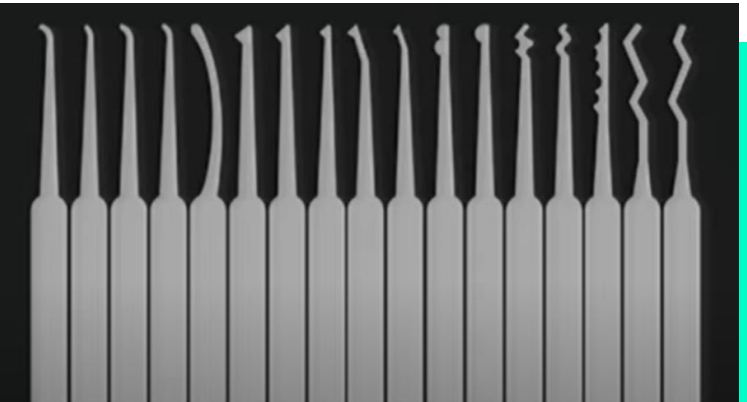
Physical breach via homemade Lock picking tools



Red Team physical pen testing
“the art of lock picking”
Presented by Josh Ryan

The art of lock picking

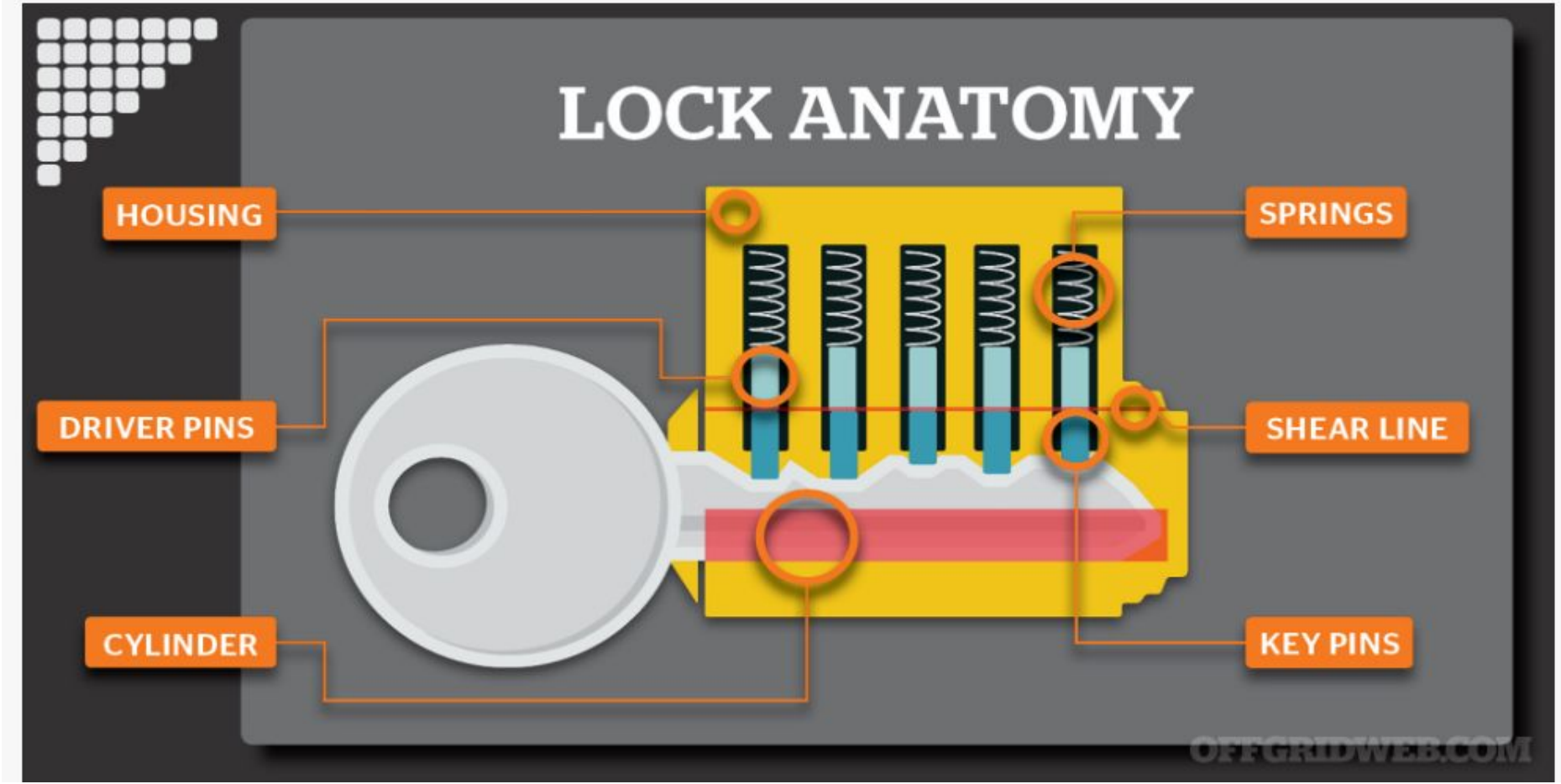
- Pin and tumbler locks aren't too hard to learn to pick if you have the right tool at hand (and spare time).
- When most people think of the use case, they think it is just for criminals or spies but pentesters often need these lock picking tools to gain their initial access into a building to set up raspberry pis or other hacking tools to the network.
- The scenario for this demo is having to pick a padlock to gain access into a server room or data center. Best to pick it and leave no trace to further your investigation.(as opposed to using bolt cutters)
- These pin and tumbler locks are the most standard you'll find for doorknobs, deadbolts and padlocks. See slides 3-4 for the mechanism internally.

https://www.offgridweb.com/preparation/lockpicking-101-learn-the-basics-of-how-to-pick-a-lock/

The Mechanism

- The cylinder is the lower portion of the lock that is torqued by hand to twist and force rotation. The pins keep it in place and prevent it from turning until the key is inserted setting the pins.
- The driver pins all are attached to springs that are forced into a specific area by the shape of the key and after being perfectly aligned with the shear line by the key pins, it allows the lock to twist open. They all vary in length that fit within the shape of the key or manually by the lock pick.
- There is usually some wiggle room and the shear line offset make it possible for the lock to be picked.

https://www.offgridweb.com/preparation/lockpicking-101-learn-the-basics-of-how-to-pick-a-lock/



https://www.offgridweb.com/preparation/lockpicking-101-learn-the-basics-of-how-to-pick-a-lock/

Tools for the job

- There are a few specific tools you need to pull off a lock pick.
- Various hook picks, half diamond picks, rake picks, ball picks and most vitally is a tension wrench used in conjunction with one of the picks best suit for the job.
- The picks used for this demonstration were actually handmade from some bladed bicycle spokes and shaved down with a grind wheel.
- They were eyeball tested but have helped me get into my house when locked out and rescue people’s bikes when they have lost their keys. See next slide for the tools used in this demo.

Legal consequences

- In the United States, it is legal to own and carry lock picks in most jurisdictions.
- Technically, California considers possession of lockpicks as a crime but usually would require malicious intent.
- If you are ever in doubt, check the legality in your area before purchases or testing your skills with lockpicking.

https://www.offgridweb.com/preparation/lockpicking-101-learn-the-basics-of-how-to-pick-a-lock/

How lockpicking relates to cybersecurity

- Lockpicking is part of the skills needed for physical pentesters to gain access into controls rooms or data centers to elevate their privileges and fully test the security of the company’s data.
- Lockpicking stations are set up at almost every InfoSec conference from DefCon to BlackHat.
- The quality of the lock you use to safeguard your data is just as important as the firewall settings you implement.

Demonstration preview

- First, I took some bladed bicycle spokes and used a grinding wheel to replicate a set of lockpicks as they were not as easy to get when I made mine.
- In this demo, I will be using a tension wrench and two different types of picks to break into a small luggage lock with just a few key pins and then a master lock with several key pins. The picks used were a rake and a double diamond.
- These locks are both not too hard to pick but in just adding a few extra pins takes that much longer to pick.
- I first insert the tension wrench to apply some tension to slip the pins into the shear line so the cylinder will rotate.
- For more sensitive locks like deadbolts and car locks the process is much different. You would have to find out which pin to start with and set each pin individually and in order, while keeping just the right tension on the tensioner.
- With these locks I used a method known as raking or passing through the pins while applying and releasing pressure on the tension wrench. There is enough wiggle room with these that they pop open relatively easily in comparison. There are several levels of difficulty you can find with these locks but if you can crack them with this method this quickly, you shouldn’t rely too heavily on them.

Video demo - (second lock took 2 minutes so feel free to skip forward)

Demonstration summary

- The demonstration was a success in that I was able to pick both locks within minutes.
- It was clear that the larger lock with move key pins made it that much more difficult to pick than the luggage lock.
- Working with these I found that the rake pick worked better with the luggage lock and the double diamond worked better with the larger lock. Sometimes figuring out the correct pick and rotation can also take time.
- However, in practice, I have only been able to pick a deadbolt a few times and can take much longer so the padlocks made for a better demonstration. Although, even your typical deadbolt is probably not too hard for the seasoned locksmith.
- One tip would be to NEVER rely on your door handle twist lock, those are even easier to pick because all you need is a flexible laminated card to slide and poke the bolt latch (As seen in the movies). So always make sure your deadbolt is locked at night.

MITIGATION

- One mitigation for having someone pick your lock would be to do the research on how hard the lock is to crack.
- Some locks actually have different shaped pins and/or pins on both side which adds complexity to the process.
- You can also use extra measures of security to backup the physical deterrent of the lock itself. Like setting up a ring doorbell or have laser trip alarms set up as a failsafe.
- You can buy insurance for whatever is behind the lock and key.
- Adding biometrics to your lock may be out of budget but if you really want to secure something bad enough, it would certainly add to the difficulty of accessing privileged areas.


THE END WATSON!