Intro to Lock Picking

Jess Hires
Jacksonville TOOOL Chapter
www.JaxLocksport.com

Introduction

Security Engineer in Jacksonville, FL

Founder and coordinator of the Jax TOOOL chapter
Coordinator of the Jax2600/DC904 group
Vice President of the Jacksonville Linux Users Group

hacker, maker, breaker, developer, teacher, blogger

Topics Covered

- Locksport
- Ethics and Legality
- Types of Locks
- Parts of a Pin Tumbler Lock
- Normal Lock Operation
- Lock Picking Tools
- Single-Pin Picking
- Raking
- Lock Vulnerabilities
- Lock Security Mechanisms
- Relation to Information Security
- Community Interaction

Purpose

- Understand how a lock works
- Identify lock picking tools
- Learn how to pick a lock
- Participate in the locksport community
- Teach your friends

Obligatory Disclaimer

It is legal to pick locks, but there are some rules:

You can only pick locks that belong to you, or where you have explicit permission from the owner.

In Florida, it is legal to carry lock picks, in most cases. If an officer suspects intent to burglarize or trespass, lock picks are treated as a burglary tool. Be smart.

We highly recommend against picking locks you rely on, such as your door or car. Picks and locks can break.

Florida's Law on Lock Picking

810.06 Possession of burglary tools.

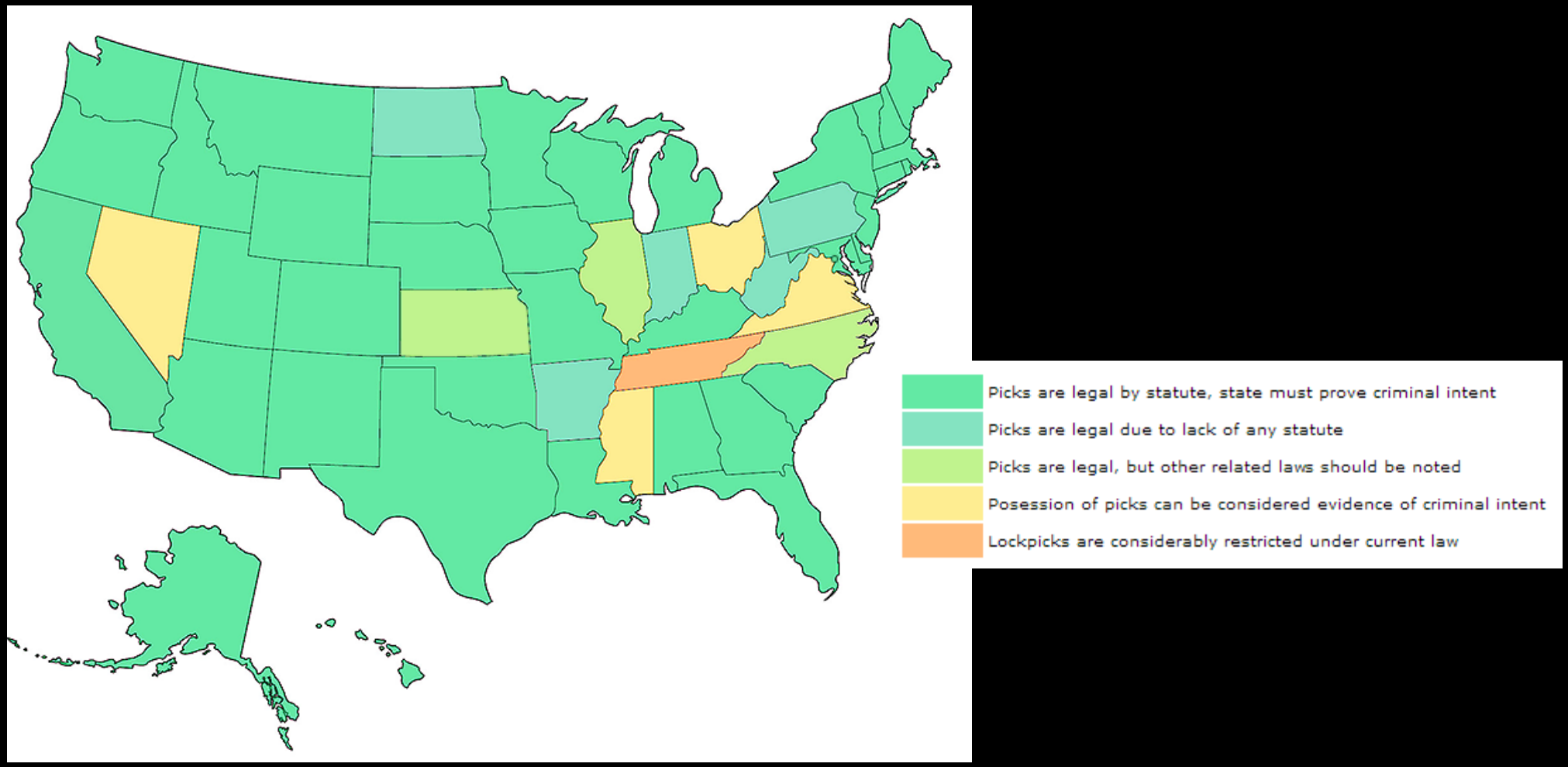
Whoever has in his or her possession any tool, machine, or implement with intent to use the same, or allow the same to be used, to commit any burglary or trespass shall be guilty of a felony of the third degree, punishable as provided in s. 775.082, s. 775.083, or s. 775.084.

Source: http://www.flsenate.gov/Laws/Statutes/2012/810.06

Each state has different laws on lock picking tools. Knowing the law can prevent you from getting into legal trouble. If traveling with lock picks, know the law of your destination.

Lock Picking Laws for Other States

TOOOL's map of lock pick laws for the US: toool.us/laws.html



What is Locksport?

Lock picking is the practice of bypassing a locking mechanism or system.

Locksport is the recreational practice of lock picking. Think of locks as complex, mechanical puzzles.

Many hackers and locksport enthusiasts gather and compete all over the world, at makerspaces and hackerspaces, DEFCON groups, 2600 chapters, TOOOL chapters, and especially at InfoSec conferences.

Who Can Pick Locks?

Anyone can pick locks with just a little bit of practice!

Two brand new lock pickers at a TOOOL JAX meeting:

There are many types of locks...

There are many types of locks...

There are many types of locks...

...many types of keys...

...many types of keys...

...and many types of tools

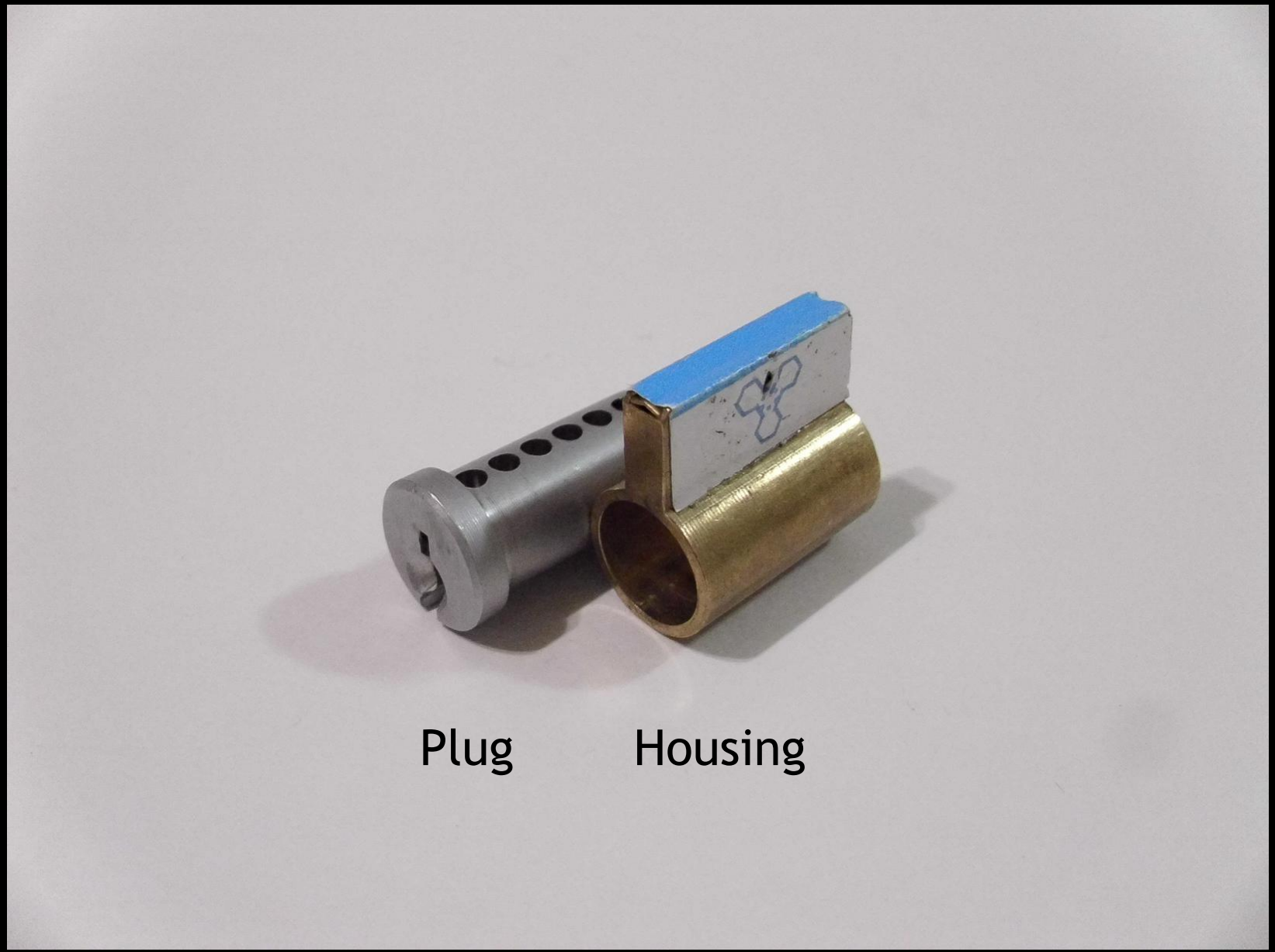
Types of locks

- Pin tumbler
- Wafer tumbler
- Combination
- Tubular
- Warded
- Lever
- Dimple
- Disc-detainer
- Magnetic
- Electronic

Parts of a Pin Tumbler Lock

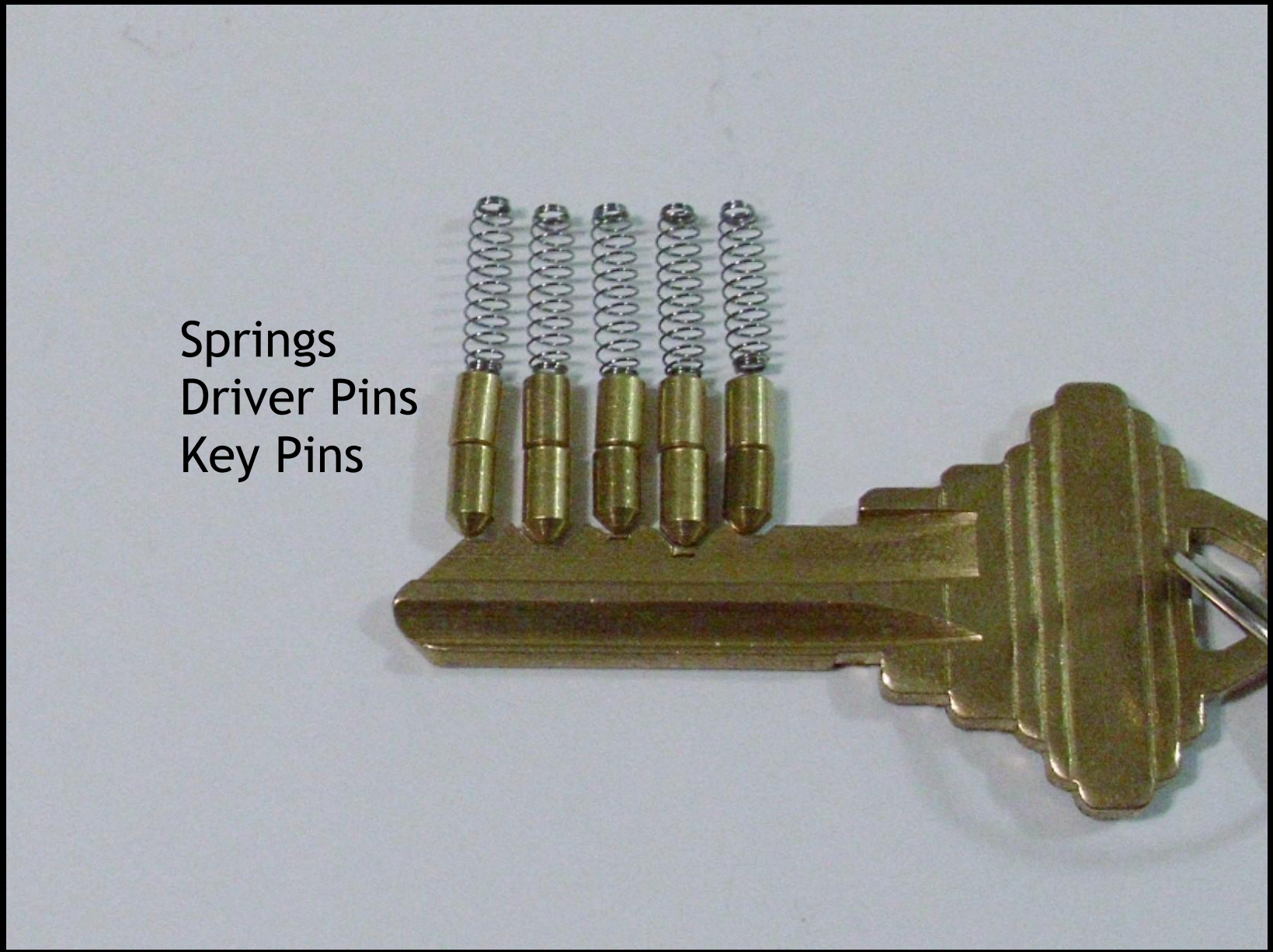
Pin Tumbler Lock

Parts of a Pin Tumbler Lock



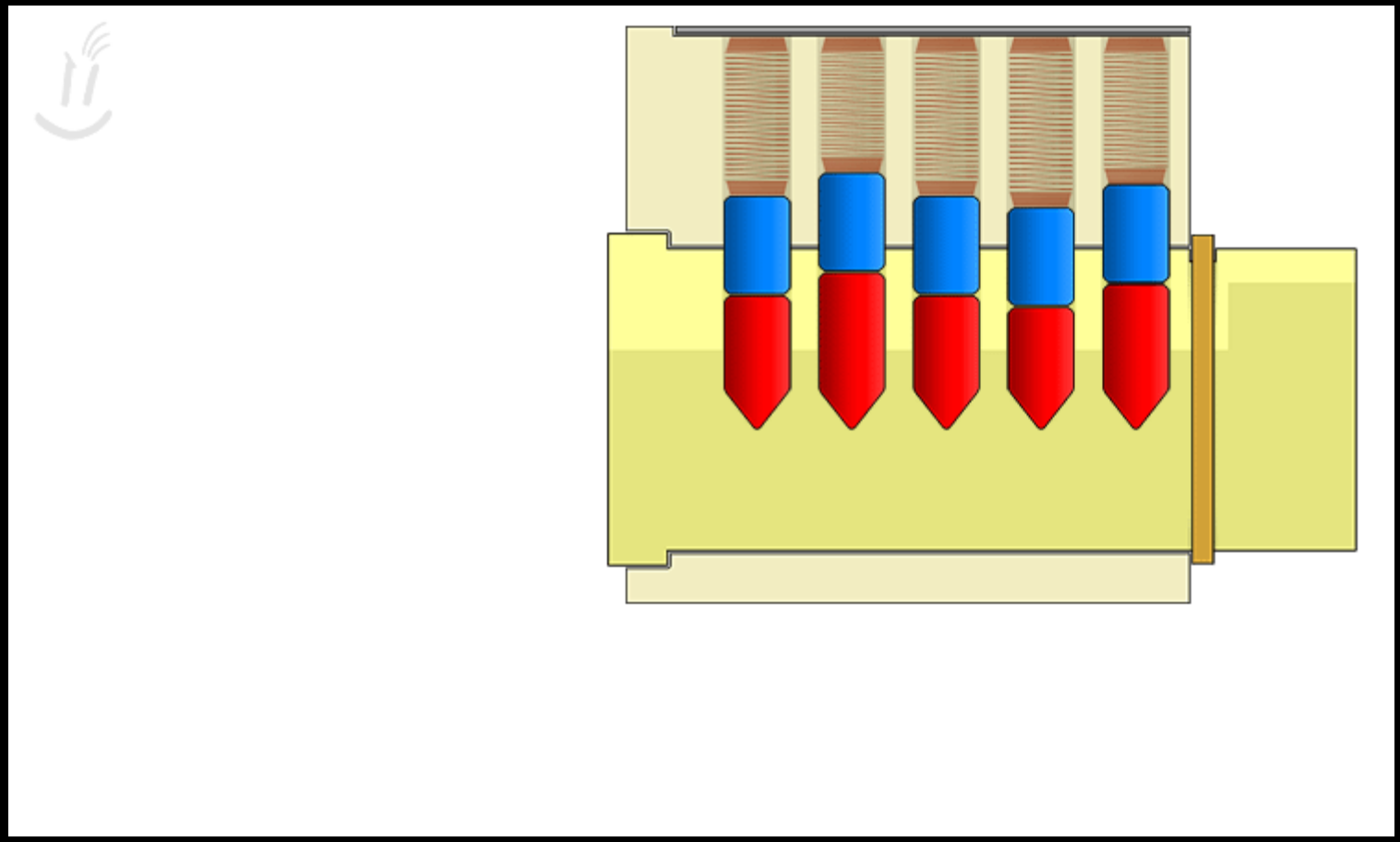
Plug Housing

Parts of a Pin Tumbler Lock



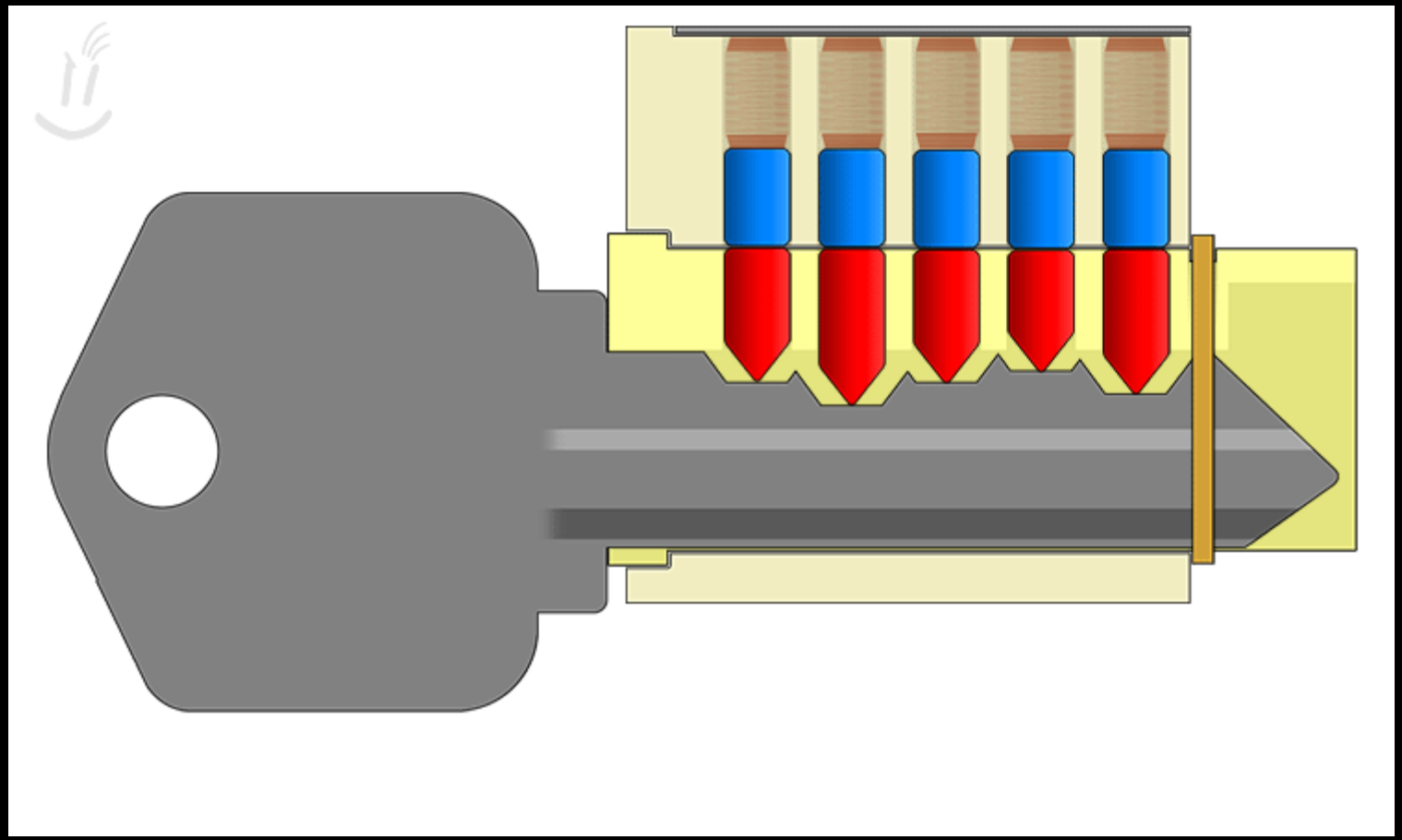
Normal Operation

Lock at rest.



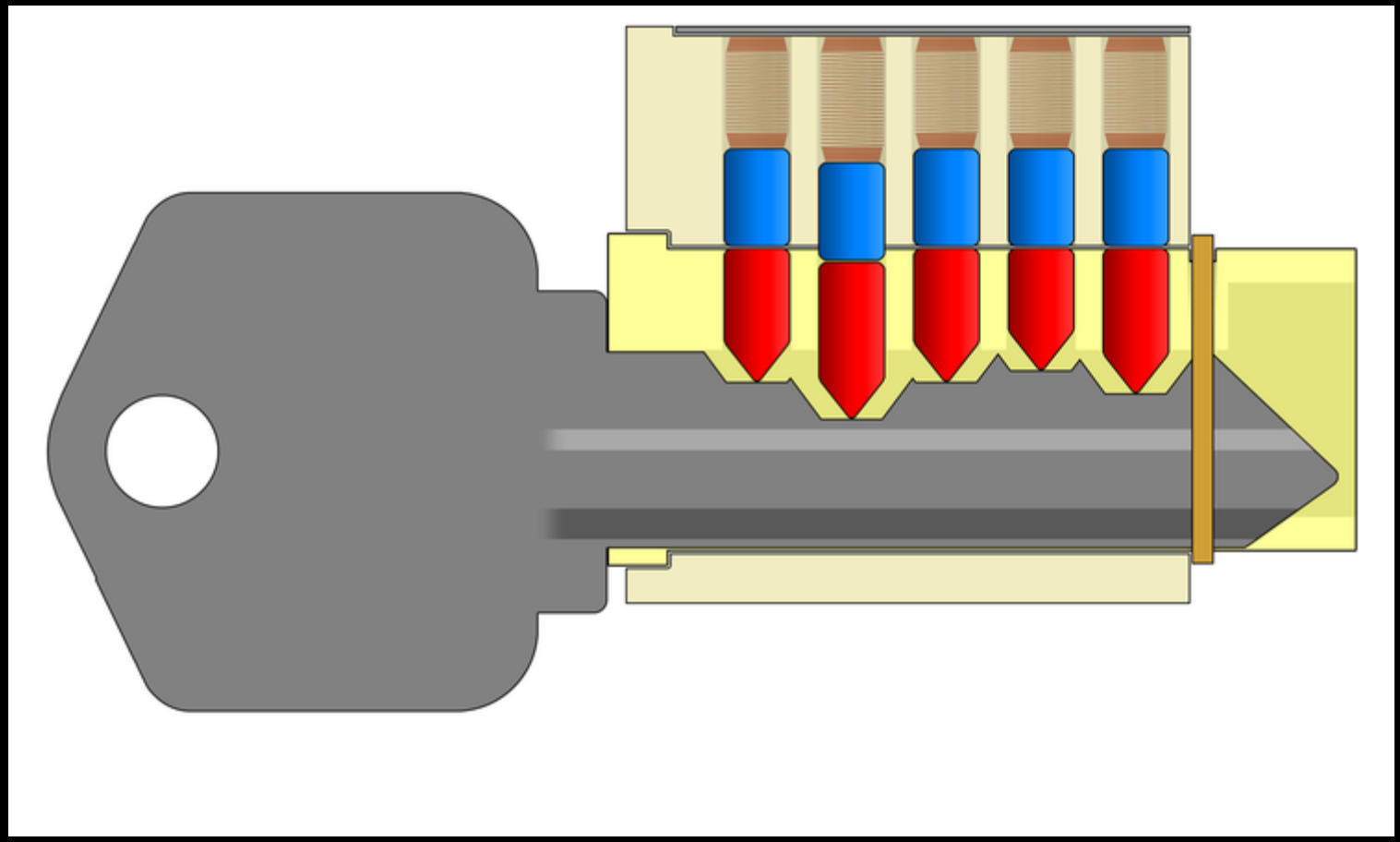
Normal Operation

Lock with correct key.



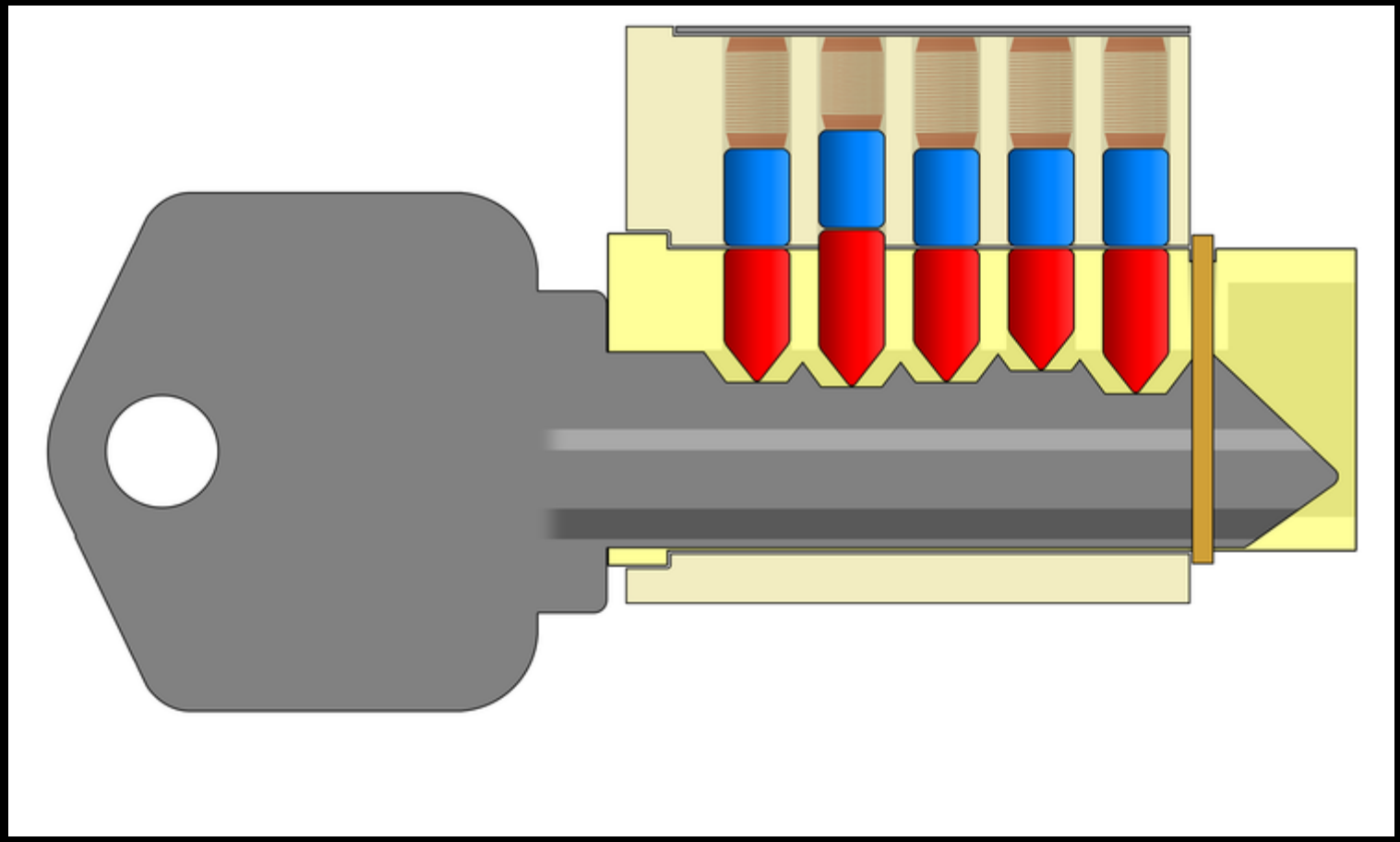
Normal Operation

Lock with incorrect key, one bitting too low.



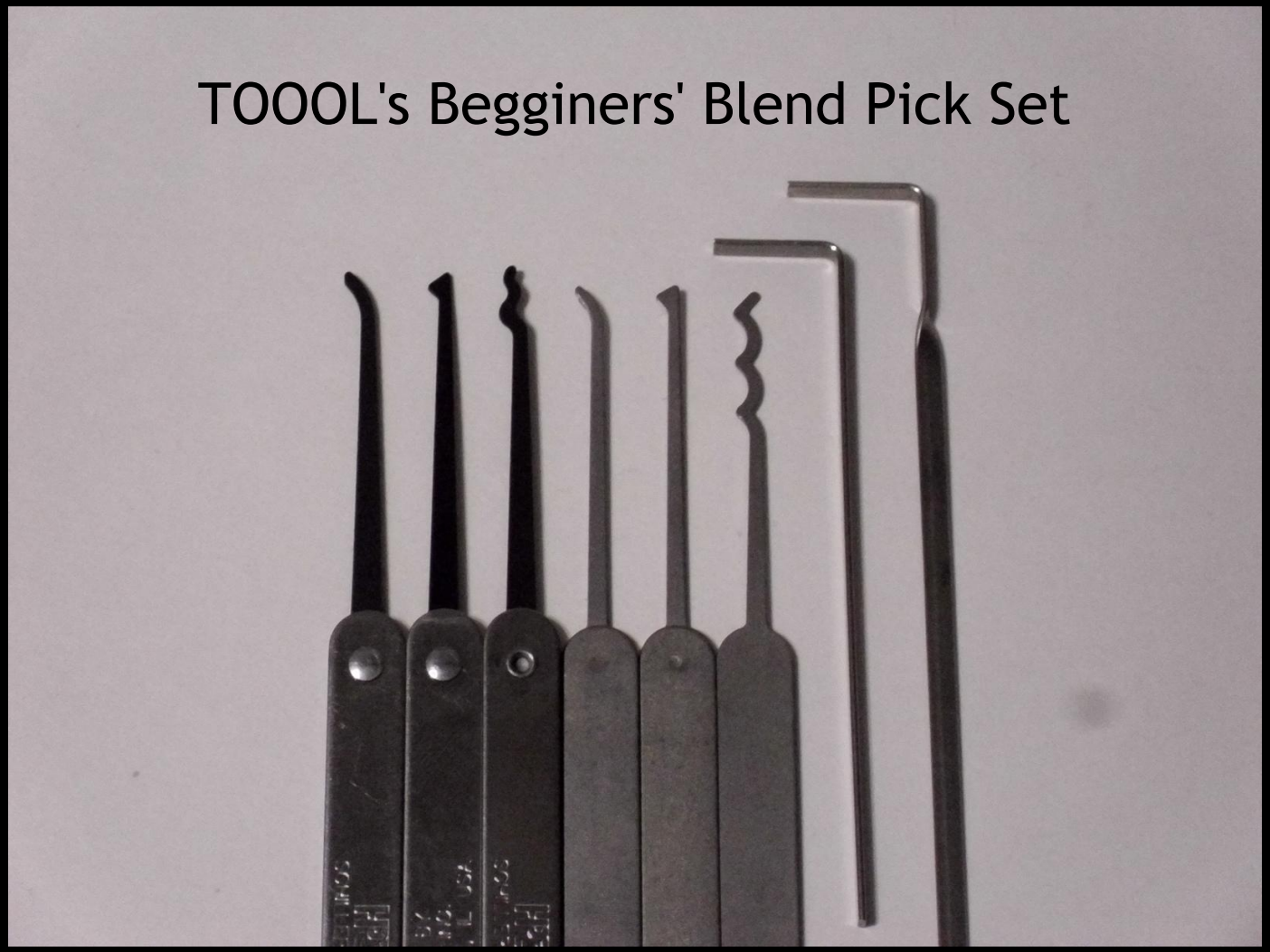
Normal Operation

Lock with incorrect key, one bitting too high.



Types of Lock Picks

Hooks, Half Diamonds, Rakes, and Tensioners



Types of Lock Picks

- Tensioners - used to apply torque to the plug
- Hooks - used for feeling and lifting individual pins
- Half diamonds - used for lifting, shoveling, and more
- Rakes - many varieties, used for lifting many pins, raking
- Ball picks - several types, typically used on wafer locks
- Broken key extractor
- Specialty picks for distinct locks types (disc detainer, warded, cruciform keyway, etc.)

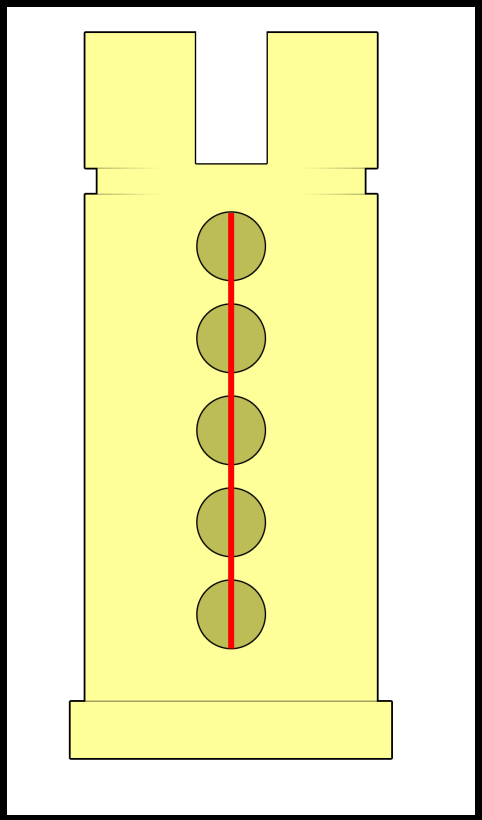
Okay, so how does it work?

The pin tumbler lock (most doors and padlocks) is susceptible to picking because of tiny tolerances and imperfections from the manufacturing process.

These manufacturing tolerances and variations allow a lock picker to manipulate each pin individually, while applying some light torque. This torque will cause a driver pin to bind. When a driver pin binds, the stack can be lifted, and a pin can be set. This is called single-pin picking.

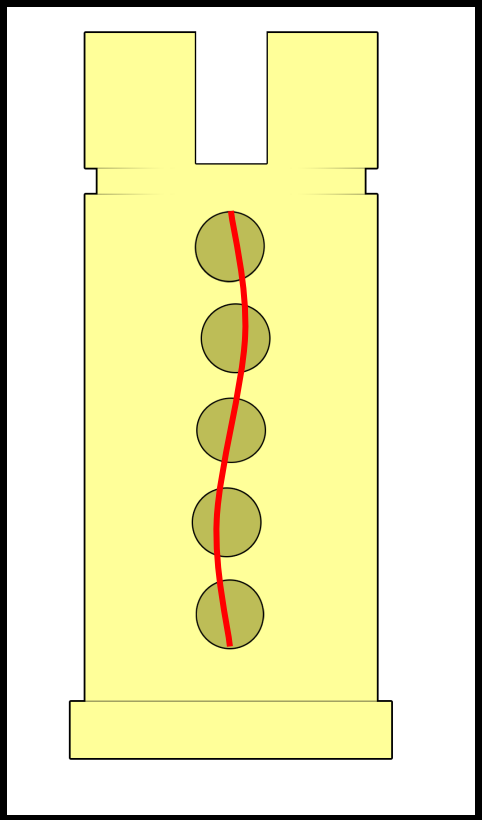
Okay, so how does it work?

In a perfect world, pin stacks would be in a straight line.



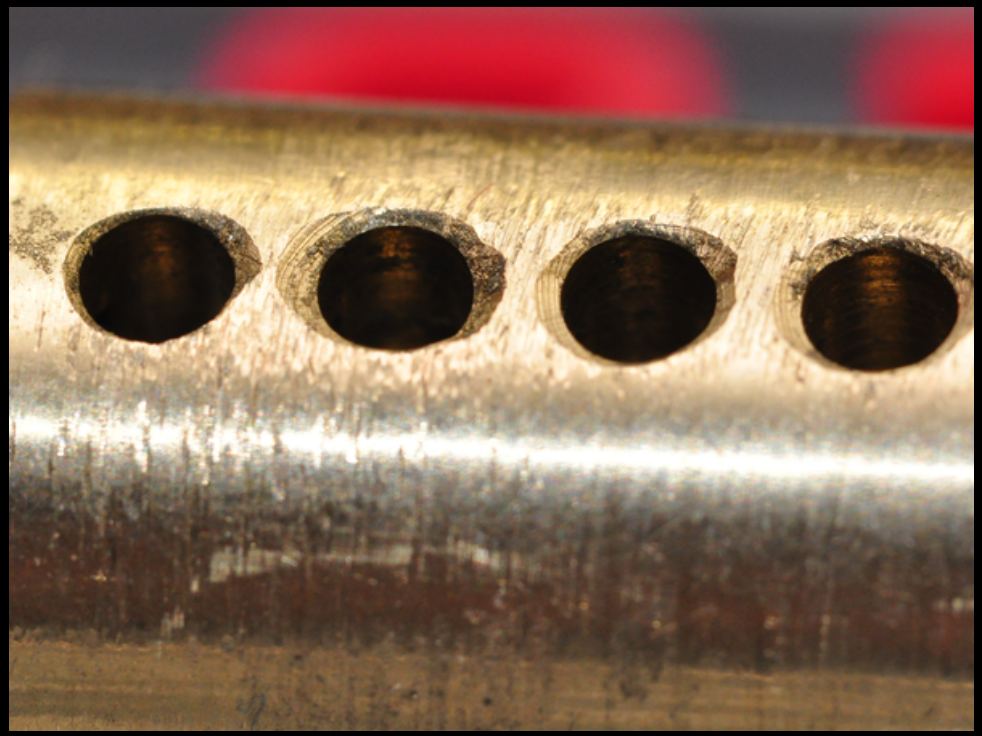
Okay, so how does it work?

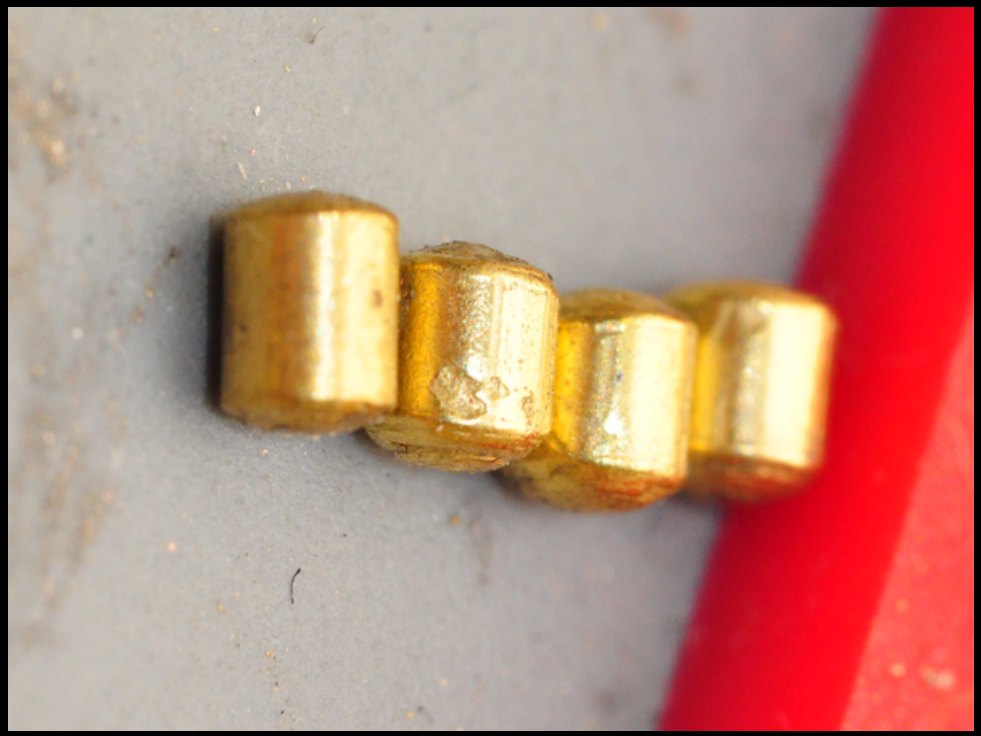
In the real world, holes can't be drilled perfectly straight, and have some variance.



Okay, so how does it work?

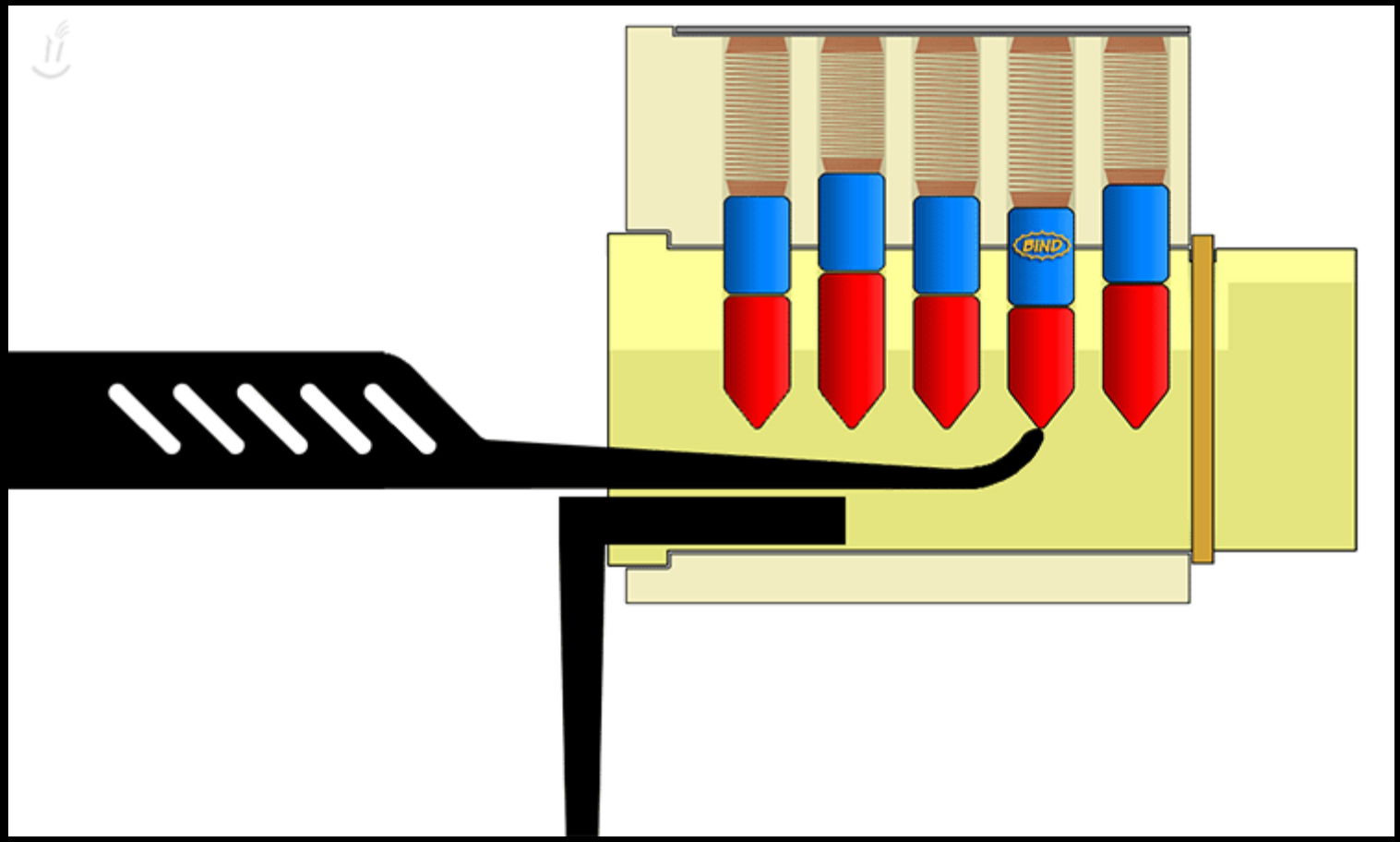
Some real world examples:





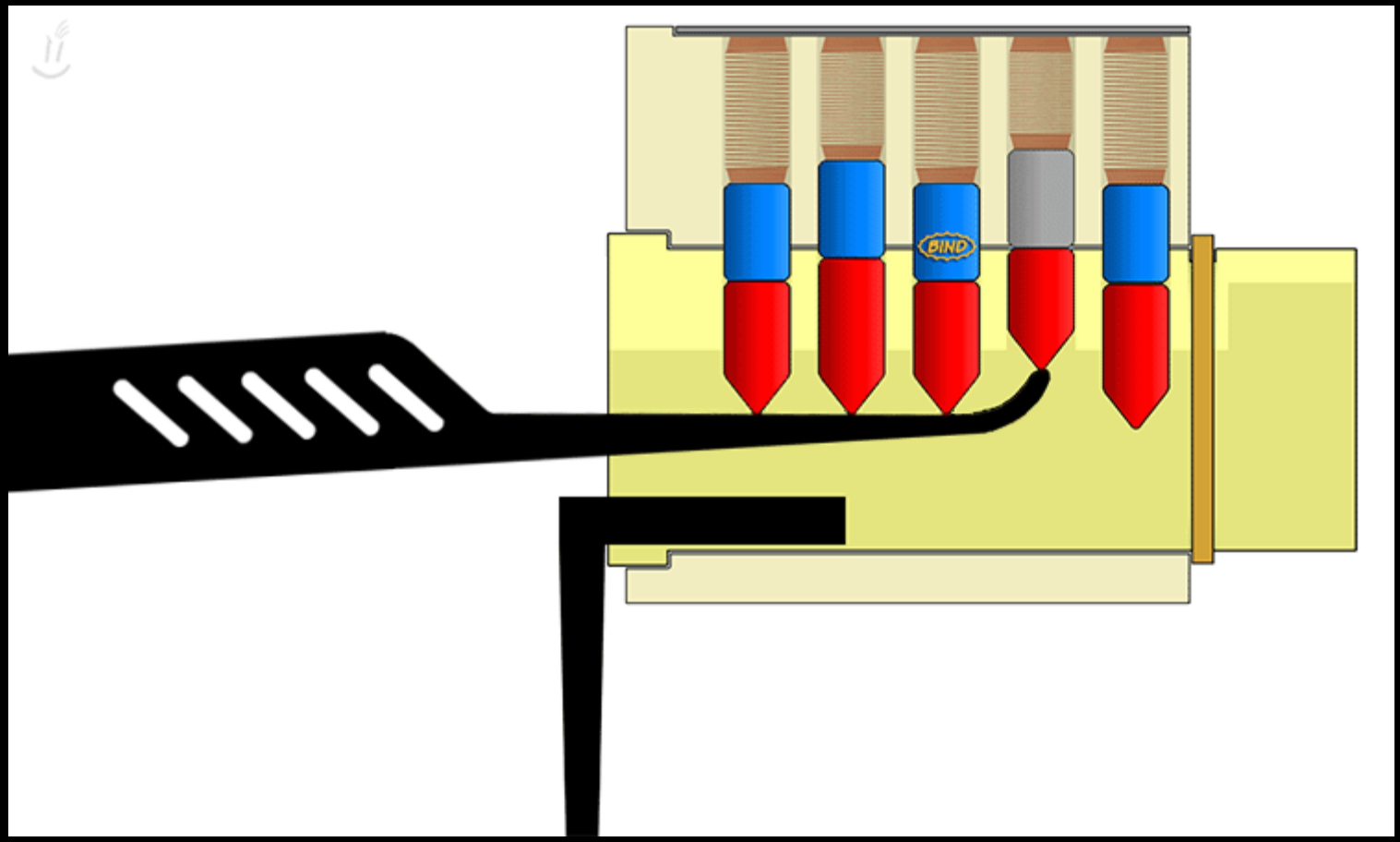
Single Pin Picking

Since there's no way to perfectly line up the pin stacks, rotational force on the plug will cause a driver pin to bind. The binding pin can now be set manually.



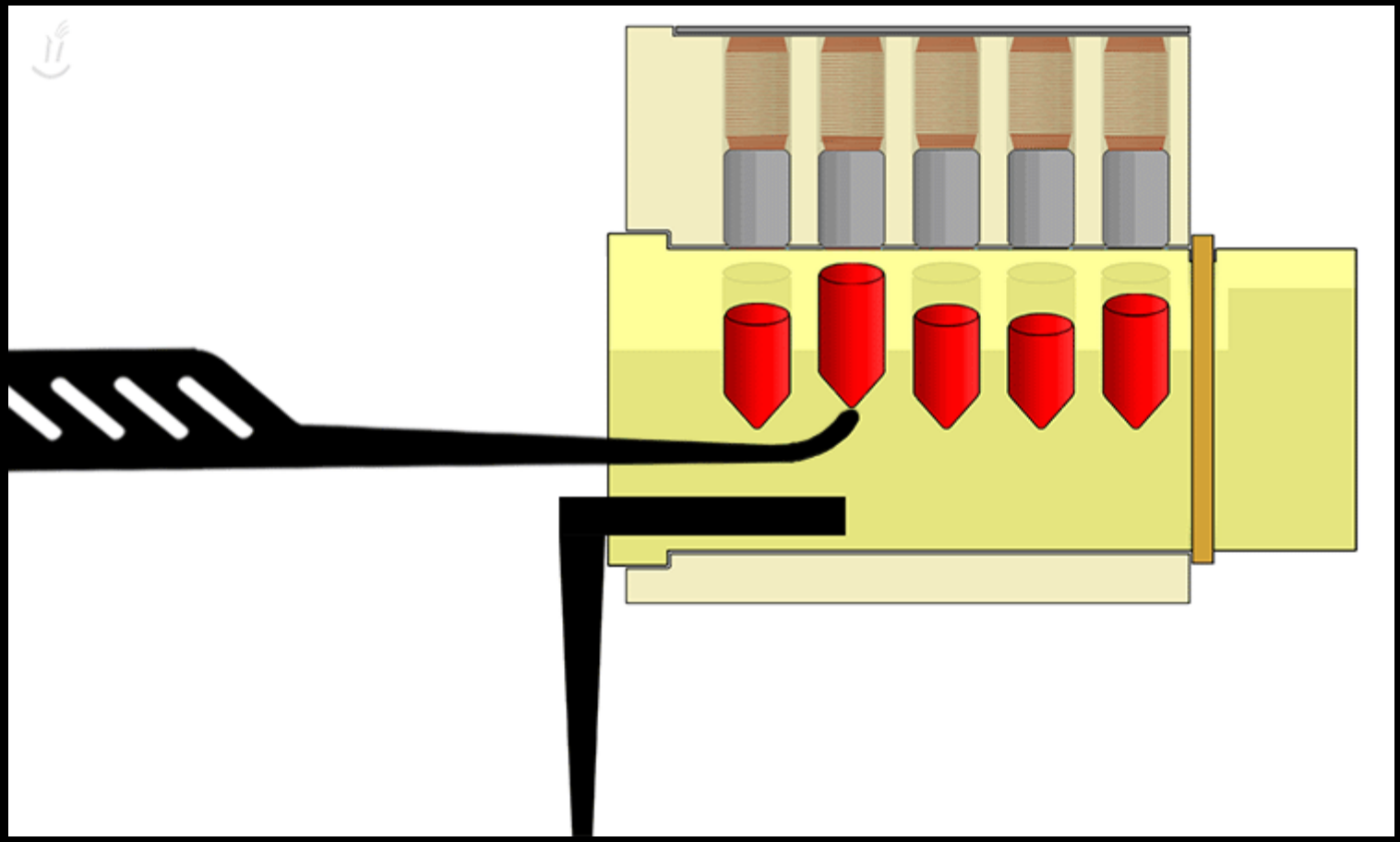
Single Pin Picking

A pin is set when the key pin reaches the sheer line. The driver pin stays in the housing, and the key pin drops back to the bottom of the chamber. Another pin will now bind.



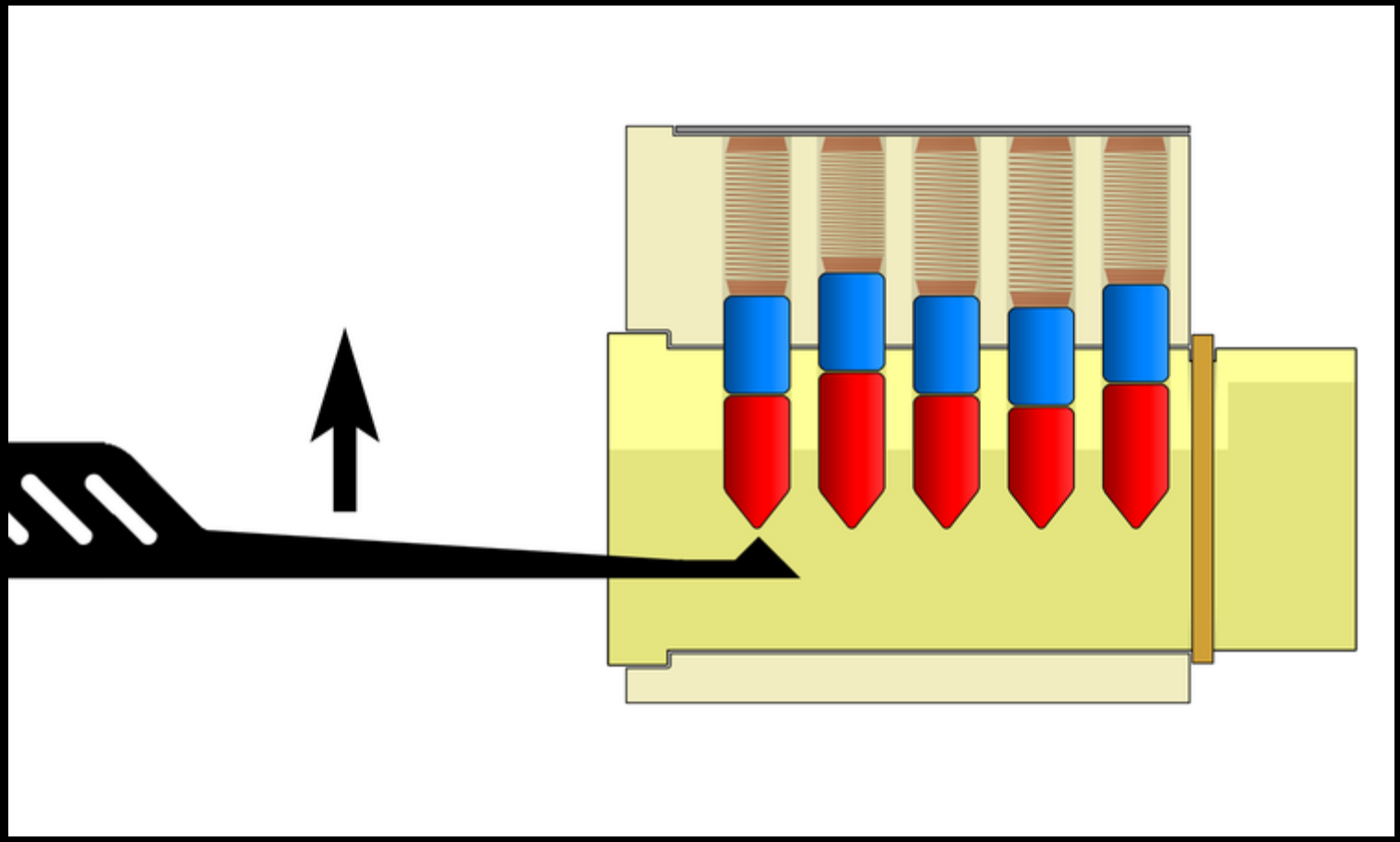
Single Pin Picking

This is repeated for each pin in the lock. Once the last pin is set, the plug will rotate, and the lock is open.



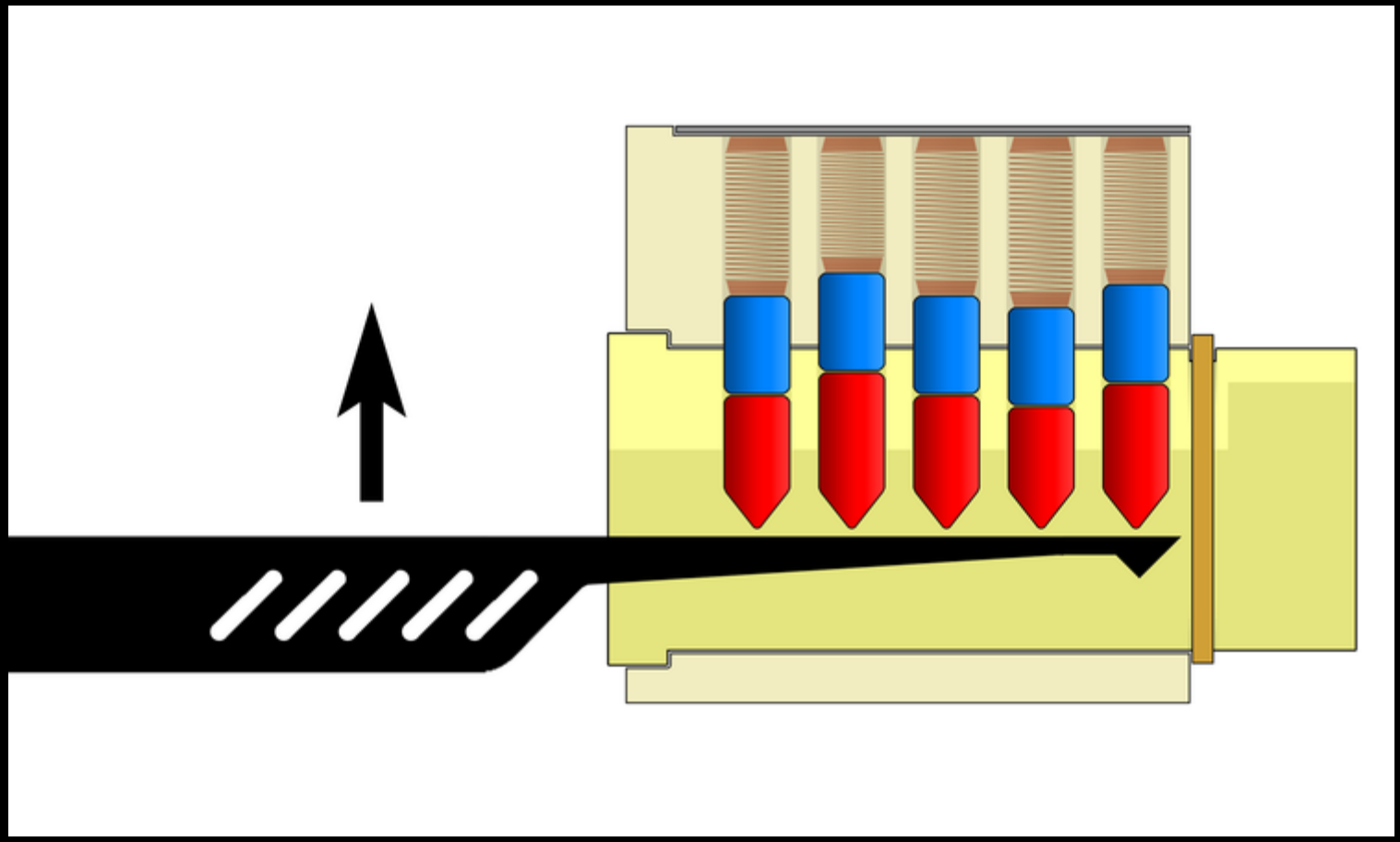
Single Pin Picking

This can also be done with a half-diamond pick.



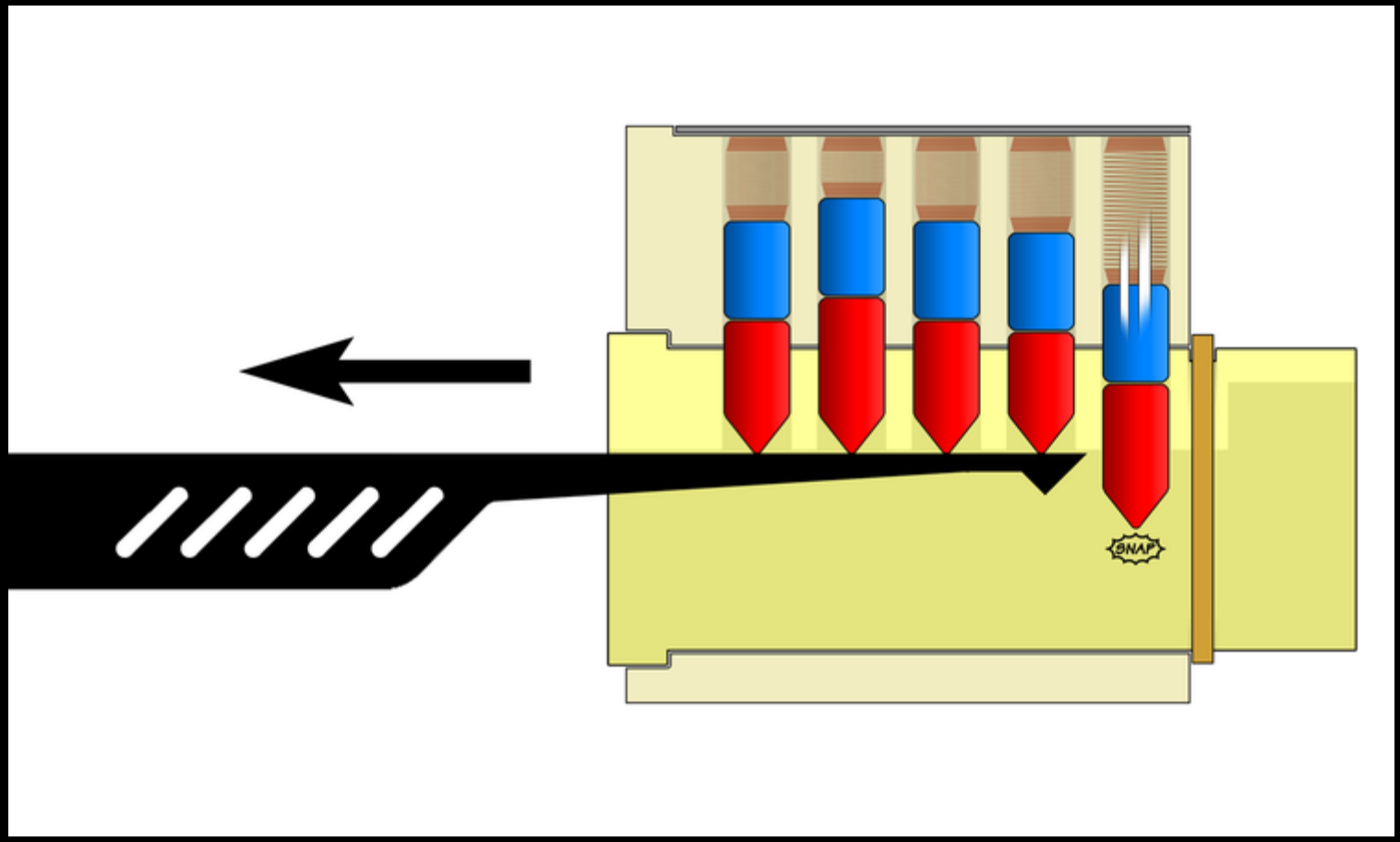
Counting the Pins

The half-diamond can also help you count how many pins are in use. Use the back of the pick to lift all of the pins.



Counting the Pins

Slowly slide the pick out of the lock, and listen for the click as each pin snaps back to the bottom of the chamber. Count the clicks to determine the number of pins.



Tension

Tension is the rotational force exerted on a plug. This is what binds the pins between the plug and housing, and ultimately rotates the plug.

Only a small amount of tension is needed to pick a lock. Too much tension increases the friction on binding pins, and will make picking difficult.

If you're ever having trouble picking a lock, remove all tools from the lock and try again with less tension.

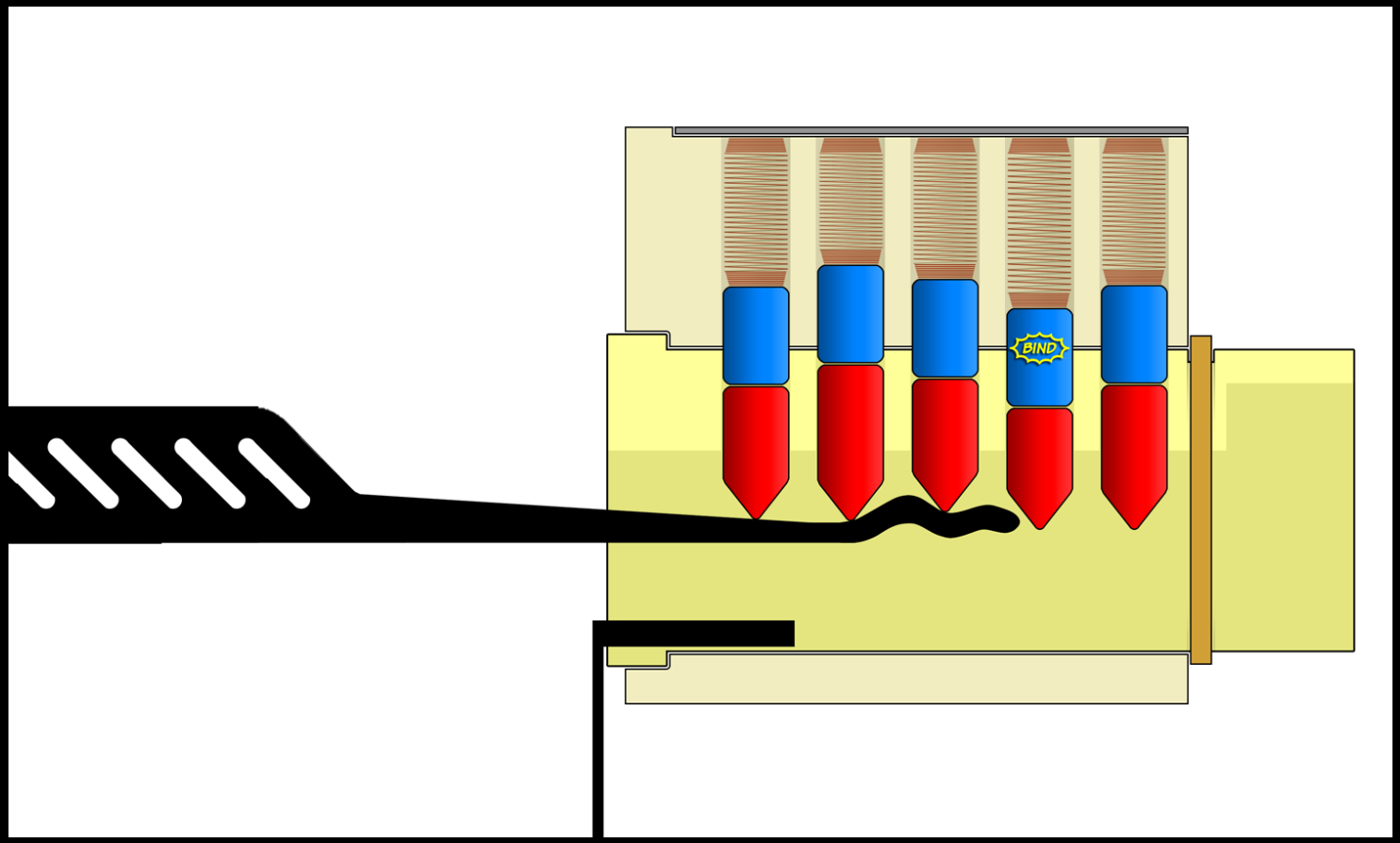
Resistance

Pin stacks give some feedback while picking. A lock picker must learn what a pin feels like in different situations.

- Normal pin stack - spring resistance only
- Binding pin - spring resistance + binding friction
- Set pin - no spring resistance, unable to lift higher

Raking

Raking is a technique that manipulates multiple pins simultaneously. It requires less feeling, but is less accurate.



Other Types of Attacks

- Bypass
- Bumping/Snapping
- Impressioning
- Decoding
- Destructive force

Security Mechanisms

- Additional pins
- Security pins
  - Spool
  - Mushroom
  - Serrated
- Sidebars

How this relates to InfoSec

Lock picking can be extremely useful on a pentest. Assuming physical security is part of the engagement, lock picking can be an invaluable skill.

The more doors, desks, and filing cabinets you can open, the more information you can find. The more computers and servers you can gain physical access to, the more attack vectors you have available to you.

Tools

TOOOL's Beginner's Blend pick set is a great starting place!

Locks and tools can also be purchased from many places:

- TOOOL, www.toool.us
- Southern Specialties, www.lockpicktools.com
- Storm Lock Picks, www.stormlockpicks.com
- Brockhage, www.lockpicks.com
- Southern Ordnance, www.southord.com
- Many, many other places online, shop around www.google.com/?q=lock%20picks

Tools can also be hand-made with inexpensive materials, such as old windshield wiper blades and hack saw blades!

Community Interaction

Many groups have interest in lock picking:

- TOOOL chapters
- LockSport International chapters
- DEFCON groups
- 2600 chapters
- Security conferences
- Hackerspaces/Makerspaces

Community Interaction

Other TOOOL Chapters and Locksport groups exist all around the US: toool.us/meetings.html

Community Interaction

If you're having trouble finding a local group, try gathering a few friends to practice together. Make it a recurring event, start inviting more people, and you'll eventually have a regularly meeting group of your own!

Questions

Jess Hires
jess@hacksonville.com
www.JaxLocksport.com