



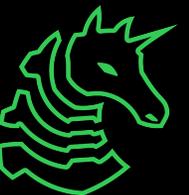
FA2023 Week 09 • 2023-10-26

Physical Security and Lockpicking

Emma, Nick, and Sam

Announcements

- Workshop with Ceasar Creek Software **TOMORROW!**
 - Siebel CS 2405 at 6-7 PM
 - Free pizza! 🍕

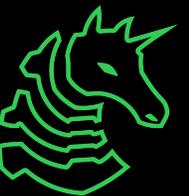
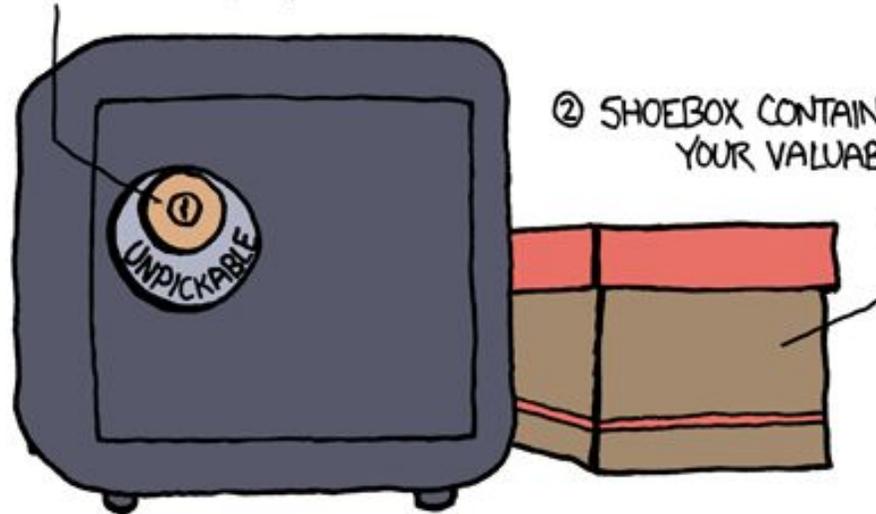


ctf.sigpwny.com

sigpwny{n0th1ng_0n_0n3}

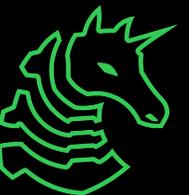
HACKERSHIELD GEEK-PROOF SAFE SYSTEM:

- ① 24-PIN DUAL-TUMBLER
RADIAL-HYBRID LOCK
(RENDERED UNOPENABLE
BY A FUSED 17TH PIN)



What is Physical Security?

- Deterring threat actors for a physical thing rather than a virtual one
 - Theft/espionage of funds or company secrets, physical harm, etc
 - Very often intersects (IoT/embedded systems)
- Threat models vary widely, what you realistically need is not what a government office needs
 - "Gates, guards, and guns" not the correct answer for everyone



Access Control

Security Revolving Door
self-managed with anti-tailgating system



-  REMOVABLE STRUCTURE
-  WITHOUT BASE, ON THE FLOOR
-  TAILGATING DETECTION SYSTEM (only authorized persons)
-  ACCESS CONTROL SYSTEM INTEGRATION
-  PIGGYBACKING DETECTION SYSTEM (single person passage)
-  FB4 BULLETPROOF REINFORCED STRUCTURE (optional)
-  PRESENCE CHECKING through ultrasonic volumetric sensors
-  BULLETPROOF ANTI-BURGLARY

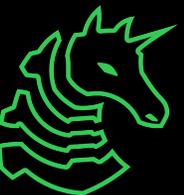
Certified glass
Turnstile glass BR1/S - P4B
Structure glass BR2/S - P6B
(optional 30/31mm BR4/S - P8B)

GRADE RC4
BURGLAR PROOF
UNI EN 1827

RC4 burglar-proof certification for the:
Co146.180.ND/NE
Co146.230.ND/NE

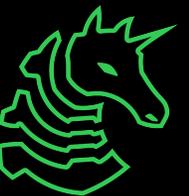
Model	Width (mm)	Depth (mm)
Co146.160.N	1600	660
Co146.180.N	1800	750
Co146.230.N	2300	1050

- Only allow people you want inside
- Fences, gates, and walls are basic forms of physical access control
- Can get more complicated
 - Keys - suitable for most civilians
 - Keycard entry



Surveillance

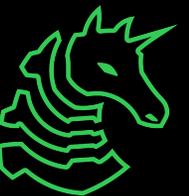
- Deters more noticeable forms of entry
 - "Just break a window/door/wall"
 - Lock bypass can be time consuming
- Cameras
 - Vanilla security cameras
 - "Smart" cameras, cloud
- Guards



"Know Your Rights"



- Different states have different laws on owning lockpicks
- Charges can be made worse if lockpicks are found on you
- Bump keys are explicitly illegal in Illinois, I will not be demoing them
- <https://www.toool.us/lockpicking-laws.php> for more details about about U.S. lockpicking law
- I am not a lawyer



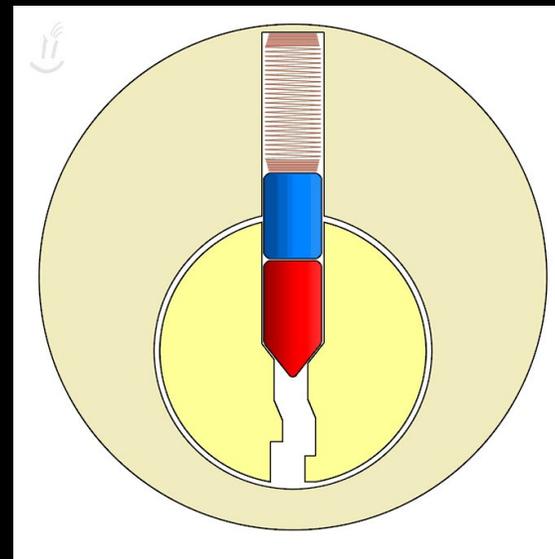
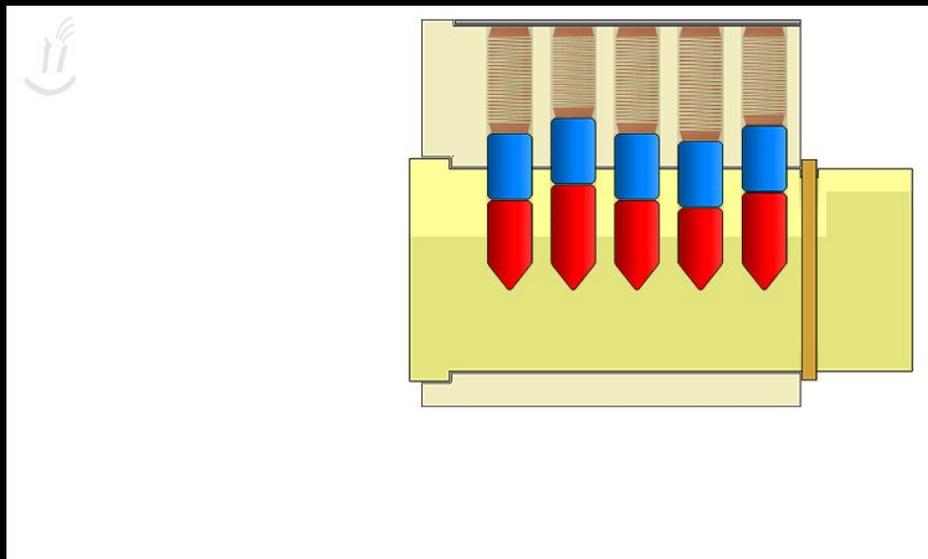
Don't Get Yourself (or Us) In Trouble

- If a lock is not owned by you, it is probably a felony to pick it
 - University locks
 - Dorm/apartment locks
 - You have permission to pick our challenge locks today
- Try not to pick anything you rely on to work
- Give us back our lockpicks/locks when you're done
 - We will give you a kit, you can share them but please don't mix tools
 - If we don't get all the picks back, we will have to notify building staff and we don't want to have to do that
 - If you want to solve these challenges outside of the meeting we have weekly locksport meetups on Mondays 8 - 9 PM
 - If you want your own lockpicks, check out our group buy

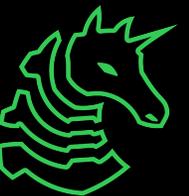


Pin Tumbler Locks

- When you think of a lock and key, probably this
- Cylinder holds pins that are cut at certain points, set in right place by key
- Tiny imperfections misalign the holes, allowing for lockpicking

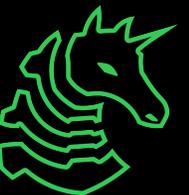


Now Let's Talk Lockpicking



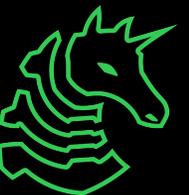
Lockpicking

- Goal: perform the roles of the key without having it
 - Physical object performing the turning action
 - Pins in the spot they need to be to turn the lock
- Manufacturing defects allow you to set pins one at a time without always having the key in place
- Method:
 - Provide tension to turn the keyway using tension
 - Set pins in place using a lockpick



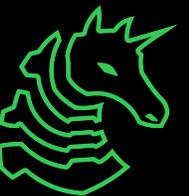
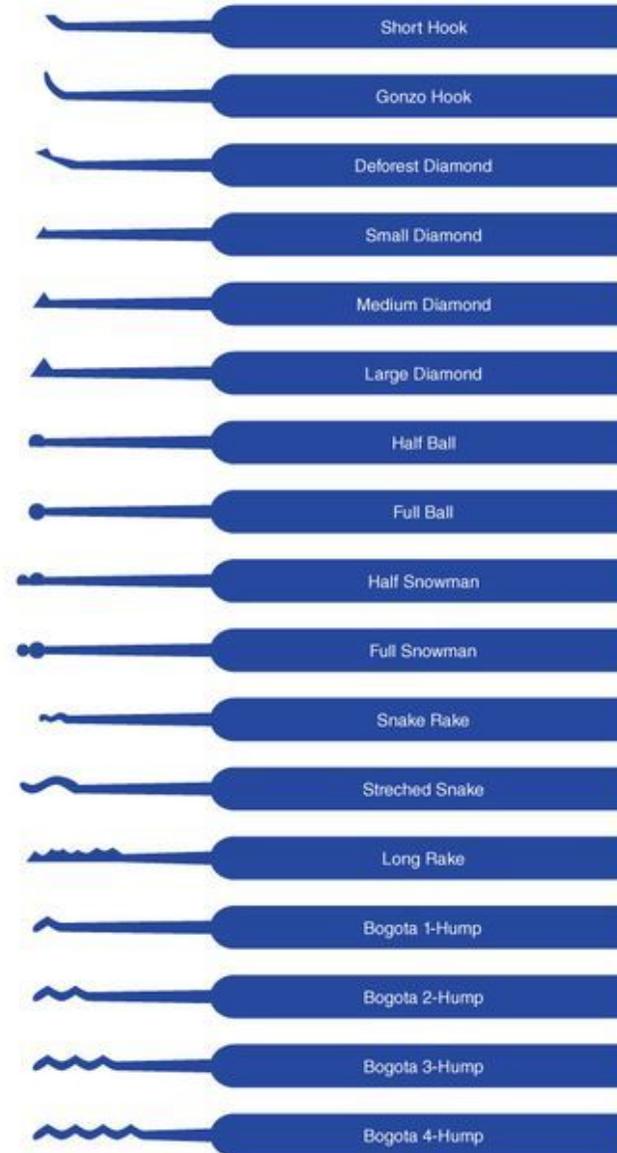
Tension

- More important than the picking itself
- Two types: bottom and top of keyway
 - Affect the environment your lockpick sits in and how you receive feedback
- The amount of pressure you give is crucial
 - Too much will make it hard to push the pins, too little will make it hard to receive feedback

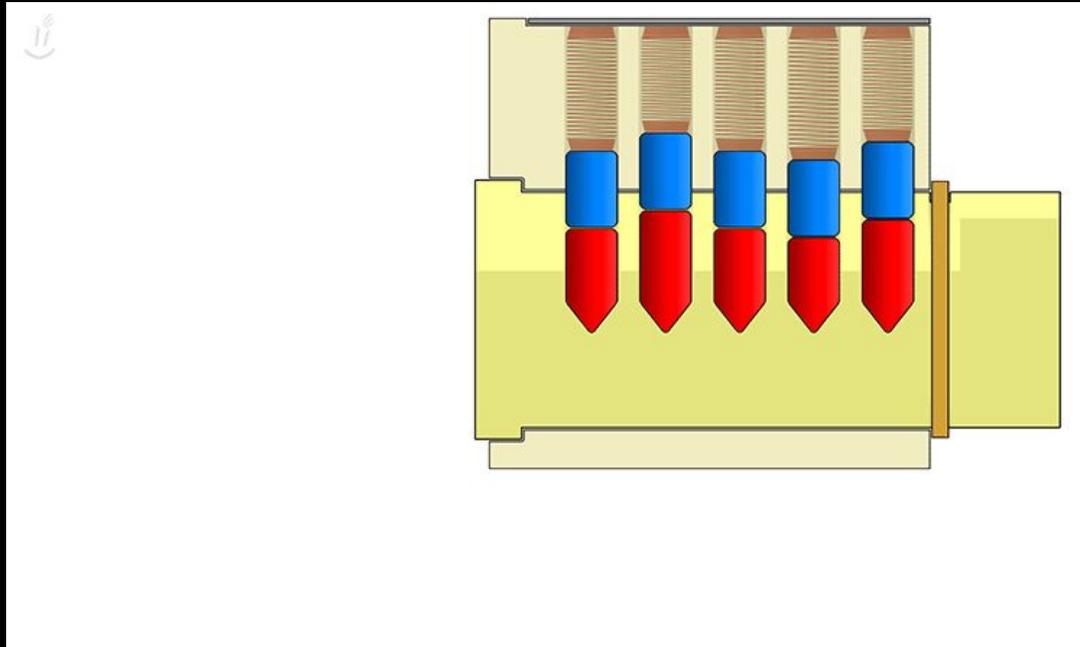


Lockpicks

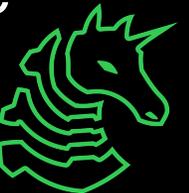
- Single pin
 - Hooks
 - Diamonds
 - Ball/snowmen
- Rakes
 - Long rakes
 - Snakes
 - Bogata



Single Pin Picking

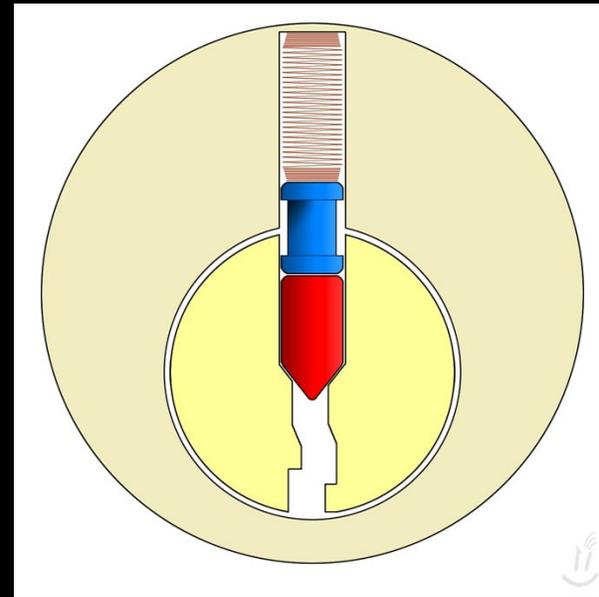


1. Grab a properly sized tensioning tool and a short hook
 - a. The crowbar shaped thing and the hook shaped one
2. Put the tensioning tool either at the top or bottom of the keyway and turn
 - a. Your picks go at the bottom
 - b. Don't push too hard, just hard enough that you'll feel feedback
3. Feel for the pin with the most tension and bring it up until it clicks
4. Continue the process until the lock is picked

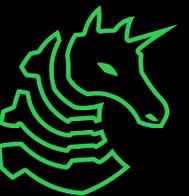


Security Pins

- Deters low-skilled attacks by making picking harder
- Come in many shapes, all designed to trick you into thinking the lock is partially picked
- Makes lockpicking more fun!

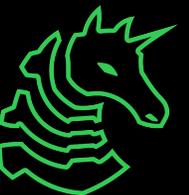


Demo: Picking a Lock



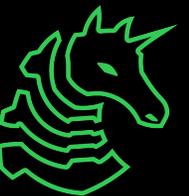
Lock Gutting

- Lock gutting is the practice of disassembling locks
- Used for variety of purposes
 - Rekeying
 - Intelligence/data gathering
 - Modification
- DO NOT GUT A LOCK YOU'RE USING FOR SOMETHING



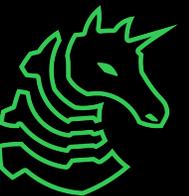
Demo: Gutting a Lock

Featuring Nick



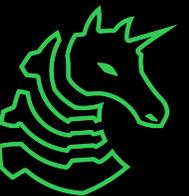
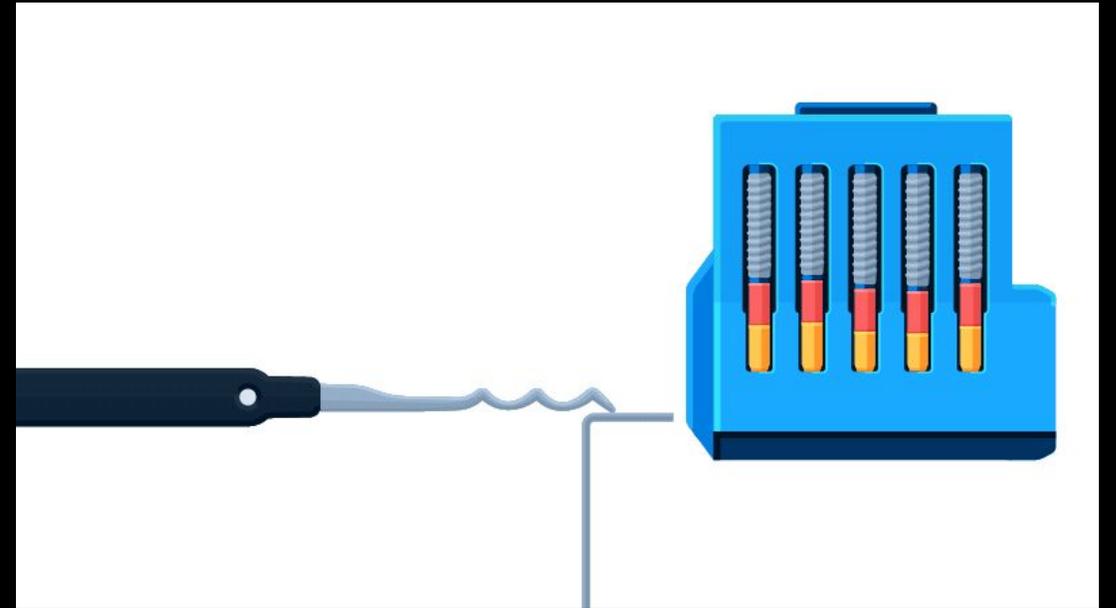
Bypass Crash Course

Non-picking techniques that still get locks open

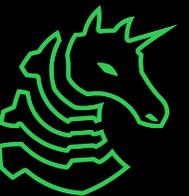


Raking

- The power of probability!
- Gently rock the wavy shaped pick inside the lock until you can turn it open with the tensioning tool
- Very effective with low security locks, becomes less reliable when you face security pins

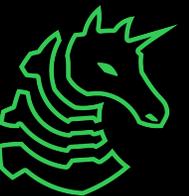
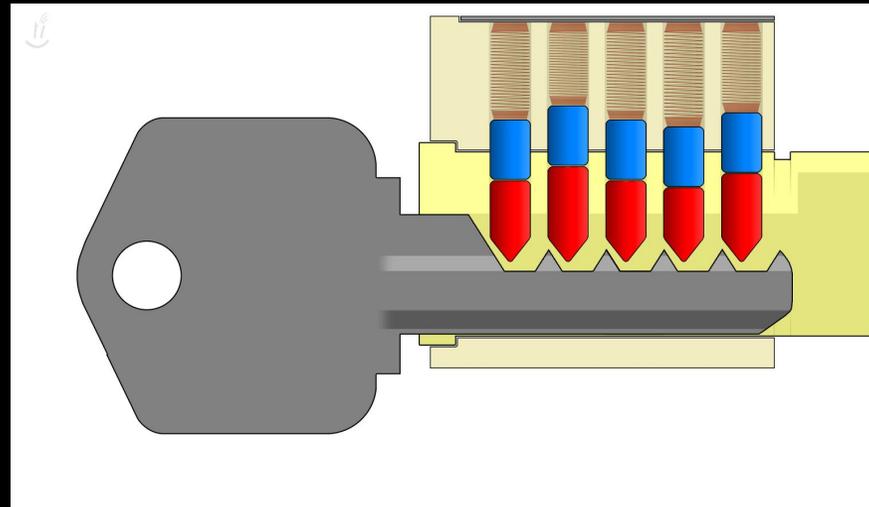


Demo: Raking a Lock



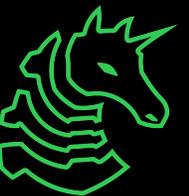
Bump Keys

- Bounce all the top pins above the shear line at the same time
- Turn the bump key
- Must correspond to the specific lock



Shimming

- Unprotected lock shackles
- Separate latch from shackle, open without touching the cylinder at all
- Works well on cheap padlocks, not so much on higher grade

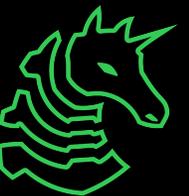


Knife Bypass

- Use a thin implement to directly manipulate locking mechanism
- Lock-specific bypass

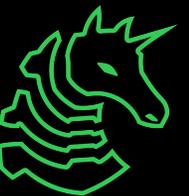
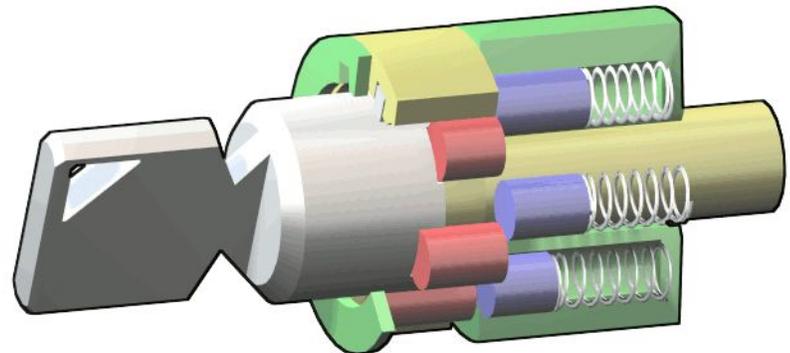
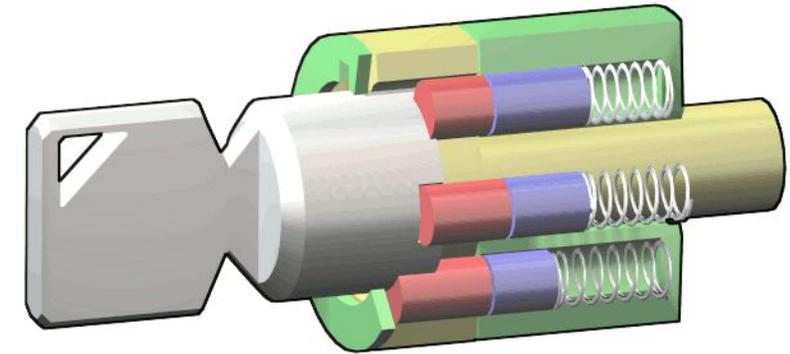
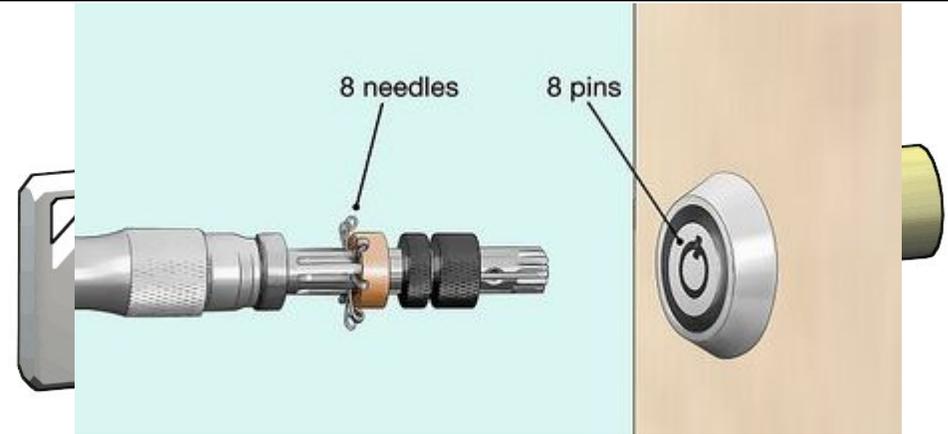


Other Weird Locks



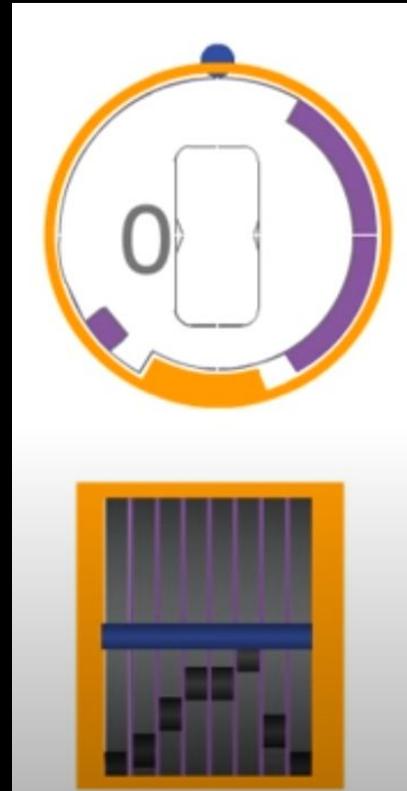
Weird Locks

- Tubular Locks place the pinstack parallel to the keyway
- Same idea overall, just different orientation
- **Horribly weak and extremely pickable**
- You can tension the core and single-pin pick by depressing the pins
- OR, by a \$4 dollar tool that acts as a master key



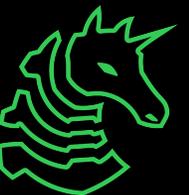
Weird Locks

- Considered "more secure," Disk Detainer locks are found in high end locks, and most bike locks (Kryptonite, etc.)
- A bar (blue) prevents the core from rotating
- Each disk has a cut at a certain rotation
- Once all disks align, the bar drops and the core rotates
- Pickable with speciality tools:
 - Same principle as tumbler locks, use one disk to tension the core, while manipulating other disks
 - Disks will click into place as you slowly lower the bar
 - A rotating manipulator allows you to rotate disks



Now You Try!

- Clear lock
 - What's happening inside the lock when you feel feedback?
- Progressive locks
 - Work your way up towards 4 and 5 pin locks
- Master Lock No 3 (blue)
 - Your first real-world lock!
- Master Lock 140 (gold)
 - Your first security pin!
- Brinks Lock
 - More security pins
- Door Locks
 - How secure is your door?
- Safes
 - Try your hand at tubular locks and safe cracking



Next Meetings

2023-10-27 • Tomorrow!!

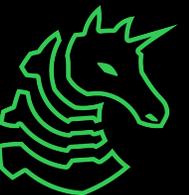
- Workshop with Ceasar Creek Software
- Learn about Ceasar Creek and grab some pizza!

2023-10-29 • No Sunday Meeting

- Enjoy your Halloweekend!

2023-11-02 • Next Thursday

- Forensics workshop with CrowdStrike and UIUC Tech Services



ctf.sigpwny.com

`sigpwny{n0th1ng_0n_0n3}`

Meeting content can be found at
sigpwny.com/meetings.

