Physical Security

Breaking and Entering:

a Tutorial

What will be covered

- Common security measures
- How to defeat them
- How to improve them

What will **not** be covered

- Hacking into the mainframe

Focus

"Any problem on Earth can be solved with the careful application of high explosives."

- Three types:
  - Surreptitious
  - Covert
  - Forced

I do teach explosives:
Tonight at **6** in **26-204**

Something to Remember…

- Never lose sight of the big picture:
  - Your goal is not to pick the lock
  - Your goal is to gain access

Social Engineering

- People like to talk
- People make mistakes
- Catch Me If You Can

Methods of Influence

- Ethos
- Pathos
- ~~Logos~~

Ethos

- Ethos
  - Acting
  - Lying
  - Confidence

Example:
Pretending to be an employee

Pathos

- Pathos
  - Sympathy
  - Trust
  - Power

Example:
Asking a favor of the janitor

Social Engineering is Powerful

- Any security measure can be defeated by a sufficiently skilled social engineer
- It is the most general method I will cover

A Building

- Goal: Gain access
- Problem: The **structure** of the building physically blocks you
- Find **vulnerabilities** in that structure

Structure

- Ducts

Structure

- Ducts
- Drop ceiling

Structure

- Ducts
- Drop ceiling
- Windows

Structure

- Ducts
- Drop ceiling
- Windows
- Gaps, above and below

Structure

- Ducts
- Drop ceiling
- Windows
- Gaps, above and below
- Utility shafts

Structure

- Ducts
- Drop ceiling
- Windows
- Gaps, above and below
- Utility shafts
- Doors

Breaking In

Skills

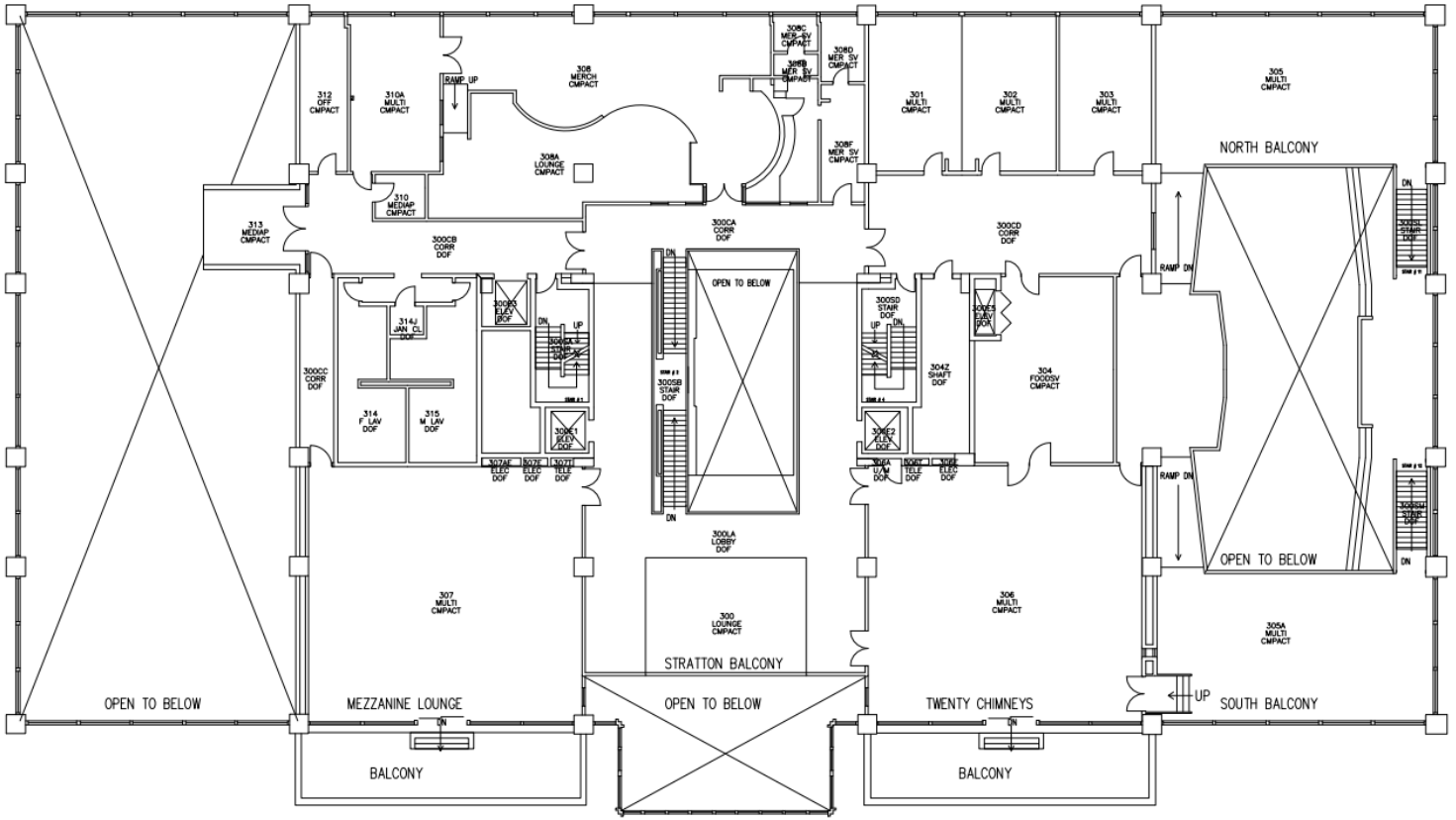
- Climbing
- Crawling
- Being a ninja

Tools

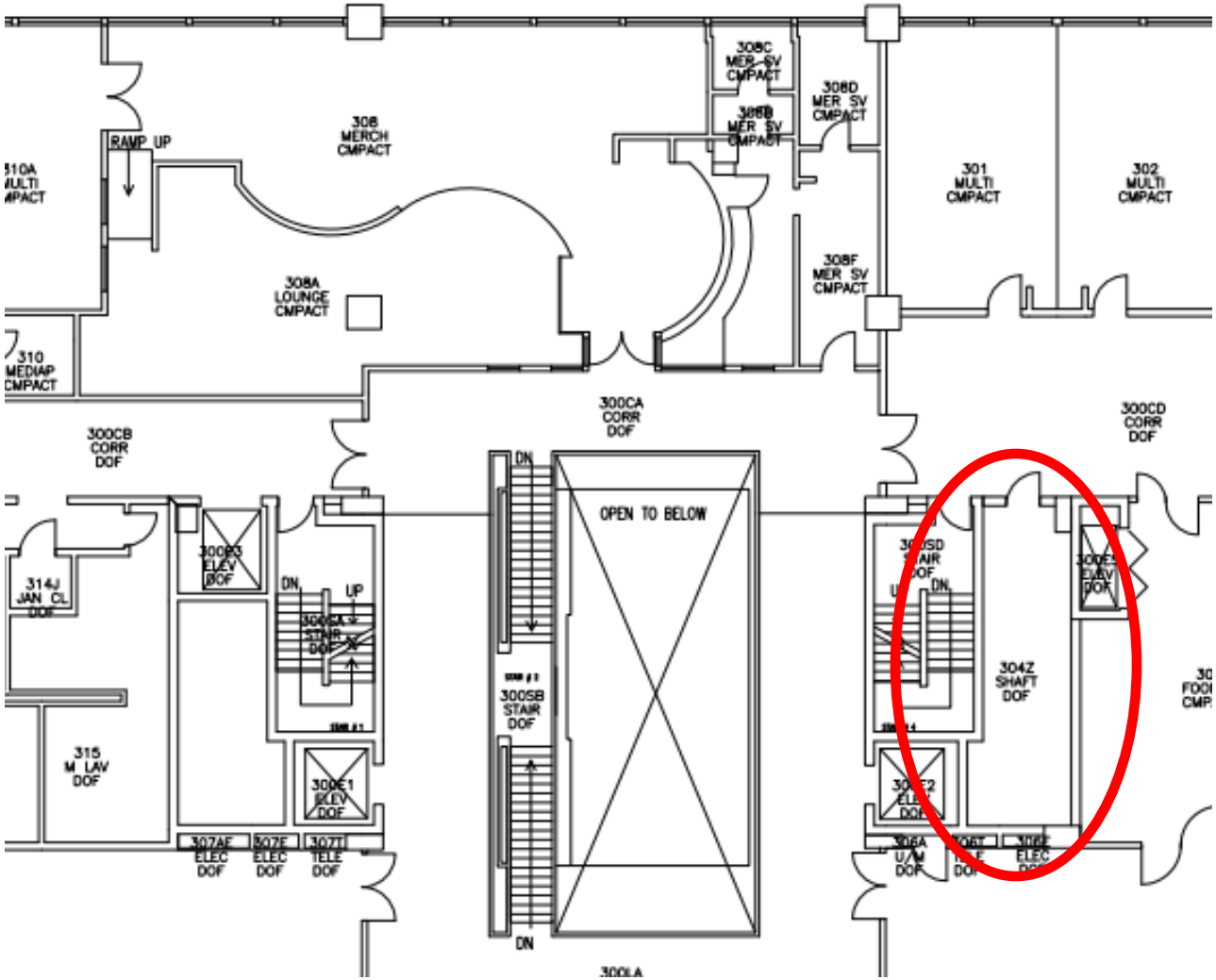
Screwdriver
Pliers
Knife
} Multitool
Headlamp

Breaking In

Floorplans



Breaking In


308C
MER SV
CMPACT
308B
MER SV
CMPACT
308D
MER SV
CMPACT
308
MERCH
CMPACT
RAMP UP
308A
LOUNGE
CMPACT
308F
MER SV
CMPACT
301
MULTI
CMPACT
302
MULTI
CMPACT
310
MEDIAP
CMPACT
300CA
CORR
DOF
300CB
CORR
DOF
300CD
CORR
DOF
OPEN TO BELOW
DN
UP
314J
JAN CL
DOF
315
M LAV
DOF
300SB
STAIR
DOF
304Z
SHAFT
DOF
307AE
ELEC
DOF
307E
ELEC
DOF
307TI
TELE
DOF
306A
U/M
DOF

Doors

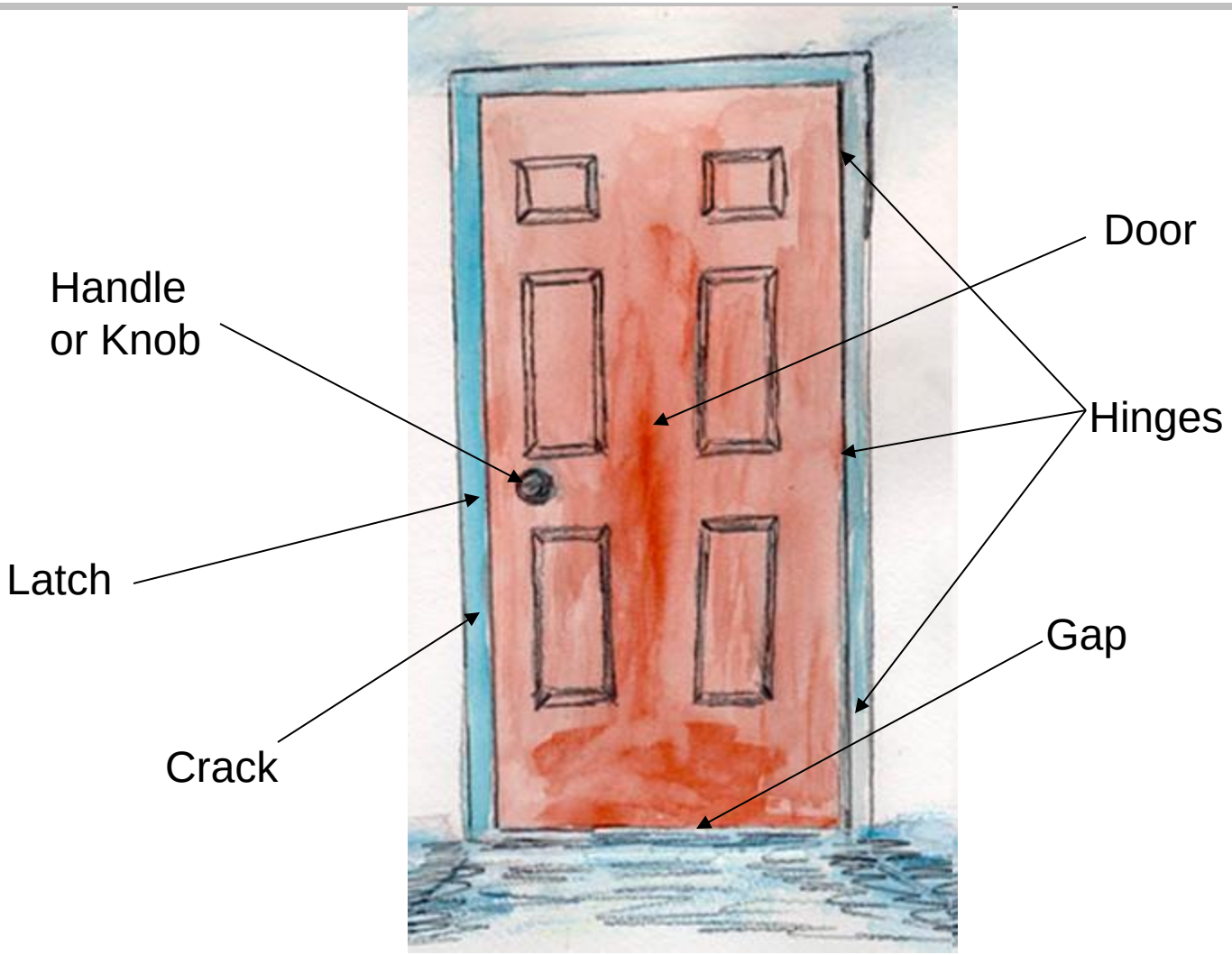
- Goal: Get through a door
- Problem: **Latch** prevents door from opening
- Find **vulnerabilities**

Compromising Doors

Q: What is the easiest way to get through a door to a secure area?

A: Walking through it

Doors



Breaking In

1. Walk through an open door
2. Get somebody else to open it
   - Knocking
   - Door surfing
3. Pull on it
4. Turn the handle

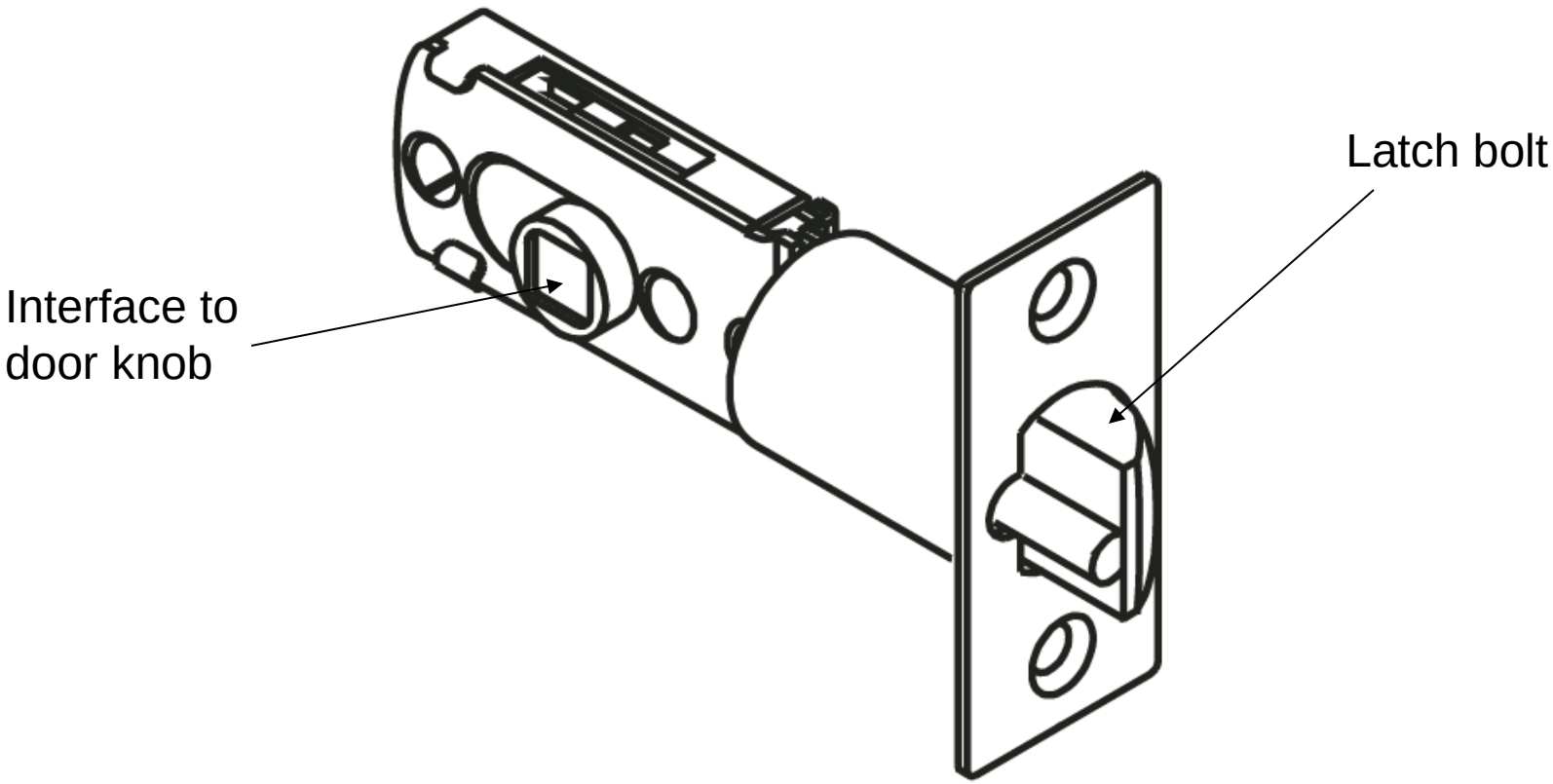
Okay, I've tried all of those
→ Exploit poor installation

- **Crack**: Prying it wider
- **Latch**: Carding and Sliding
- **Gap underneath**: Reach through and open from the inside
- **Hinges**: Removing the pins
- **Other features**: Exposed screws, vents

Card and Slide

- Exploits friendliness of latch

Latch



Spring latch

- Apply pressure to the end of the bolt
  - Or the angled face
- The bolt will retract
  - As if the door were closing
- The door can be pulled open

Dead bolt

- Does not have an angled face
- Is not susceptible to end pressure
  - Will not retract if you push on it

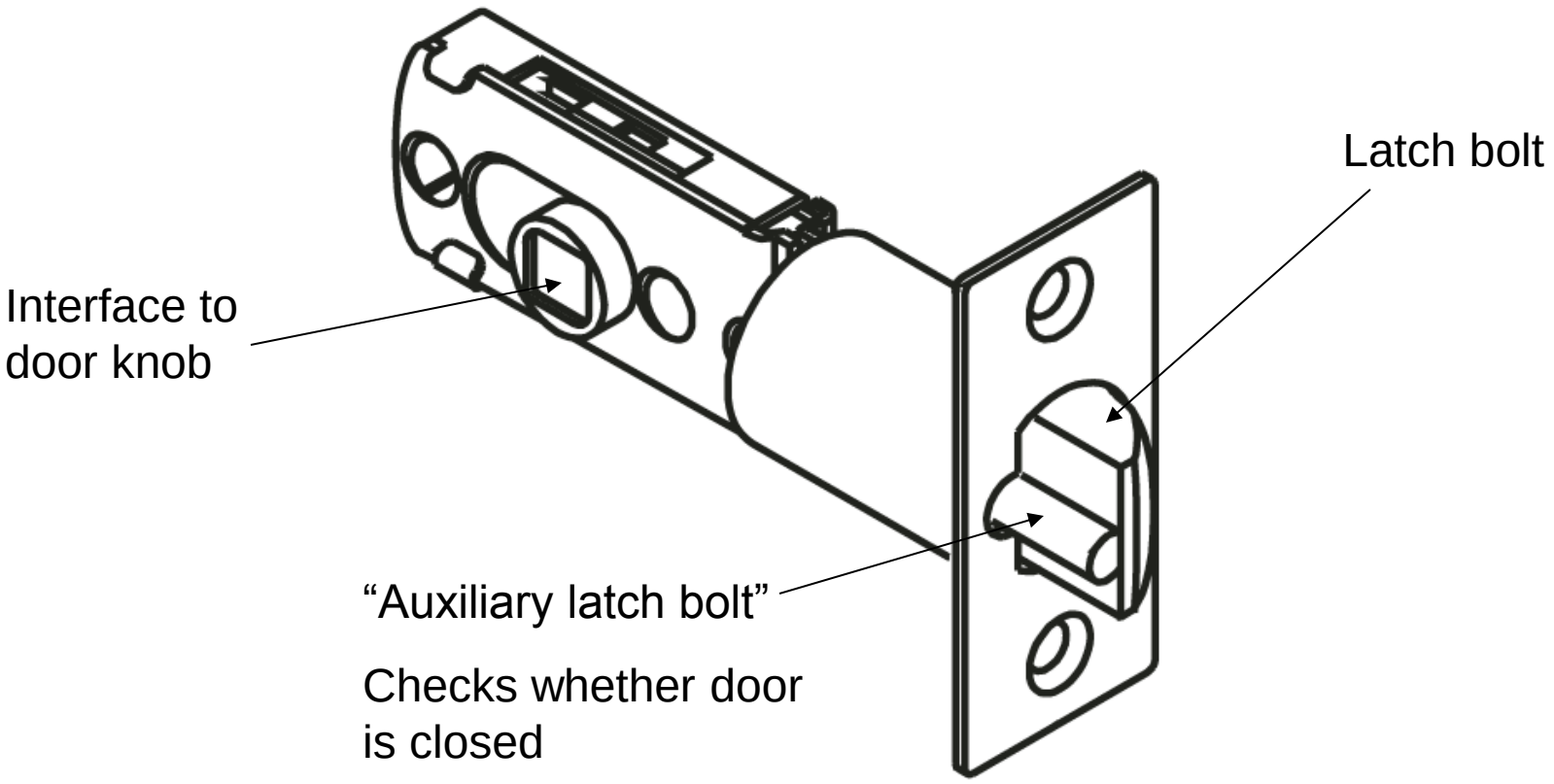
- Not susceptible to carding or sliding

Dead latch

- Combines both ideas
- Will retract freely when the door is open
- Will not retract when the door is closed
  - Except by the handle

- Not susceptible to carding or sliding
  - Unless it is broken or installed incorrectly!

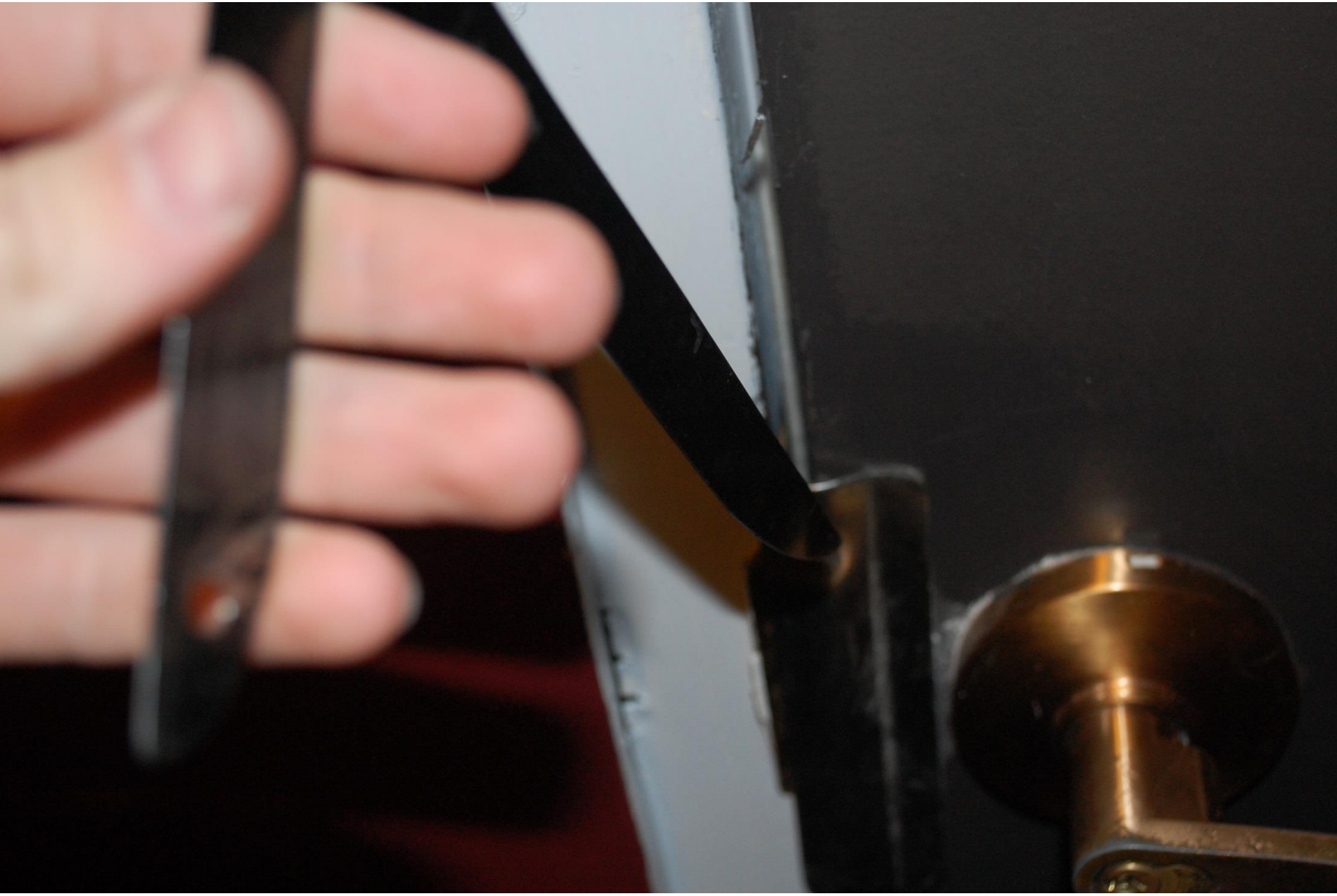
Latch

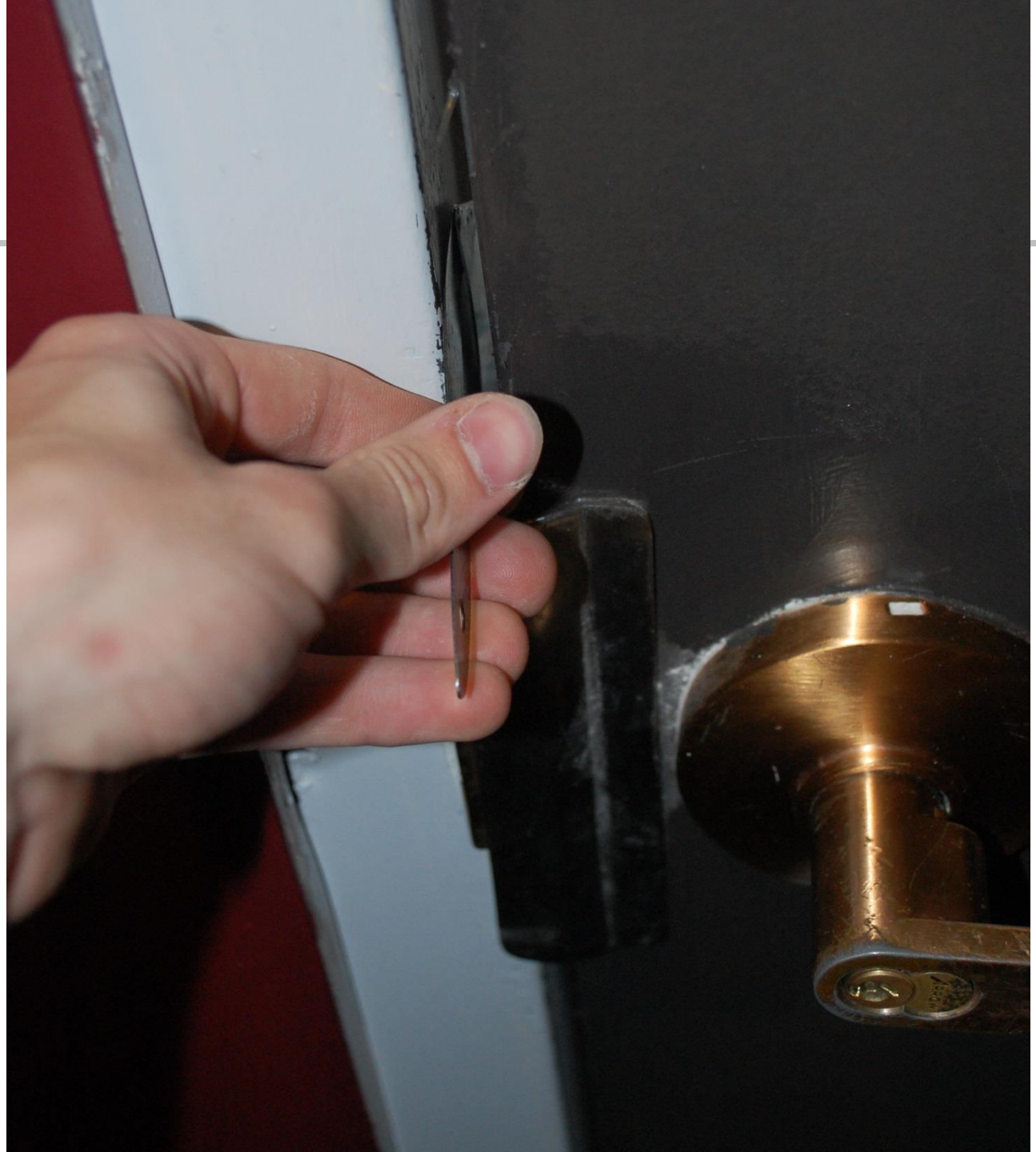

Latch bolt
Interface to door knob
“Auxiliary latch bolt”
Checks whether door is closed

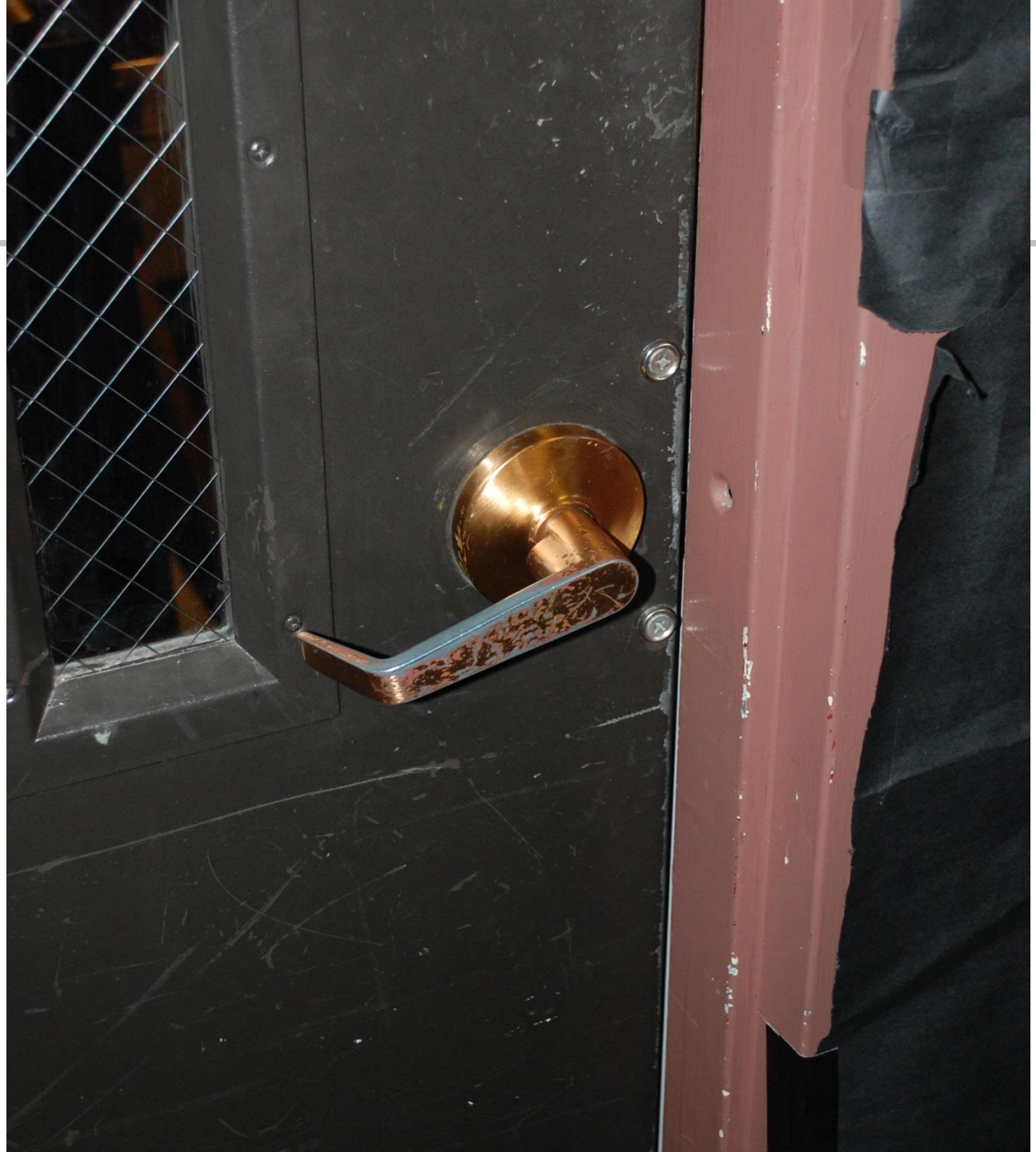
Sliding

- Insert slide into crack, behind latch
- (Optionally) Apply slight tension to the door
- Pull slide down and towards you
  - Depress latch
- Door opens


OH GOD YES
Our Milkshake Brings All the Boys to the Party
Saturday, 10pm
1E
Our Milkshake Brings All the Boys to the Party
Saturday, 10pm
1E





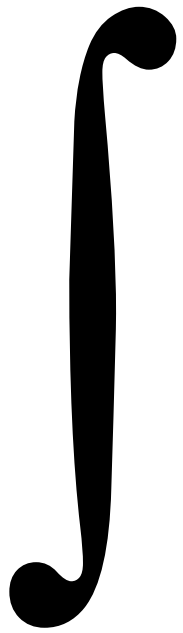


Carding

- Insert card into crack
- Work card around the shape of the jamb
- (Optionally) Apply slight tension to the door
- Push card into latch
  - Depress latch
- Door opens

Integral

- Opens door from inside
  - Turning handle

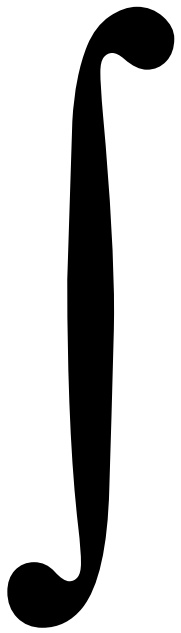


Integral

- Insert integral through gap below door
- Swing up onto door handle
- (Optionally) Apply slight tension to the door
- Pull down
- Door opens

Integral

- Opens door from inside
  - Turning handle or knob



Breaking In

1. Walk through an open door
2. Get somebody else to open it
3. Pull on it
4. Turn the handle
5. Crack / Card / Slide / Integral
6. Hinges / Screws / Vents
7. Lock Cylinder

The 80-20 rule

- You can now probably get into about 80% of “secure” places
  - And we haven’t even talked about anything too complicated yet

Locks

- Mechanical

Locks

- Mechanical
- Optical

Locks

- Mechanical
- Optical
- Radio-Frequency

Locks

- Mechanical
- Optical
- Radio-Frequency
- Magnetic

Locks

- Mechanical
- Optical
- Radio-Frequency
- Magnetic
- Tactile

Locks

- Mechanical
- Optical
- Radio-Frequency
- Magnetic
- Tactile
- Biological

Attacks

- Theft of the physical key
- Listening for the code during a transaction
  - “Sniffing”
- Reading the code from the key
  - “Snooping”

Common Mechanical Locks

- Pin tumbler

Common Mechanical Locks

- Pin tumbler
- Wafer tumbler

Common Mechanical Locks

- Pin tumbler
- Wafer tumbler
- Warded

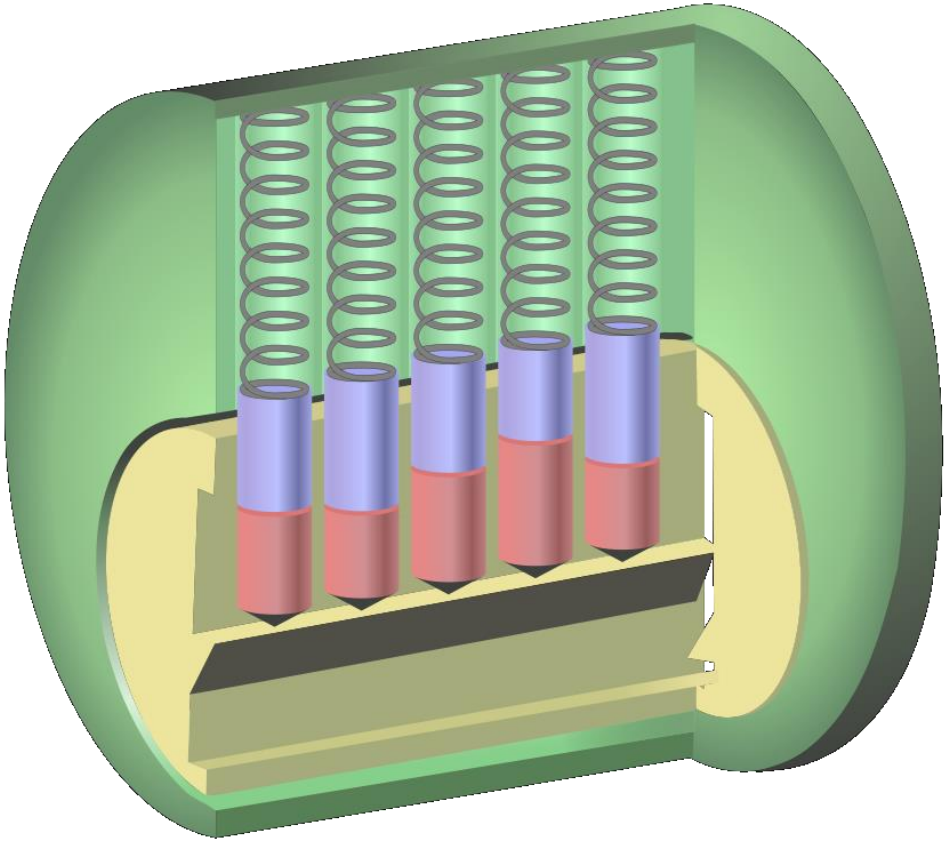
Common Mechanical Locks

- Pin tumbler
- Wafer tumbler
- Warded
- Tubular

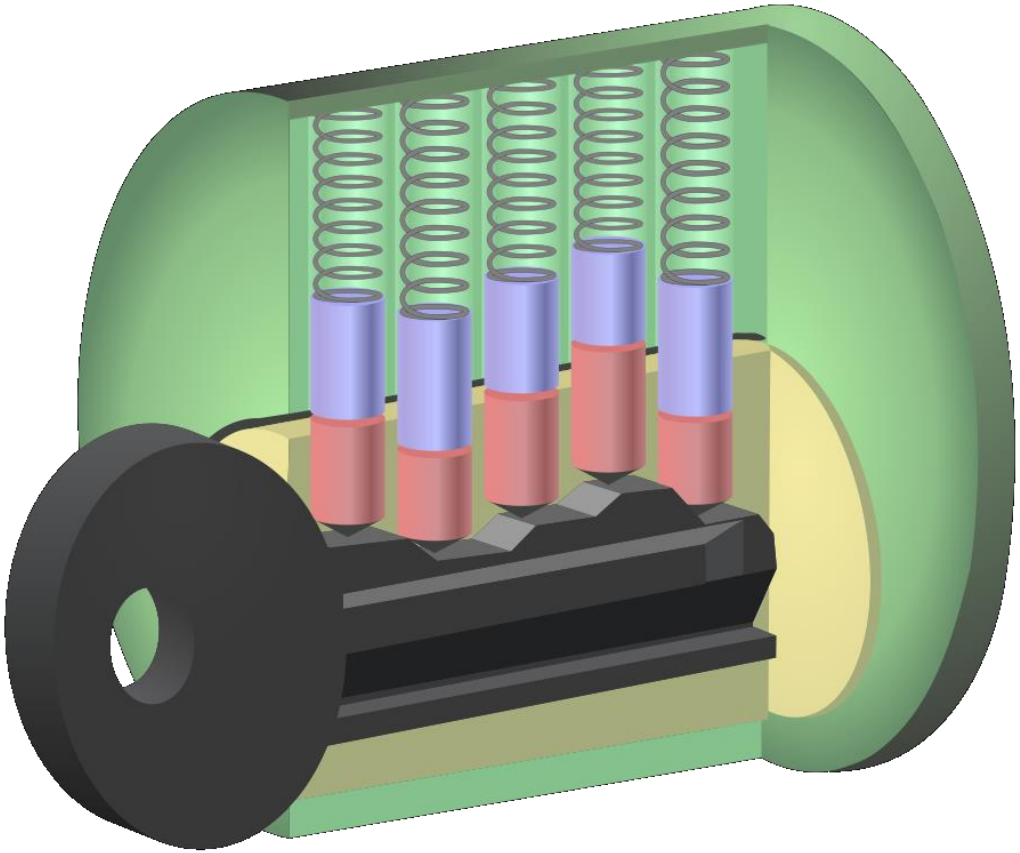
Common Mechanical Locks

- Pin tumbler
- Wafer tumbler
- Warded
- Tubular
- Disc detainer

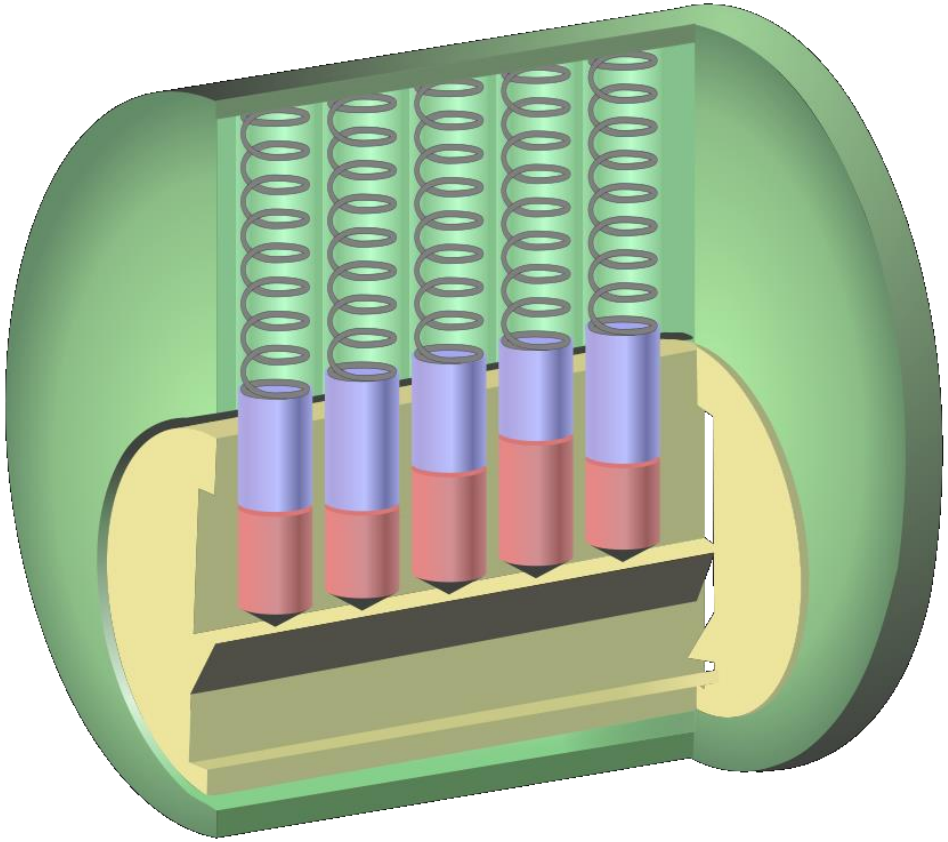
Pin tumbler



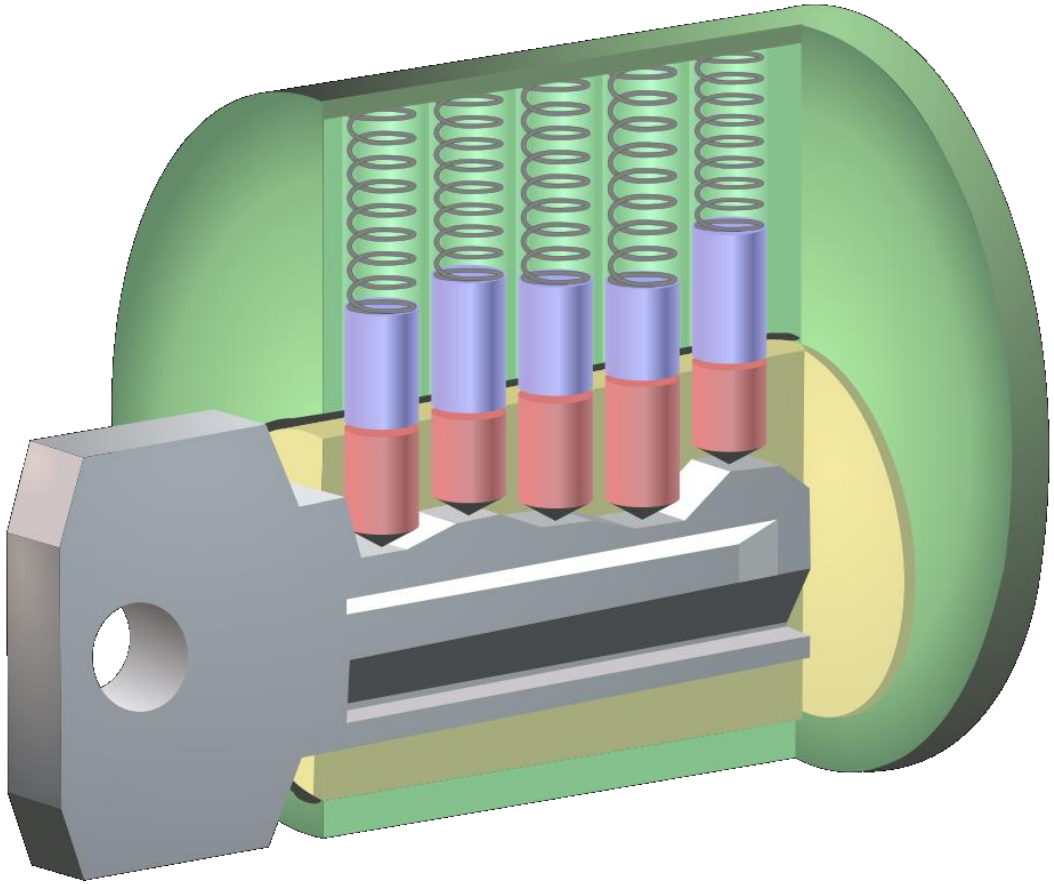
Pin tumbler



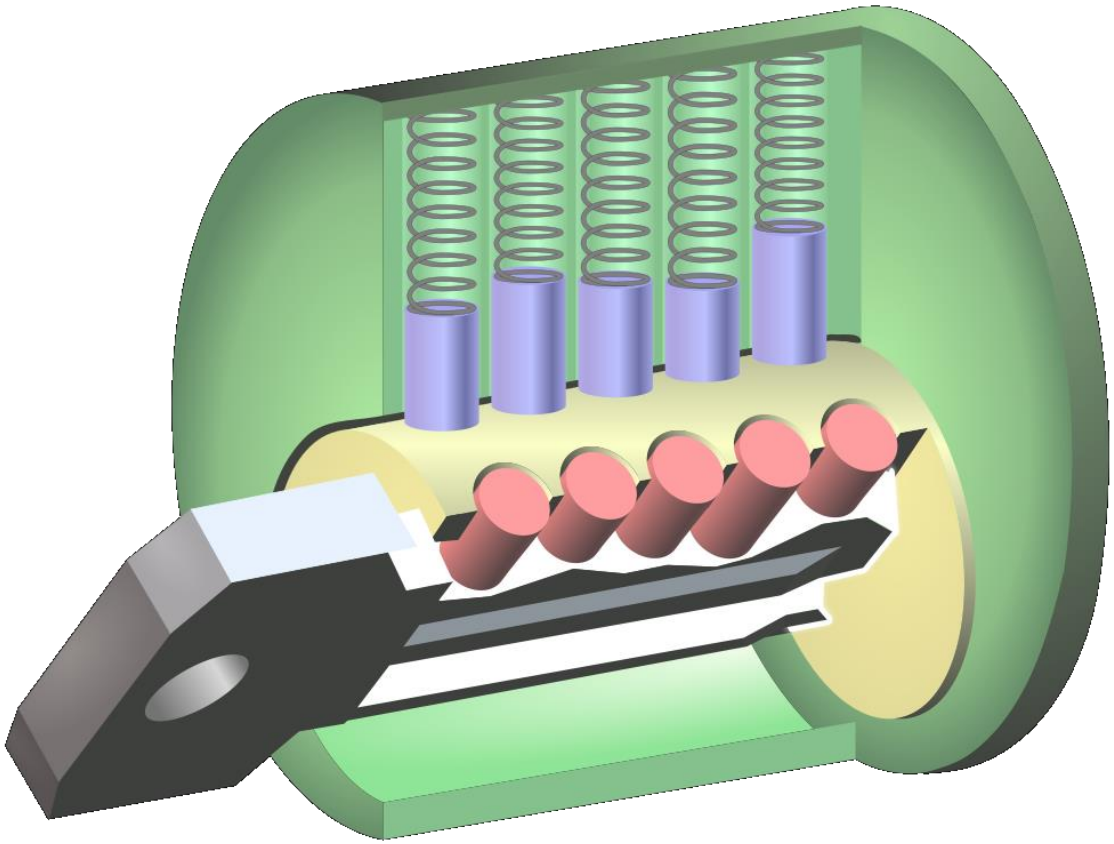
Pin tumbler



Pin tumbler

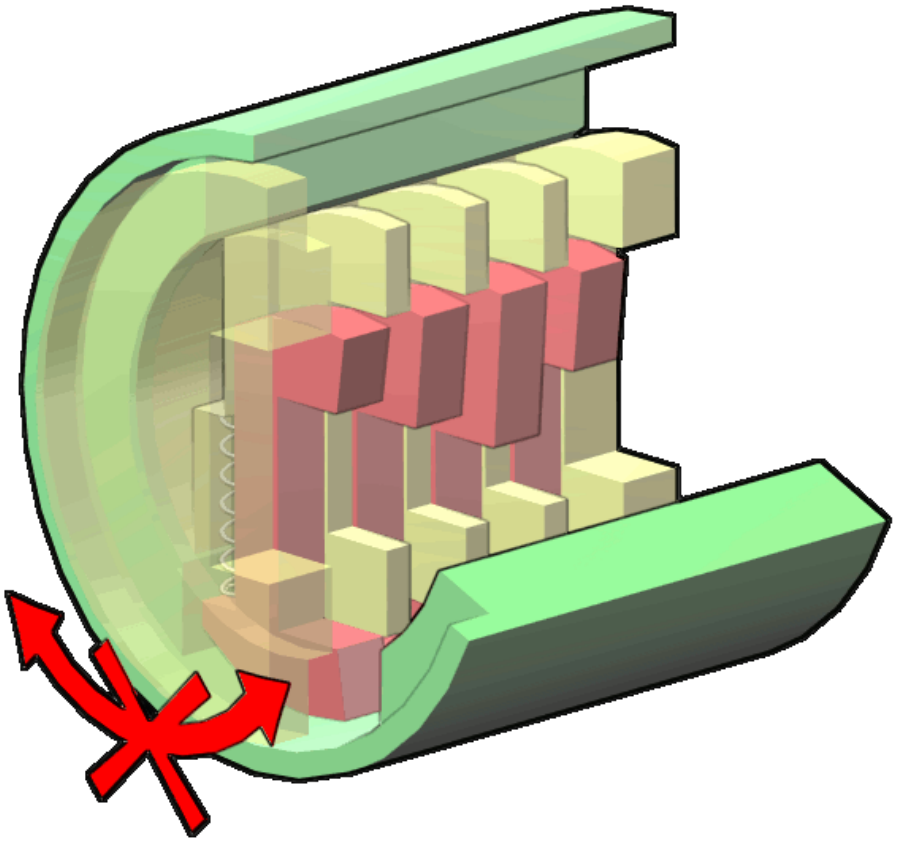


Pin tumbler

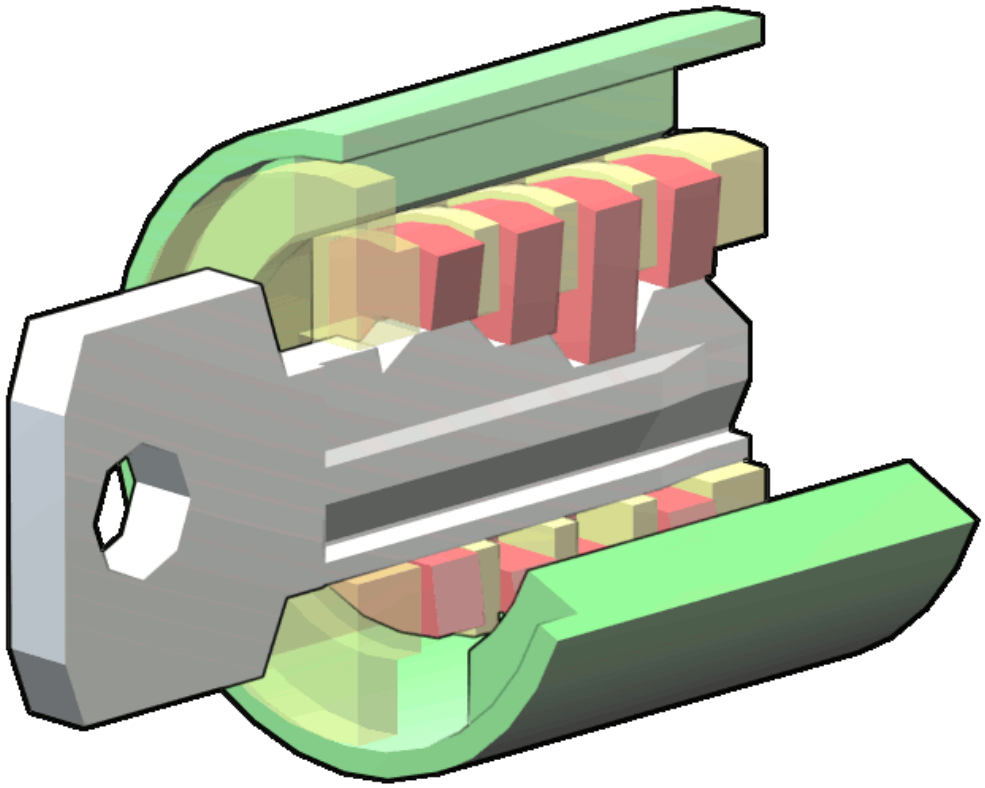


Pin tumbler

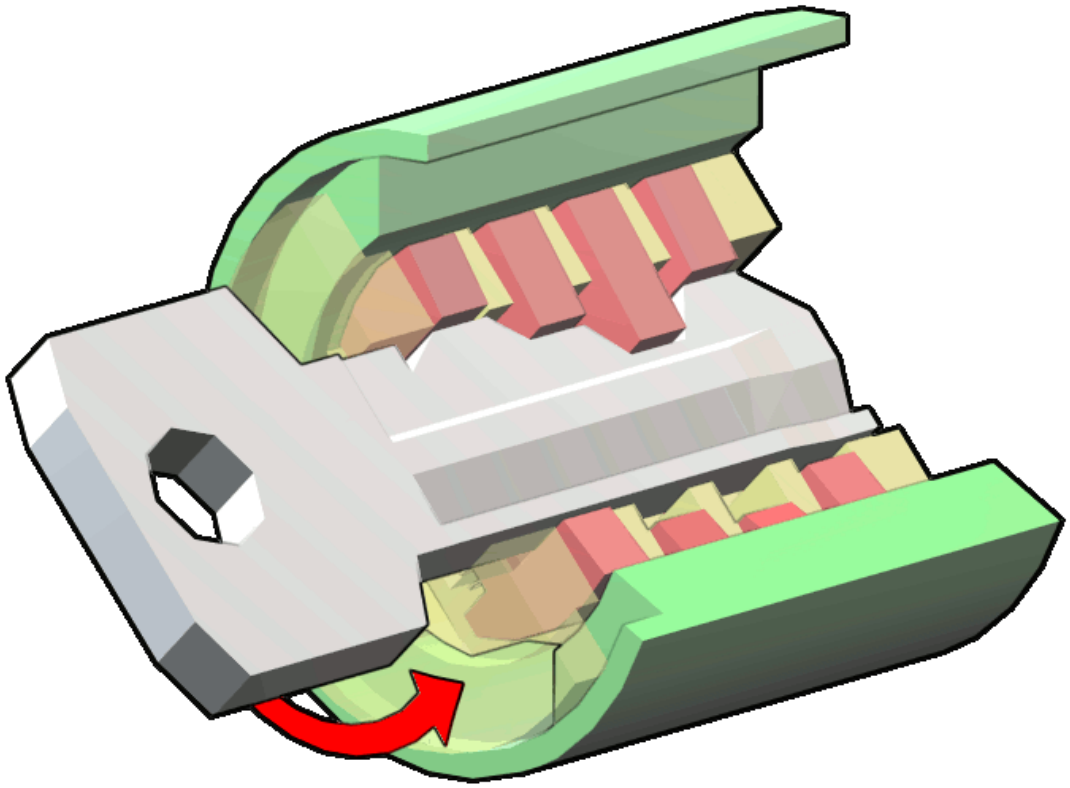
Wafer tumbler



Wafer tumbler



Wafer tumbler



Vulnerabilities

- Careful Manipulation
  - Move the pins or tumblers slowly until they are all at the shear line
- Chaotic Motion
  - Apply enough energy to the pins or wafers that they bounce around chaotically and at some point form a gap at the shear line

Careful Manipulation

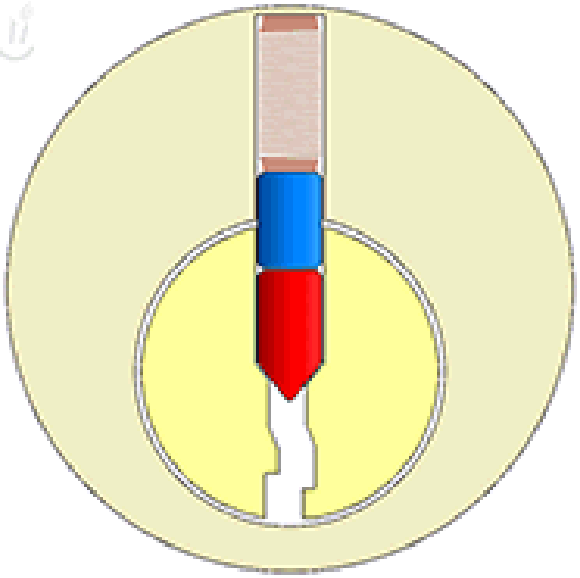
- Picking
  - Exploit mechanical defects to isolate each pin
  - More on this soon
- Impressioning
  - Use binding action at the shear line to mark a key
  - Click

Chaotic Motion

- Pick gun
  - Vibrate the pin stacks until they all split at the shear line
  - Click
- Bumping
  - Apply energy to the pins using a specially cut key and a hammer, causing them to bounce and eventually split at the shear line
  - Click

Lockpicking

- Imagine a one pin / one wafer lock



Lockpicking

- Imagine a one pin / one wafer lock
- Add more pins
  - Apply tension
  - Due to mechanical defects, one pin stack will bind
  - “Set” the pin stack
    - Pinch-off effect at the shear line
  - Another pin stack will bind
  - Set every pin stack
- Isolate each pin stack so that picking a 4-pin lock becomes picking 4 one-pin locks

Lockpicking Wafer Locks

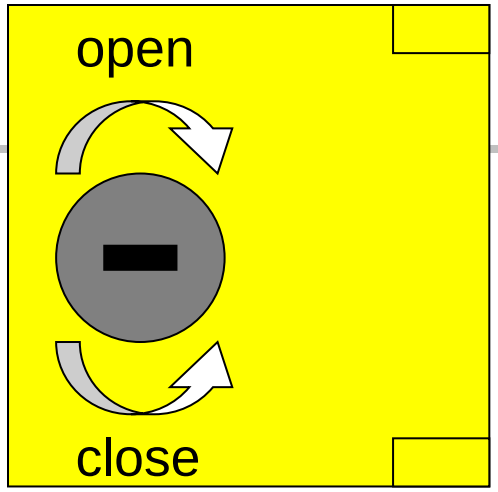
- After a wafer sets, the plug will rotate a very small amount
  - Pinch-off effect at the shear line
  - The wafer will become fixed in place
- As long as you don’t over-lift the wafers or over-torque the plug, a haphazard lifting motion with the pick will open the lock very quickly
  - If this does not work, try to feel each wafer and see if one is not set

Lockpicking

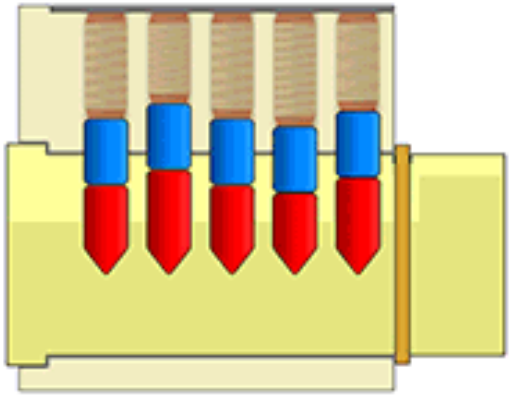
- Get a box
- Get a pick (hook or snake)
- Get a tension wrench

→ Open the box

Lockpicking



- Imagine a one wafer lock
- Add more pins
  - Apply tension
  - Due to mechanical defects, one pin stack will bind
  - “Set” the pin stack
  - Another pin stack will bind
  - Set every pin stack



Intrusion Detection

Q: What's worse than walking through a door and hearing an alarm go off?

A: Walking through a door and not hearing an alarm go off

Sensors

- Reed switch

Sensors

- Reed switch
- PIR

Sensors

- Reed switch
- PIR
- Ultrasound

Friendly Sensors

- Turn on lights
- Open doors
- Prevent alarms from sounding
  - On “inside” of door combined with handle / crash bar sensor
  - Checks that a person is exiting
  - Would not be tripped by a slide / integral

Angry Sensors

- Trigger alarms
  - Silent
  - Audible

Reed Switches

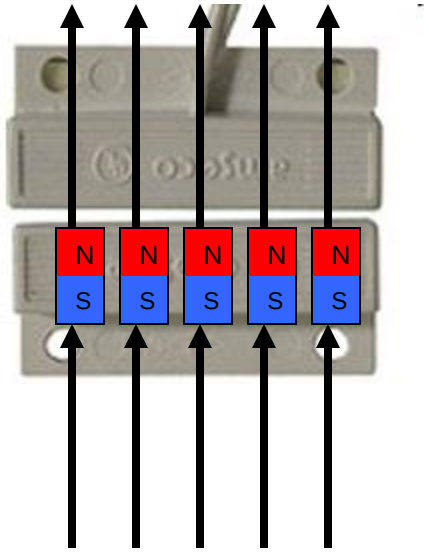
- Magnetically controlled switch
  - If there is a magnet field present, the alarm will not go off
- Usually on “inside” side of door
- Door opens

  → Magnet moves away

  → Alarm sounds

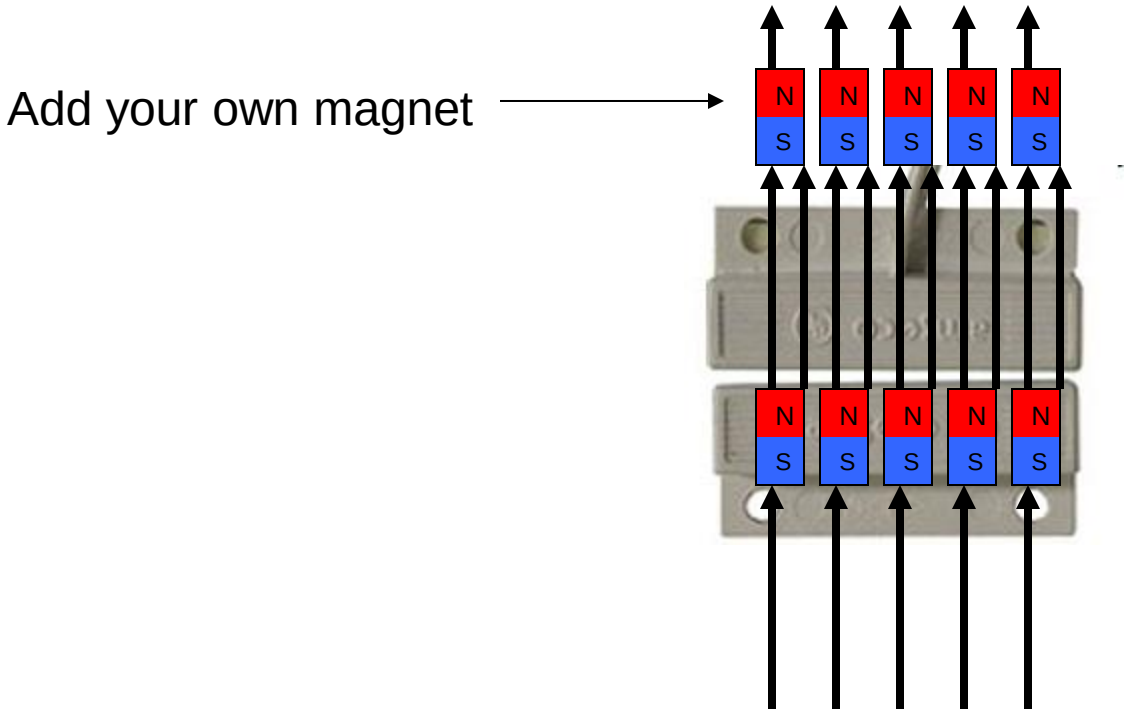
Defeating Reed Switches

- Make sure the magnetic field never goes away



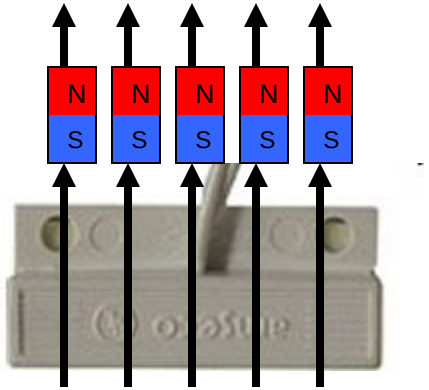
Defeating Reed Switches

- Make sure the magnetic field never goes away



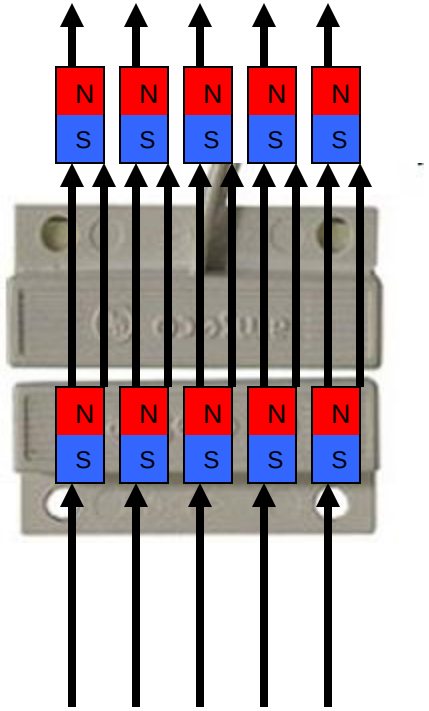
Defeating Reed Switches

- Make sure the magnetic field never goes away



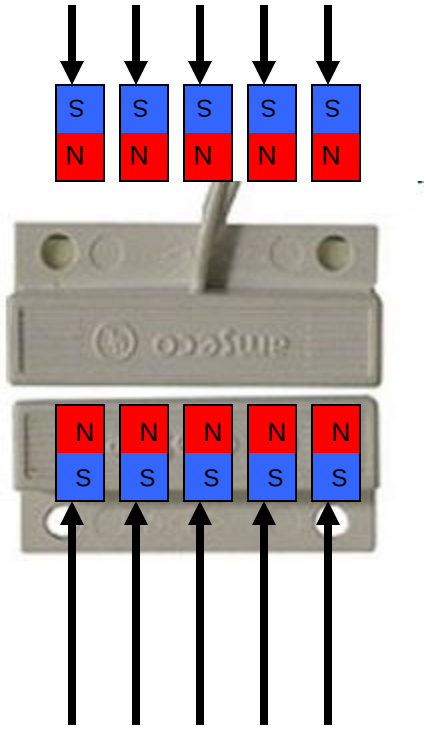
Defeating Reed Switches

- Make sure the magnetic field never goes away



Defeating Reed Switches

- Make sure the magnetic field never goes away



If polarity is incorrect,

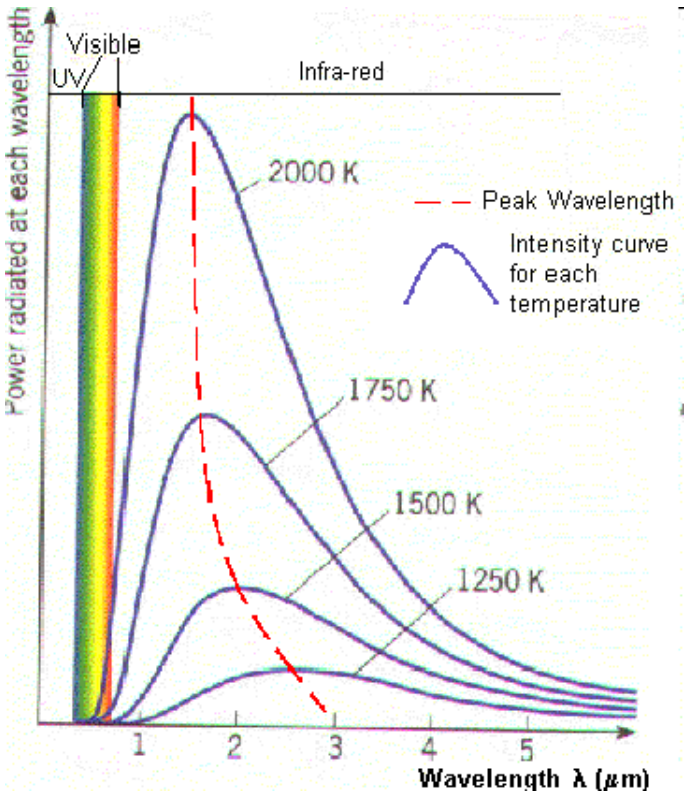
Alarm goes off while door is still closed!

Defeating Reed Switches

- Reed switches are on the inside of doors
- You can’t attack a reed switch from the outside
  - However, if you ever have access to the inside, you can disable the reed switch for later use
- Often, you will have to find another way around the door

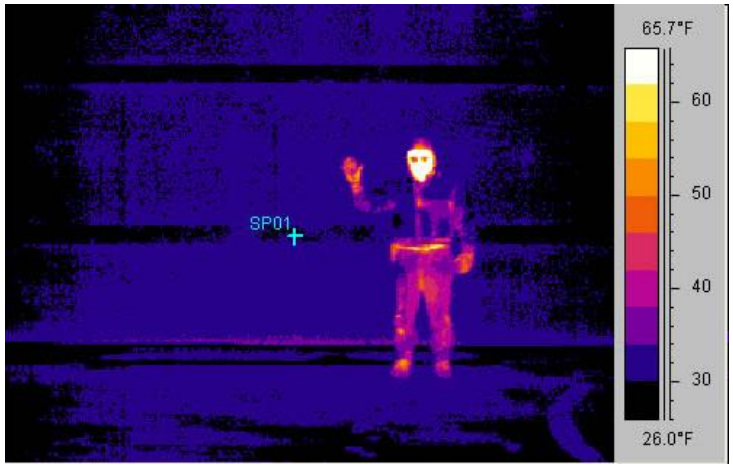
Passive Infrared (PIR) Sensor

- Radiated heat is a form of light
  - Long-wave IR
  - Too long to see
  - Behaves like light



Passive Infrared (PIR) Sensor

- Radiated heat is a form of light
  - Long-wave IR
  - Too long to see
  - Behaves like light
- To the sensor, your body appears to be glowing



Defeating PIR

→ Block or reflect your body's heat

– Some materials are opaque to long-wave IR

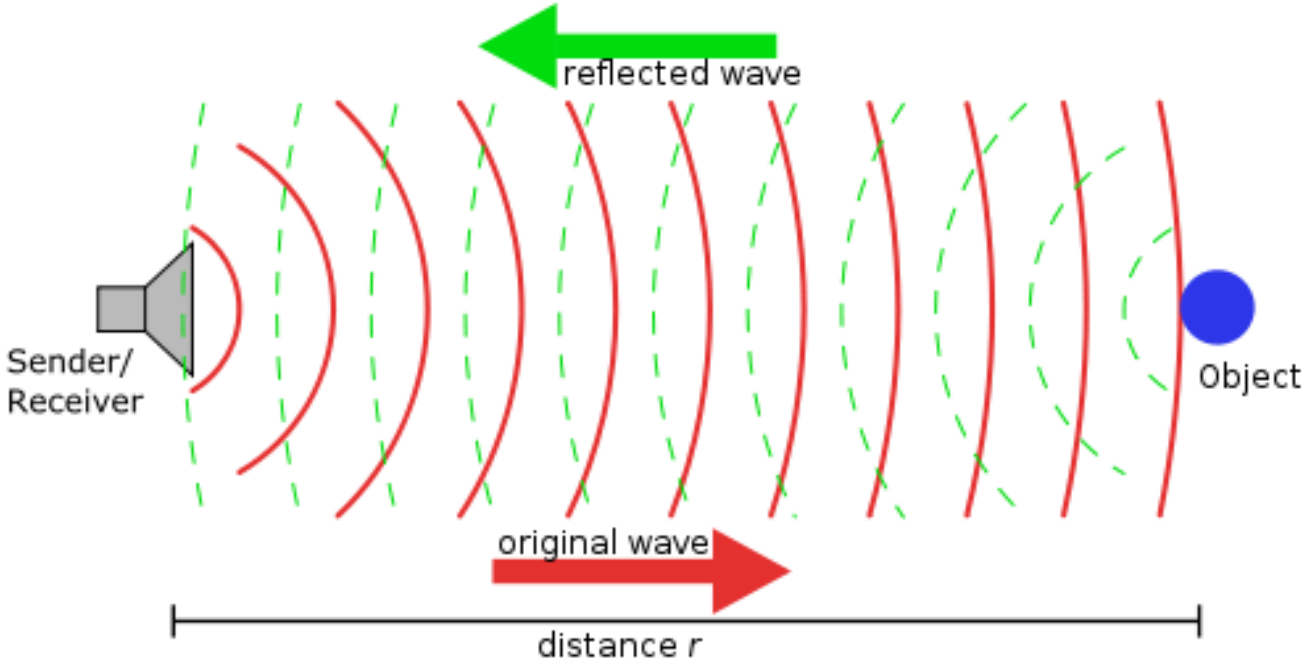
- Glass
- Thin film of oil
- Walk incredibly slowly

– Sensors detect a rapid change in IR

Supplementary Reading:
Mythbusters, Diamond Heist

Ultrasonic Sensors

- Speaker emits high-frequency “Ping”
- Microphone hears echo
- Travel time tells you distance to nearest object



Defeating Ultrasonic Sensors

- Cause no reflections
  - Absorb sound
- Bed sheet

Supplementary Reading:
Mythbusters

Setting off Alarms

- Monitoring system
  - Logs the event, no response
  - Unlikely to be noticed
- Silent alarms
  - Triggers response
- Audible alarms
  - Designed to scare away intruder
  - Often no response

Listening for Response

- A simple HAM radio can listen to the police
- As per FCC regulations, all allocated frequencies are published
  - Even private security

http://www.radioreference.com/apps/db

Setting off Alarms

- Response is often slow
- Rapidly exit
- Casually walk away
  - Social Engineering

Where to go from here?

- Security Audit / Penetration testing
- Locksport
- Urban Exploration
  - Exploration of abandoned buildings
- Infiltration
  - Exploration of off-limits areas of active buildings
  - “Hacking”

High Security Locks

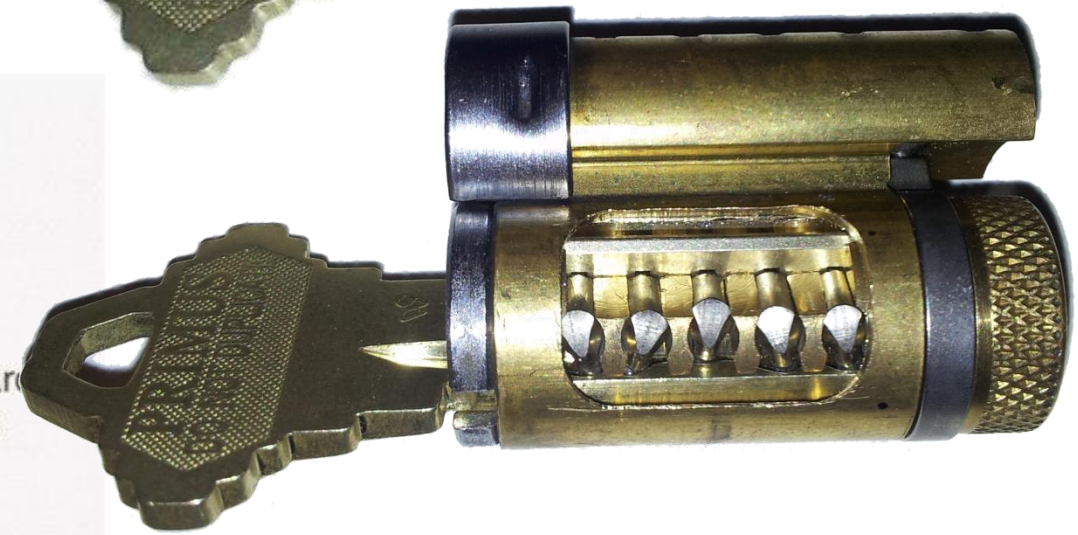
- Medeco m3 and Biaxial
  - Pin tumbler
  - Security pins
  - Pin rotation matters
- Schlage Primus
  - Pin tumbler
  - Side “finger” pins
    - Height matters
    - Rotation matters

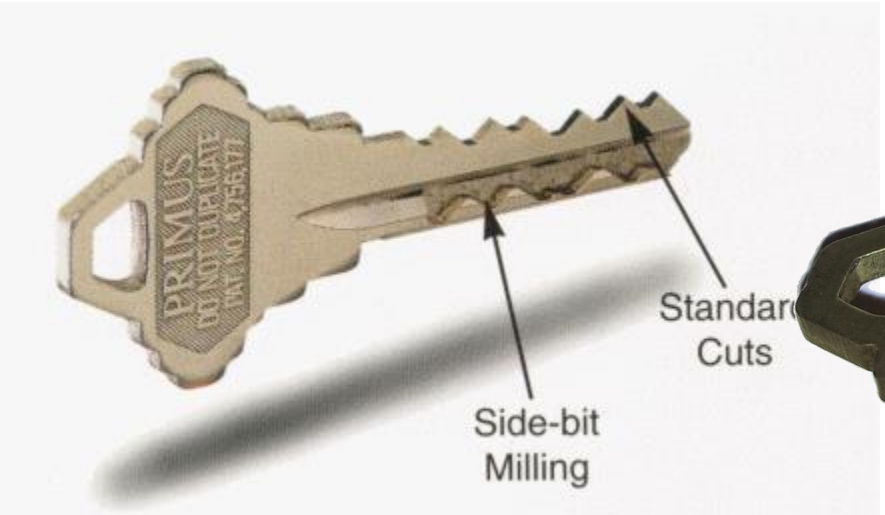
Schlage Everest

- Single finger pin in the back
- Must be raised to the right place to open the lock
  - However, this height is a known constant
  - And happens to be the exact thickness of a thick paperclip
- Attack
  - Insert paperclip
  - Lock is reduced to simple pin tumbler design

Schlage Everest

Schlage Primus





Schlage Primus

- With high tension, sidebar binds after pins
- With lateral tension, sidebar does not bind
- Isolates security features
  - Pins can be picked
  - Sidebar can be picked as well, but it is HARD

Schlage Primus

- Sidebar codes are sold to locksmiths by Schlage
  - Will be the identical within a facility
  - Very easy to acquire a sidebar
- Split-key attack
  - Grind down a key until it is just the sidebar
  - Any Primus on that sidebar has been reduced to a simple pin-tumbler lock

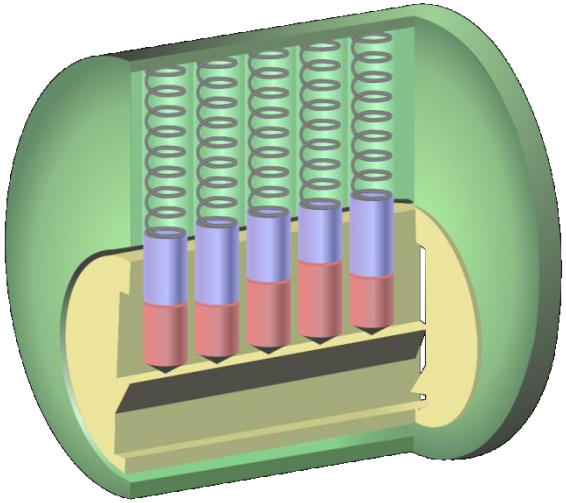
Example: Grind down a spare room key and gain access to any part of the building through a split-key attack

Schlage Primus Everest

- Patent extension of Schlage Primus
- Adds the “Everest” additional finger pin
- Still susceptible to split-keying

Get a Key

- Steal one, or…
- Get the information to make one
  - Photograph
  - Disassemble a lock



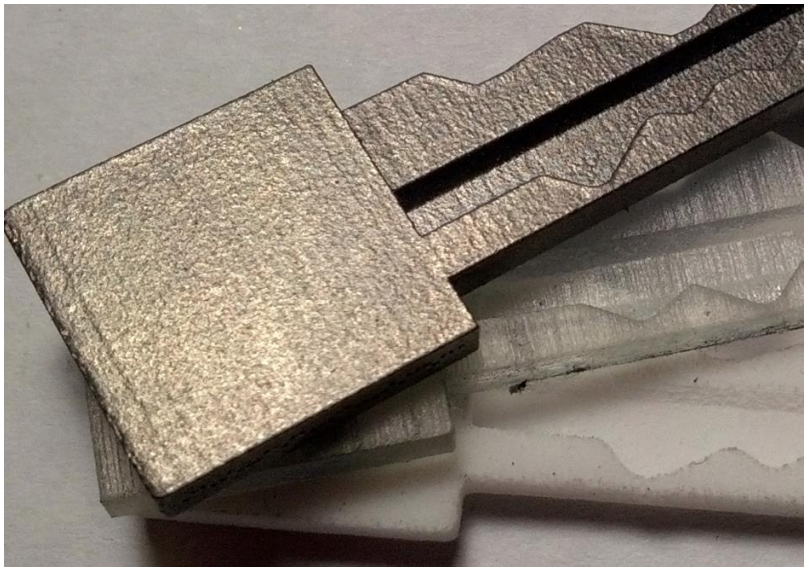
Supplementary Reading:
“Contextual Physical Security”

Make a key

- Can you copy a key?
  - Hardware store
- Can you make a key from a picture?
  - Hand-filing

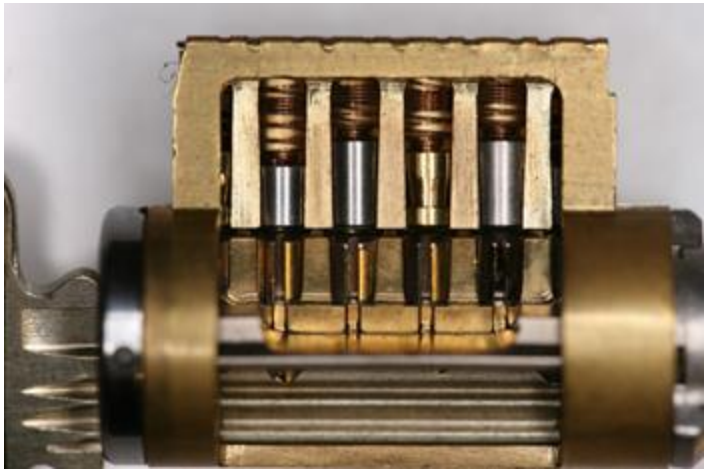
Make a key

- Can you make a high security key?
  - 3D Printing



Supplementary Reading:
My *DEF CON 21* talk

Medeco Biaxial



$$$

Medeco Biaxial

- Picking
  - Hard due to pin rotation
  - Unlike Primus, there are true and false gates
- Many vulnerabilities
  - Picking
  - Code setting keys
    - Vulnerability in issued sidebar codes
  - Split key does not work

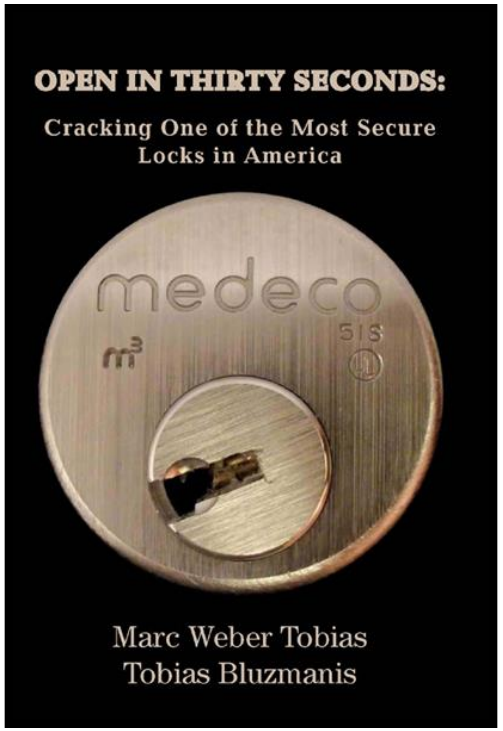
Medeco m3

- Patent extension of Medeco Biaxial
- Added “slider”
  - Analogous to the Everest finger pin
  - Always depressed to a constant depth
  - Can be defeated with a paperclip in the same way as Everest
- Made the keyway wider, facilitating picking
- Arguably *less secure* than Biaxial

Medeco

- Marc Weber Tobias
- UL-437 high-security standard:
  - Resistant to picking or bumping for a minimum of 10 minutes
- Wired test: 6 locks
  - Longest: 9 minutes
  - Shortest: 7 seconds

Are there any “high-security” locks?



Kaba E-Plex

- FIPS 201 Government Certified as High-Security
  - Only lock to achieve such certification
- Used in pentagon, White House, etc.

Fails:

- Shorting Electronics
- "Rapping"

Johnny Long

- Click [5:30]

Thanks

- Slides will be emailed to the class list

Eric Van Albert

ervanalb@mit.edu