Lockpicking

Dylan Smyth – CorkSec 2016

This talk will cover...

- What is Lock picking & why does it matter?

- Pin Tumbler Locks

- Picking & Raking

- Security Pins

- Bypass

- Prevention

What is Lock picking?

- Non-destructive form of entry

- Manipulation

- Fun!

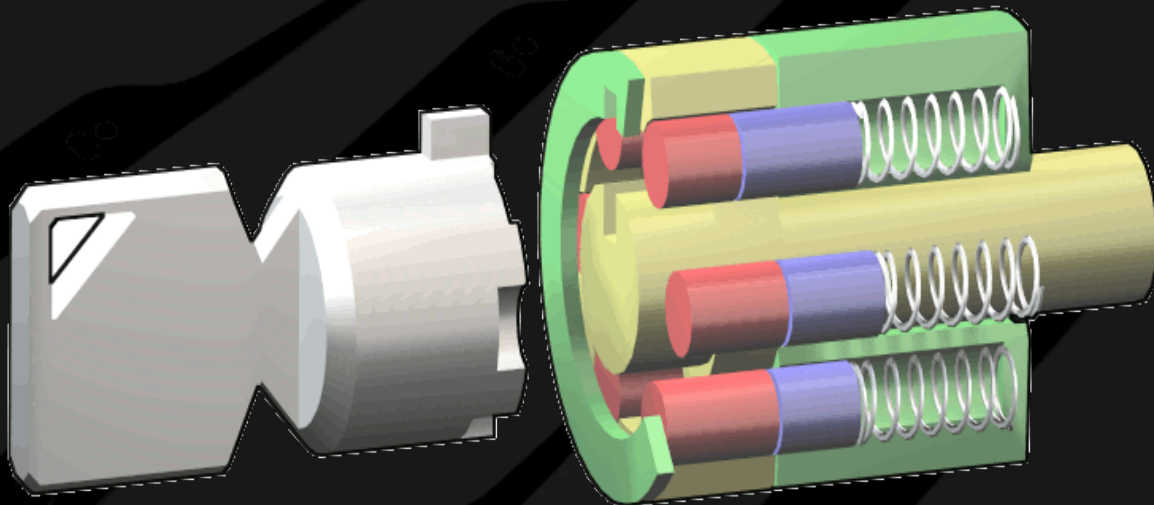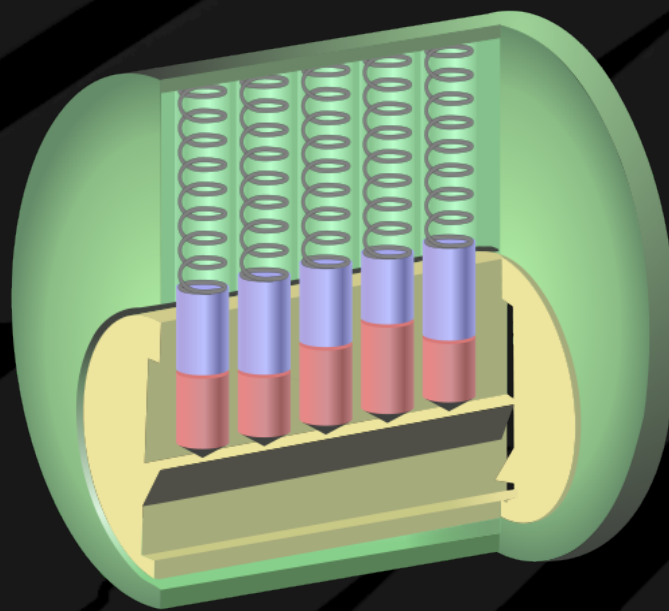*Only attack locks you have permission to attack!

Why does it matter?

- Physical Security

Pin Tumbler Lock

- Found in...

    - Cylinder Locks

    - Tubular Pin Tumbler Locks
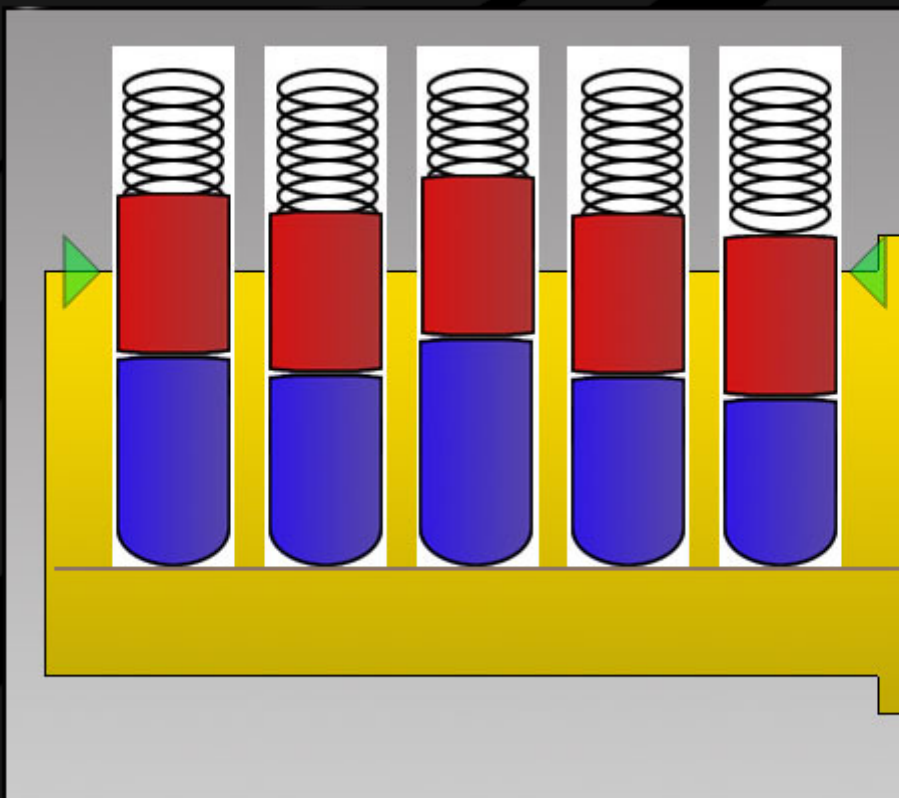
Pin Tumbler Lock
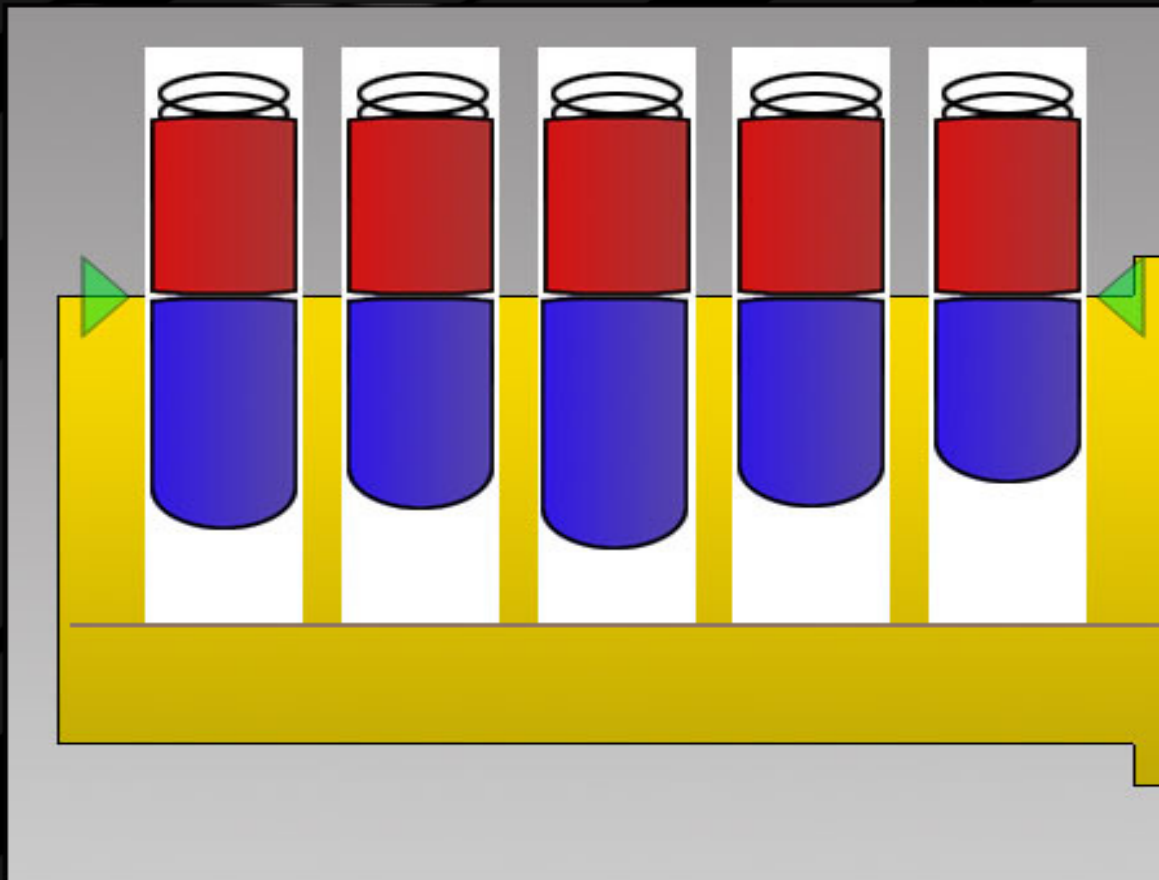
Components

Shell
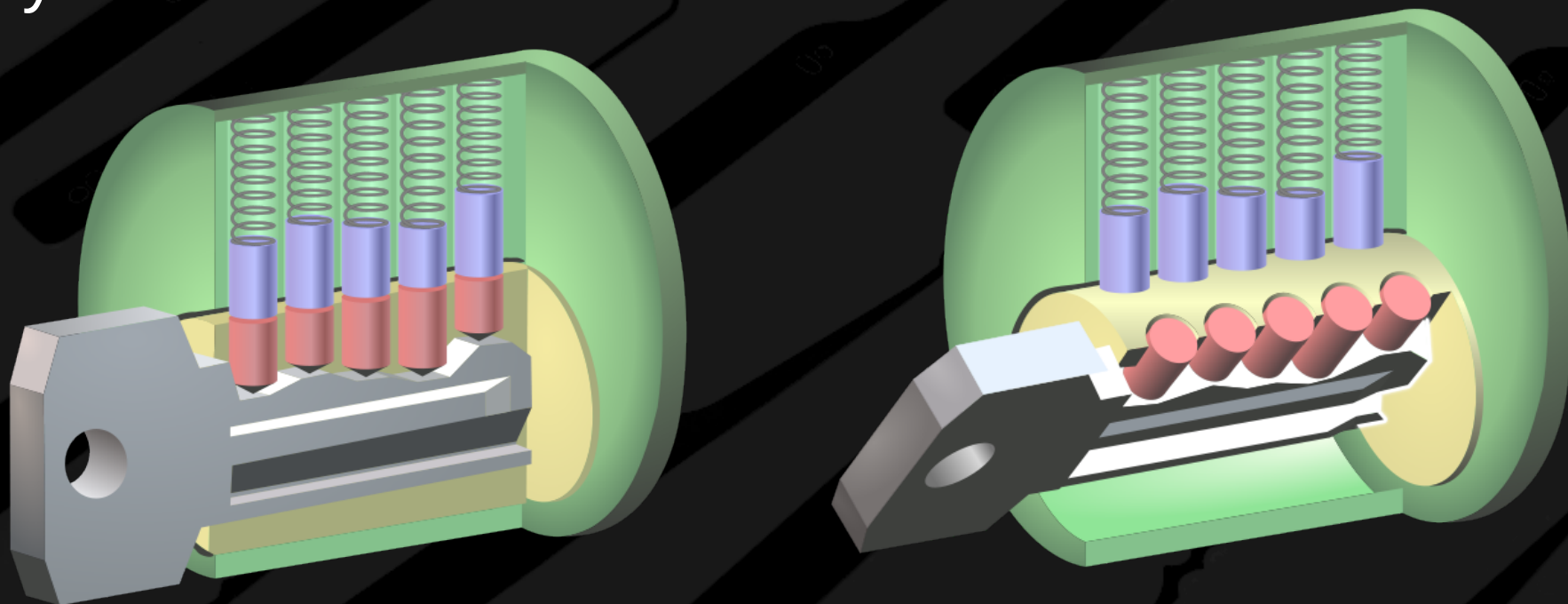
Plug

Driver Pins

Key Pins

Shear Line

Pin Tumbler Lock

When the pin stack is split at the shear line, the plug may turn.

Pin Tumbler Lock

This state should only be reached when the correct key is inserted.
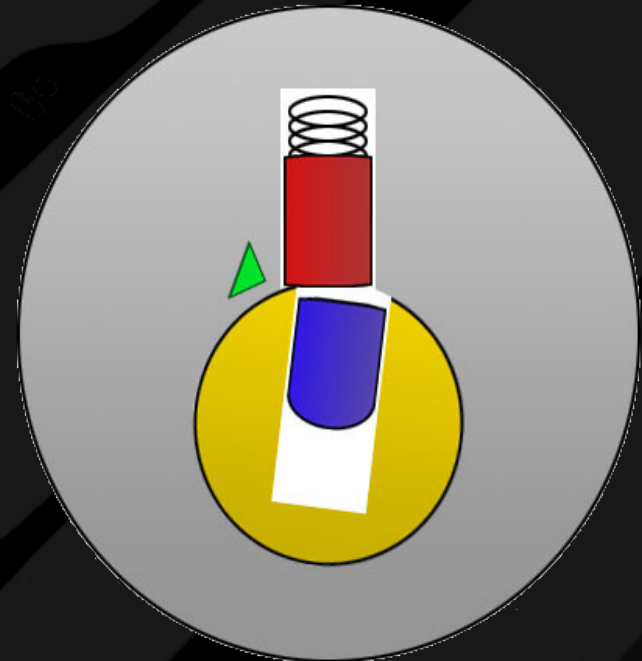
Pin Tumbler Lock

- Imperfections in the lock can be exploited.

- The Binding Effect
    - Caused by minute differences in pin diameter and/or pin chamber alignment.

    - When tension is applied to the lock, the only one pin will bind against the chamber.

    - This pin can then be set and the next largest pin will bind.

Pin Tumbler Lock

- Exaggerated example of imperfect pins:
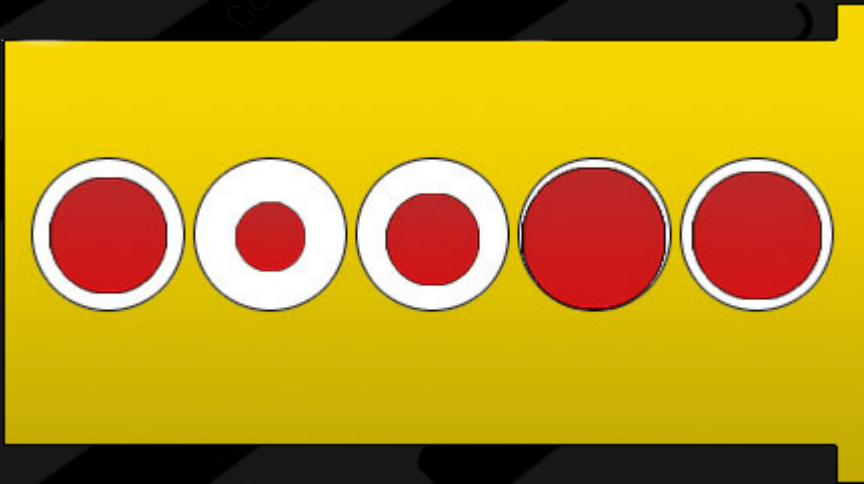
- When a pin is set, the next binding pin will allow the plug to rotate just enough to hold the set pin in place.
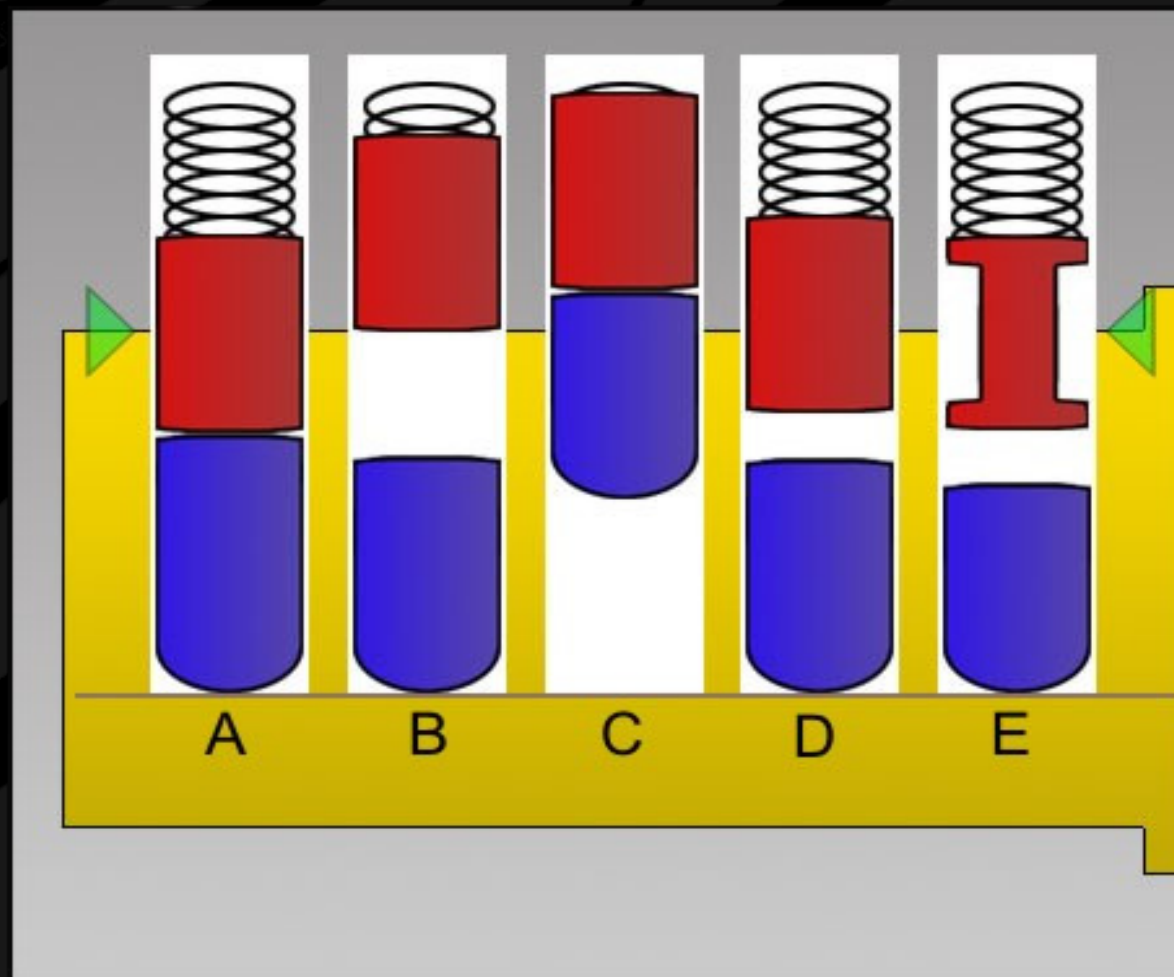
Pin Tumbler Lock

- Pin States

A) Resting
B) Set
C) Over Set
D) Under Set
E) False Set

Picking & Raking

- Tension is applied to the lock using a Tension (Torsion) Wrench. (Shown in red)

- The binding pin is set using a Pick or a Rake.

Picking

- Steps:
  - 1. Find binding Pin
  - 2. Set it
  - 3. Repeat

- Speed Bump Method
  - Place the pick at the rear of the lock
  - Drag over the pins until a pin doesn't feel as responsive as the others. This is the Binding pin.
  - Set the pin and repeat.
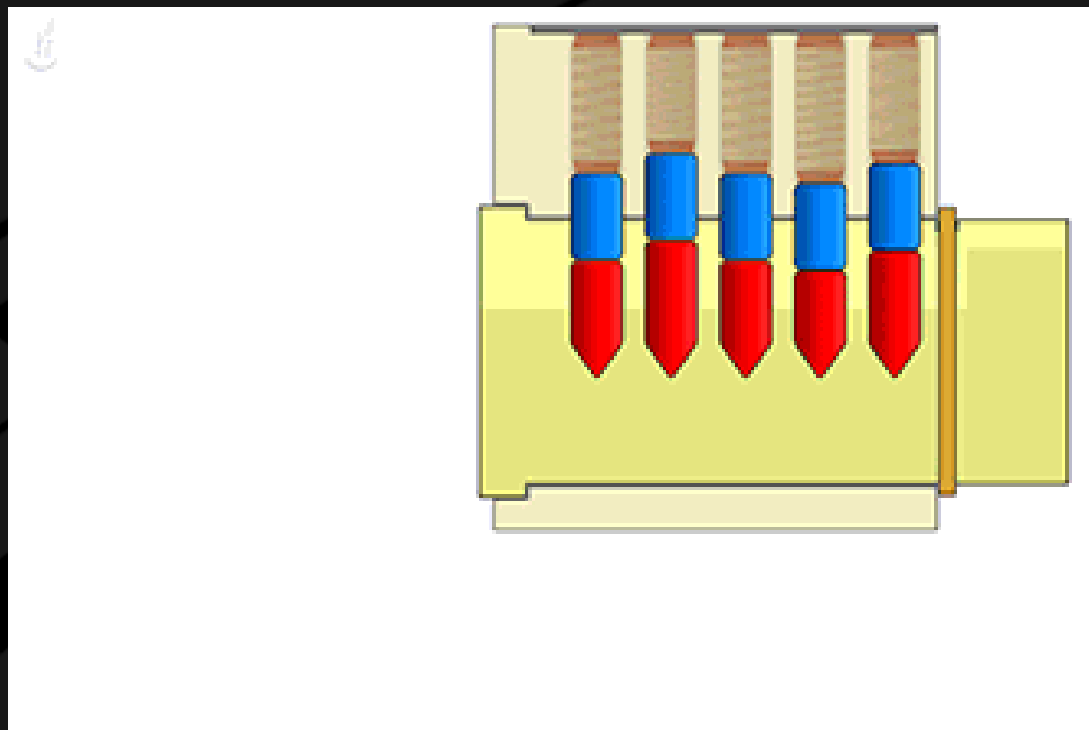
Picking

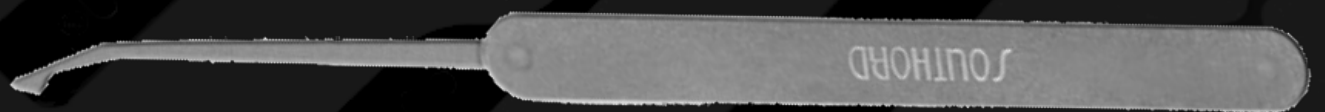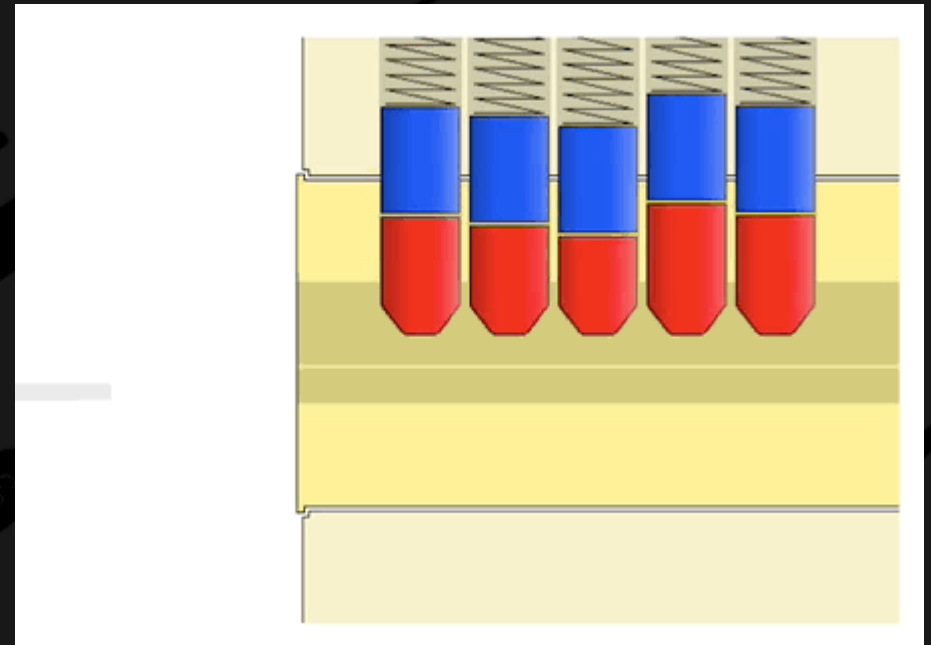- Common Pick Types

Half-Diamond

Hook

Single Ball

DeForest

Raking

- More aggressive than picking.

- Aim is to bounce the driver pins into the set position.

- This is done by quickly running (or "raking") a rake back and forth over the pins.

Security Pins

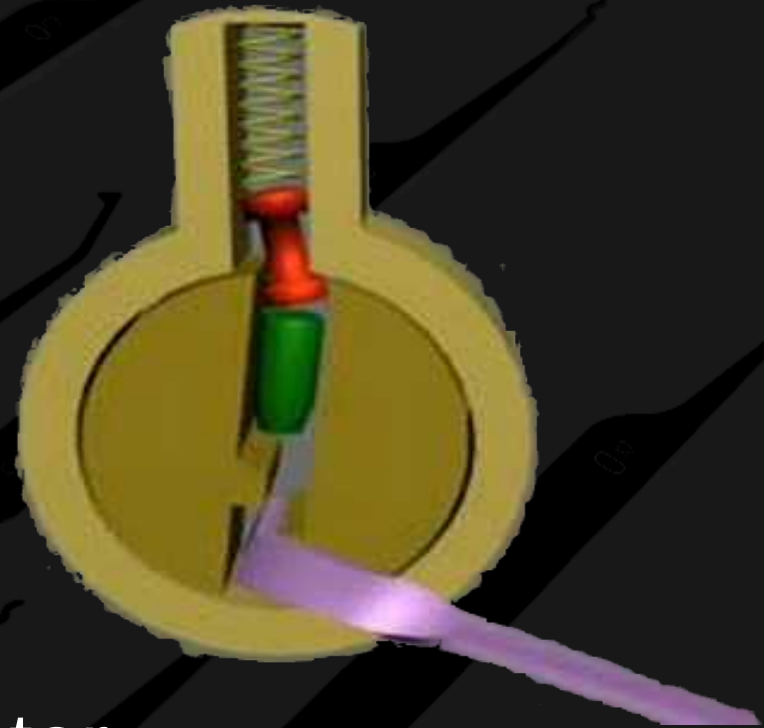- Security pins can be used in place of a regular driver pin, key pin, or both.

- The aim is to have the pin get caught at the shear line, disrupting the picking attempt.

- Many types; Mushroom, Serrated, Spool....
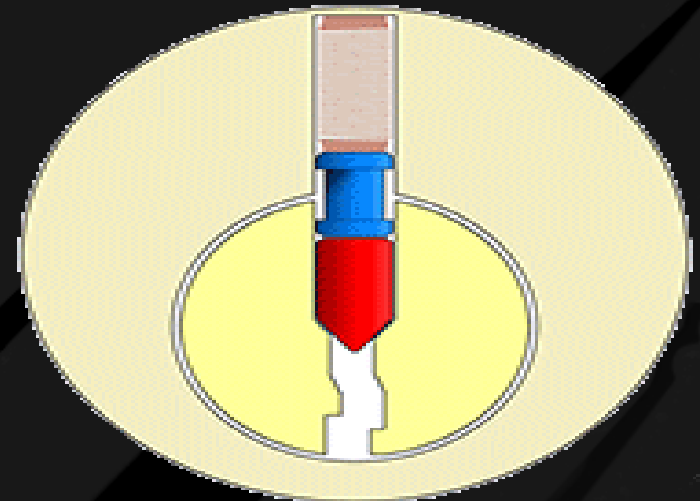
Security Pins

- Spool Pin

  - Most common type of security pin.

  - Contains a long narrow center.

  - This pin will bind only when all other pins have been set. This creates a "False Set".

Security Pins

- Spool Pin

    - They can still be beaten!

    - When a Spool Pin binds, it identifies itself.

    - When it is identified...
        >Apply pressure to the pin
        >Reduce the tension until the pin sets.
        >Reset any pins which have unset in the process.

Bypass

- Lock mechanisms on some padlocks can be bypassed altogether.

- This is made possible by lack of a "shield" between the key way and the actuator.

- A tool is inserted through the key way and used to move the actuator, opening the lock.

Prevention

- For high security locks, security pins are not enough.

- A "Side-Bar" adds another obstacle to the picking process.

- A shield in a padlock can prevent a bypass.

- The shield is an object which simply divides the key way from the bolting mechanism.

Questions?