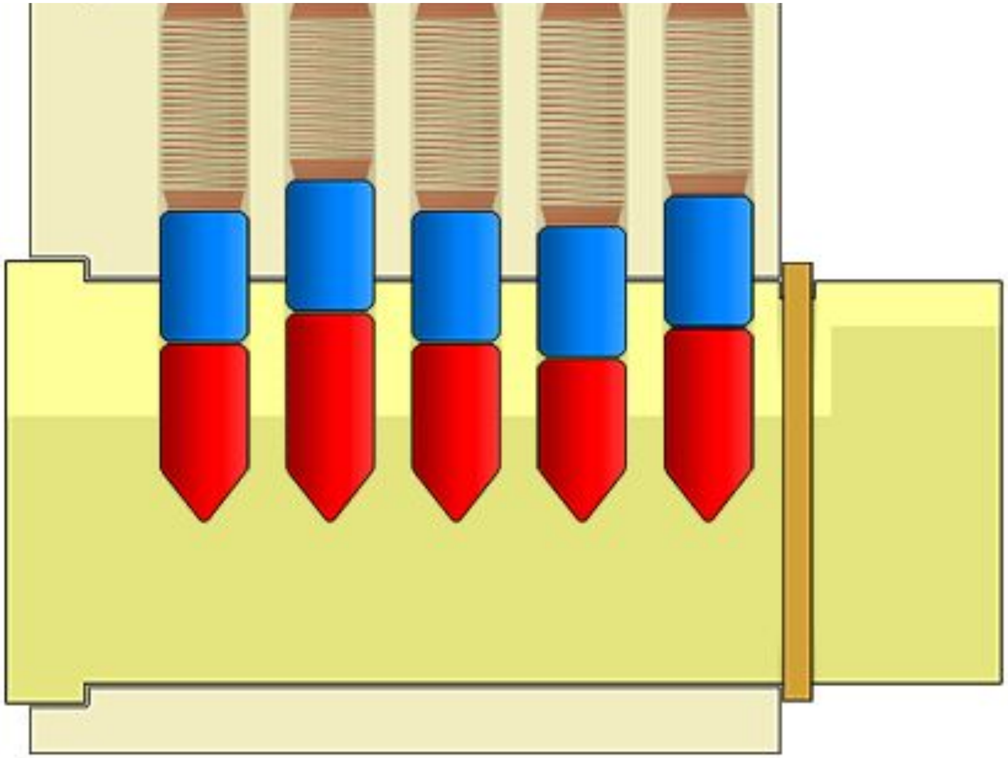
- Mostly legal. Some states (VA) criminal intent unless you have a reason



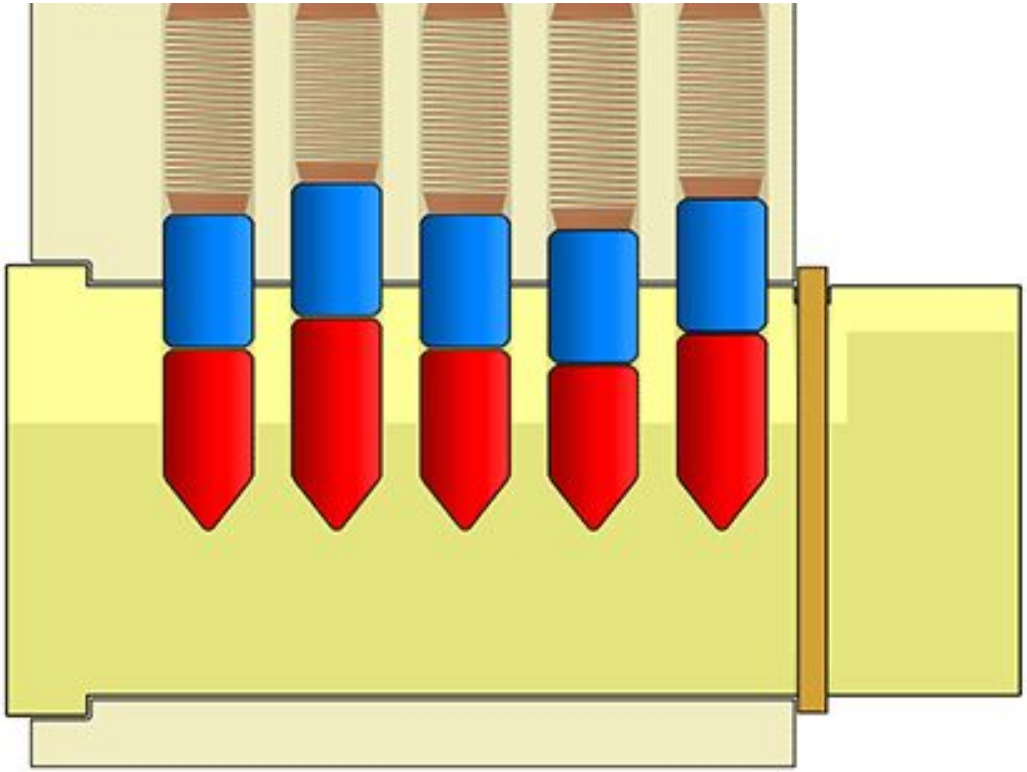
Picking: how a key opens a lock



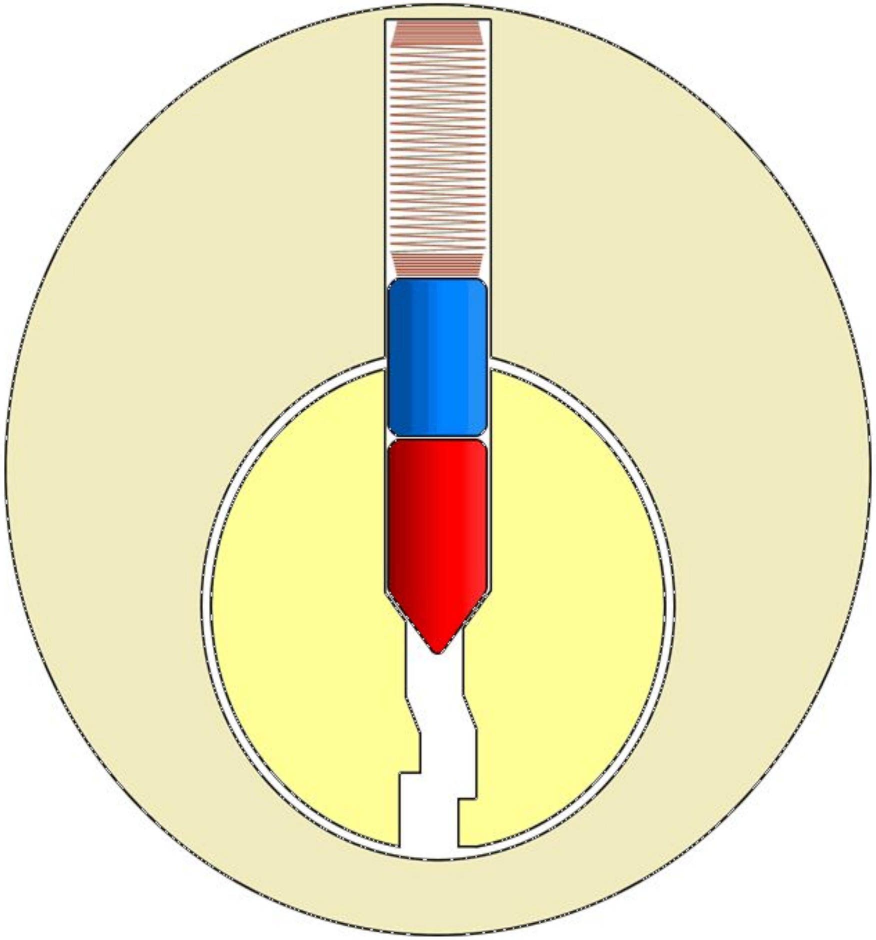
Picking: how a key opens a lock

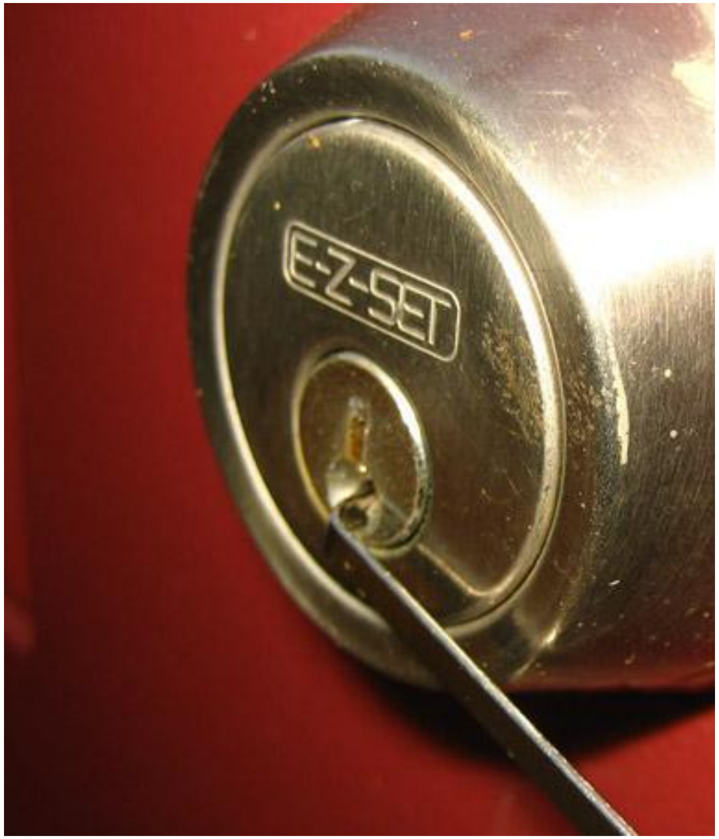


How Lockpicking Works



Tension Wrenches

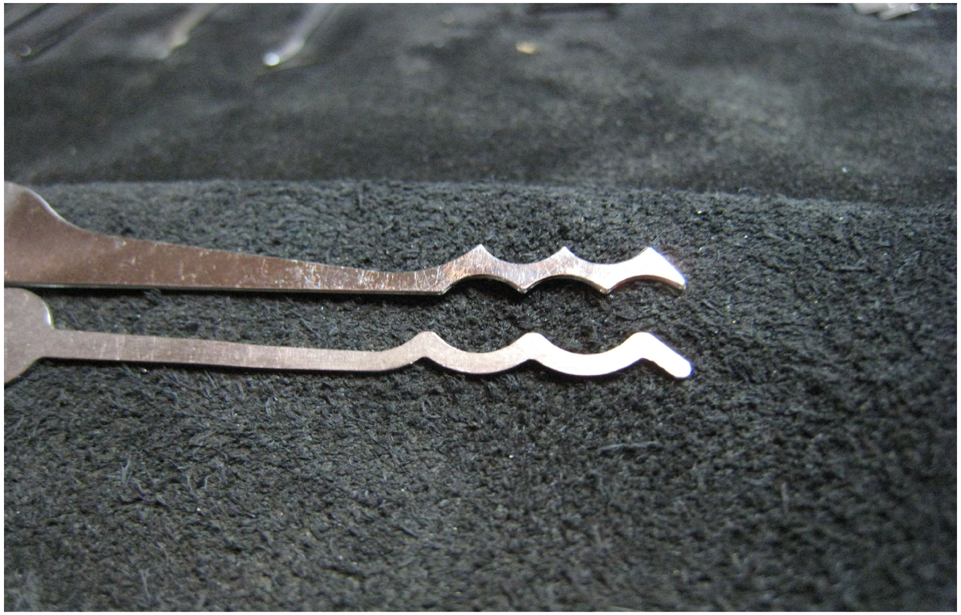




Lockpicking Tips

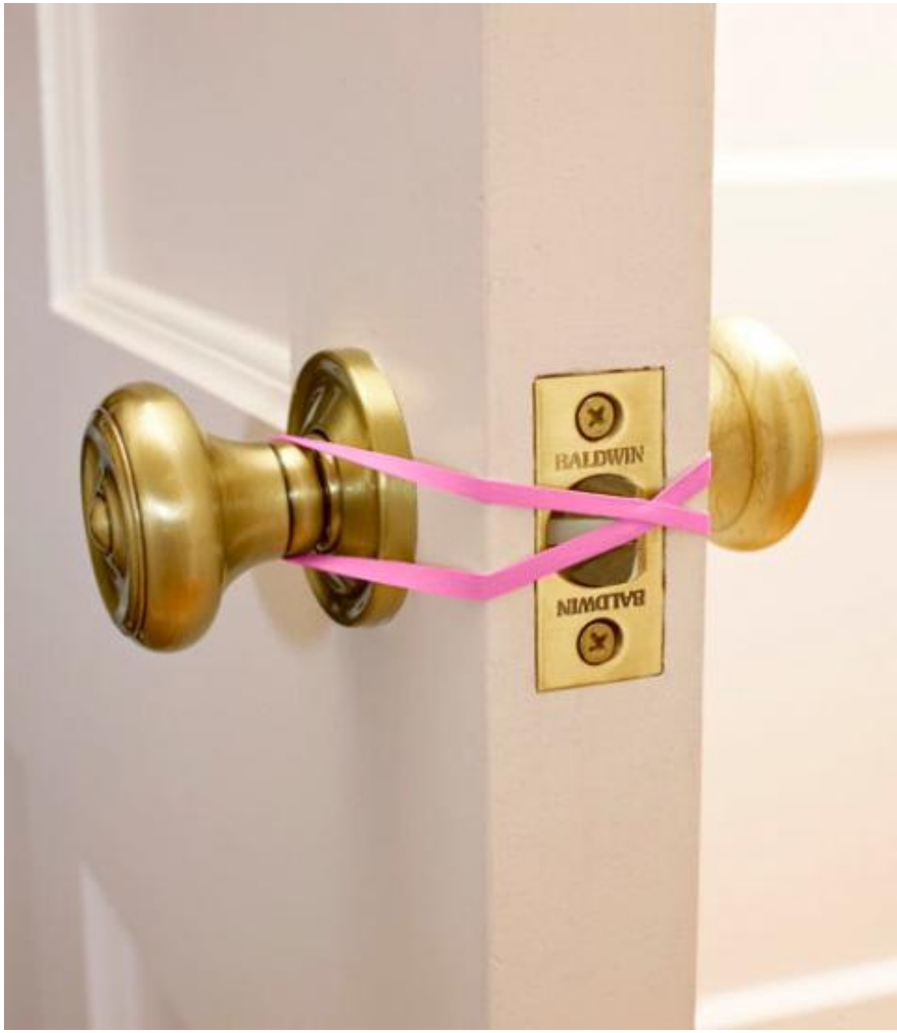
- Use a rake
  - Faster
  - Works on locks with fewer pins

- Remember which way the lock turns



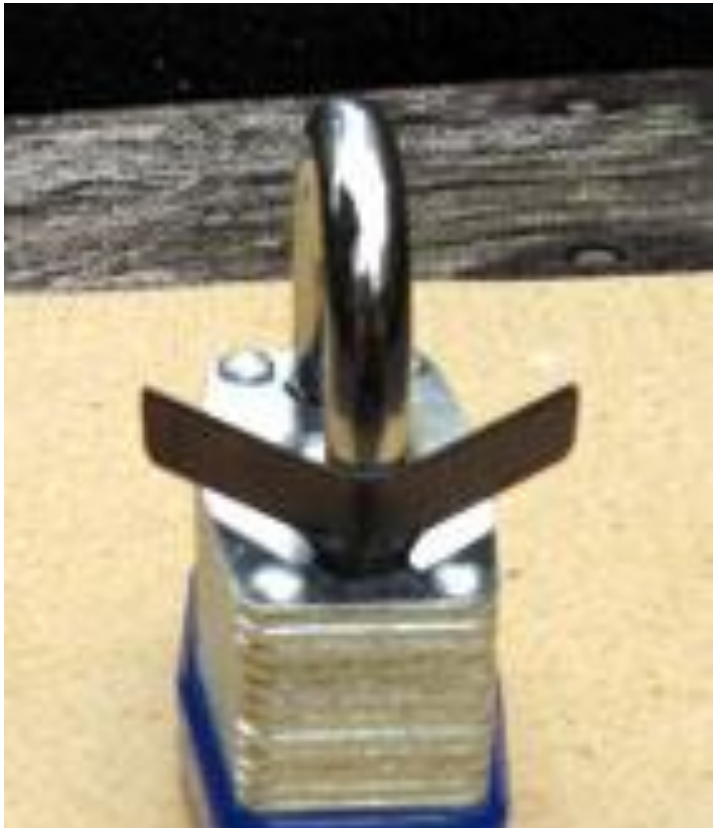
Dirty Tricks: Persistence

- Rubber band
- Tape part of used gift card to inside of door
- Prop door slightly open



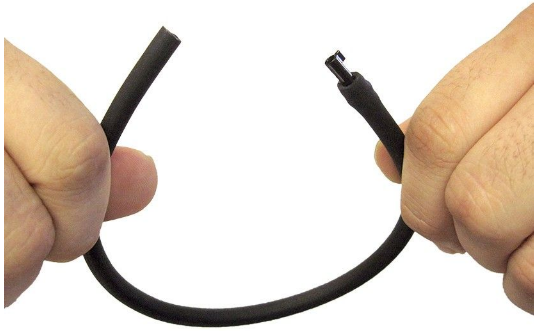
Shimming

- Shimming = jamming thin piece of metal or plastic inside lock



Handcuffs

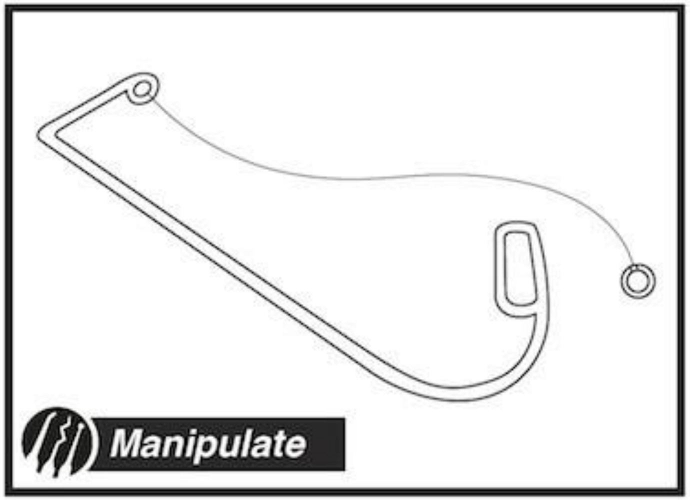
- Key (lmao)
- Pick
- Shim
- Break



Combination Locks

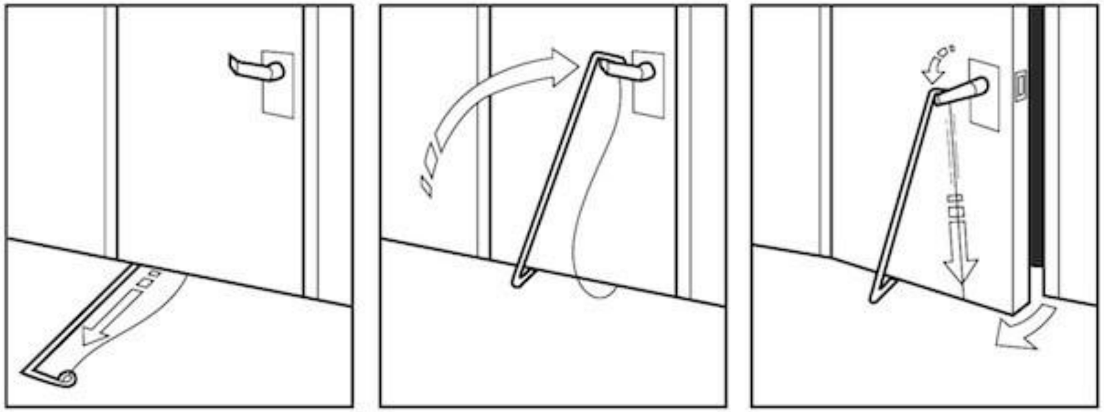
- Listening for a pin drop
- Feeling for a pin drop

Hotel Doors



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

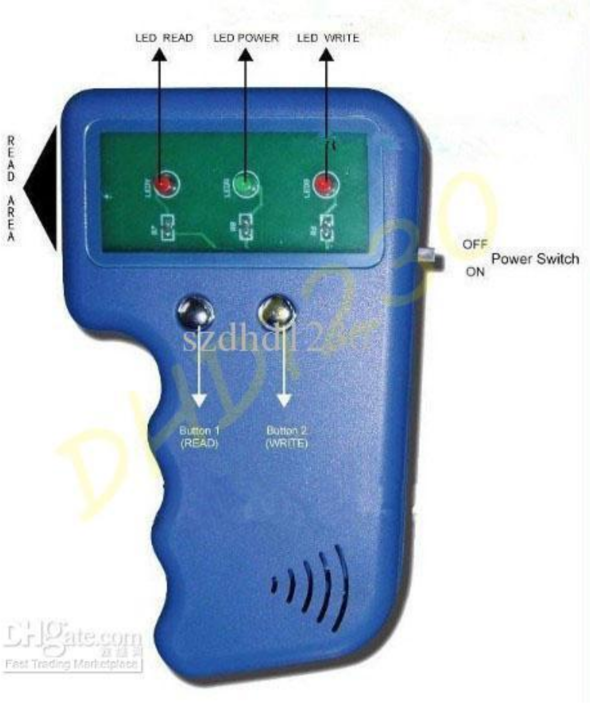
Step 3:
Pull down on cable to open the door

Magnetic Card Locks

- Cloning

RFID Locks

- Radio Frequency Identification (RFID)
- Proximity Cloning
- NFC = high frequency



125kHz

Car Keys

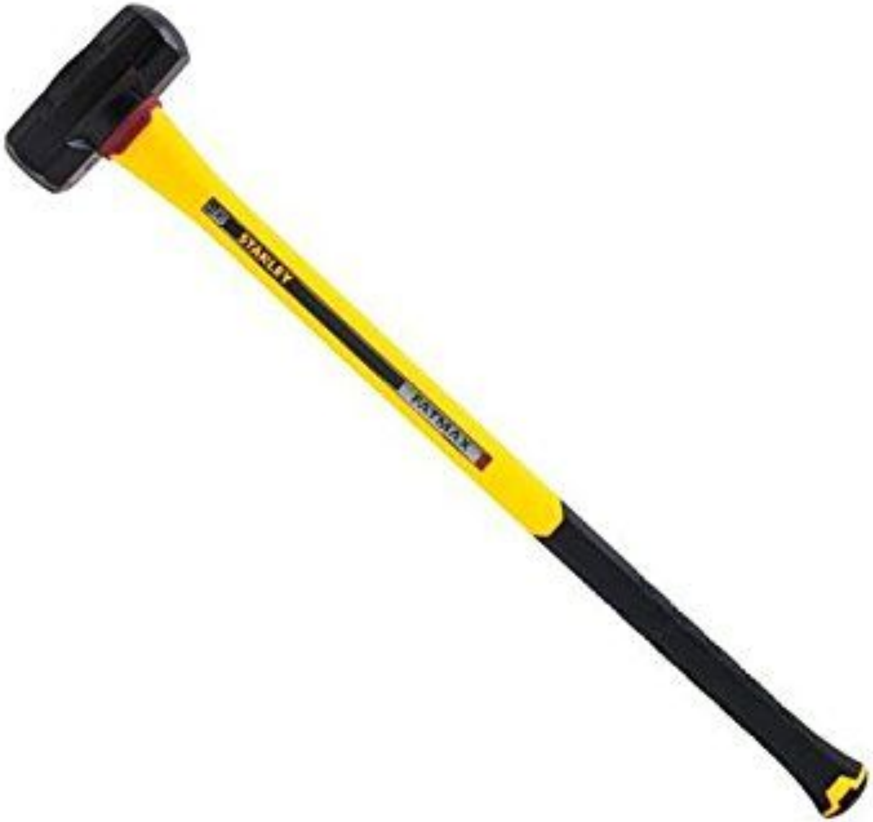
- Rolling Codes
  - Pseudorandom algorithm, secret seeds

- Replay Attack
  - DEFCON: Drive It Like You Hacked It

- Amplification Attack
  - 2016 discovered by German security firm
  - Drop an amplifier near the key fob
  - Have a strong receiver connected to amplifier

Ol’ Reliable

- Super complex 1337 lock picking tool



Security Cameras

- Shodan
  - BlackHat talk: Exploiting Network Surveillance Cameras Like a Hollywood Hacker

- Ethernet Hacking
  - DEFCON 23: Looping Surveillance Cameras through Live Editing

- IR Blinding
  - People can’t see infrared, many cameras can

TOOOL

- The Open Organisation Of Lockpickers
- 1st Wednesday of every month @ The Board Room
  - 21+

Practical Exercise

- Pick clear lock

- Training CTF
  - New web challenge (credit to Hung Mao Chen)
  - tctf.competitivecyber.club
  - collaborate

- GRIMM Crypto Challenge
  - #grimmchallenge

- Knowledgeable Members
  - Give a talk
  - Add to TCTF

Proud Sponsors

Thank you to these organizations who give us their support:

BATTELLE

It can be done™