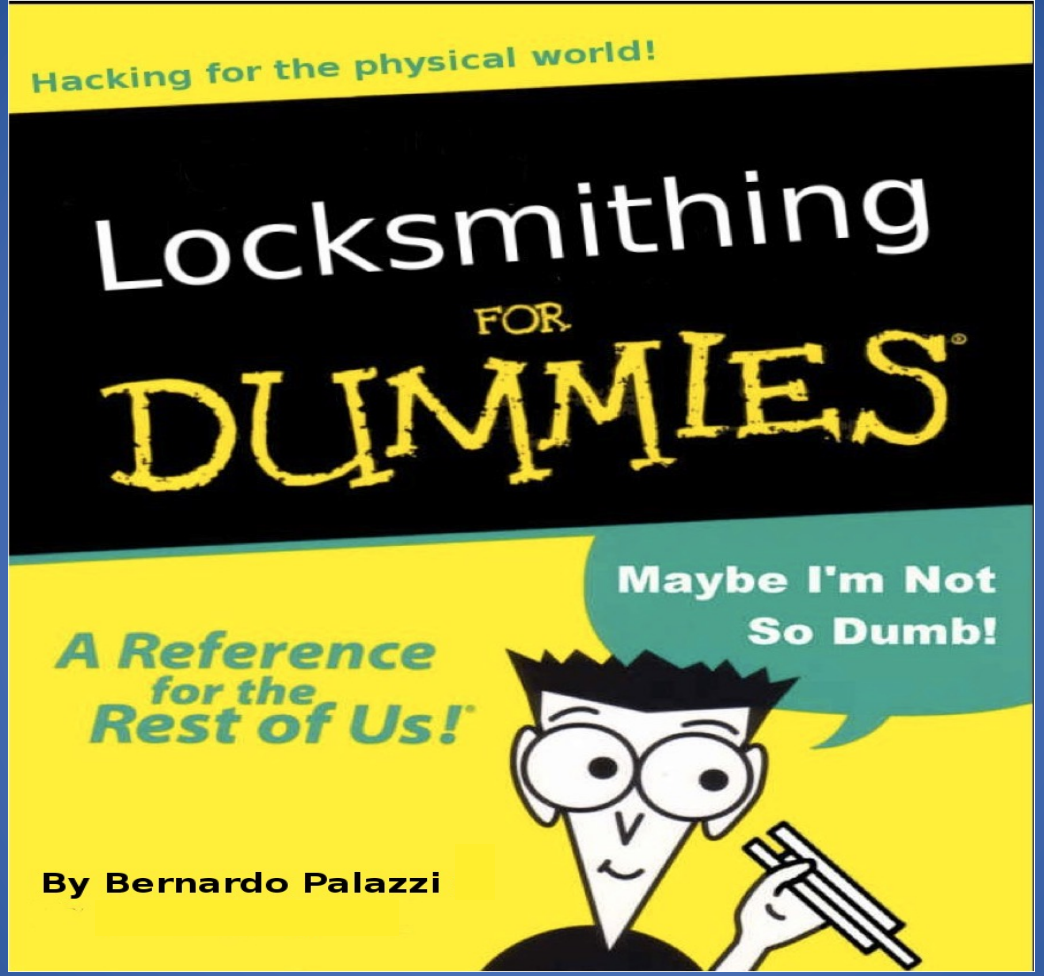

Hacking for the physical world!
Locksmithing
FOR
DUMMIES
Maybe I'm Not So Dumb!
A Reference for the Rest of Us!
By Bernardo Palazzi

Legal Notice

- Laws regarding lockpicking vary significantly state-by-state
- In most states purchase and possession of dedicated lockpicking tools is legal
  - Penalties are raised significantly if you get caught using them in commission of a crime
  - Typically moves an offense from a civil offense or misdemeanor to a felony

What Is Physical Security?

- Any physical object that creates a barrier to unauthorized access
- This includes: locks, latches, safes, alarms, guards, guard dogs, doors, windows, walls, ceilings, floors, fences, door strikes, door frames and door closers

Is Physical Security An IT Concern?

- You have been working hard to secure your network from cyber attacks
  - Redundant layers of antivirus programs, firewalls and intrusion detection systems should protect against every possible electronic method of entry
- But what if an attacker gains access to the server room or network wiring closet ...
- Is you network still safe?

Compromising Locks

- For centuries, the lock has been one of the cornerstones of physical security
  - We rely on dozens of them every day to protect people and assets
- The trust most people place in locks is unwarranted
  - Most locks can be easily compromised with nondestructive methods
  - Sometimes within seconds and with readily available tools
- “Locks keep honest people honest”

Destructive vs. Nondestructive Entry

- Destructive entry
  - Involves using force to defeat physical security
  - Methods involve crowbars, bolt cutters and sledge hammers
  - Negative impact on IT resources is apparent
  - Remediation steps also obvious
- Nondestructive entry
  - Compromises security without leaving signs of a breach
  - Defeats intrusion detection
  - Greater and long-term threat

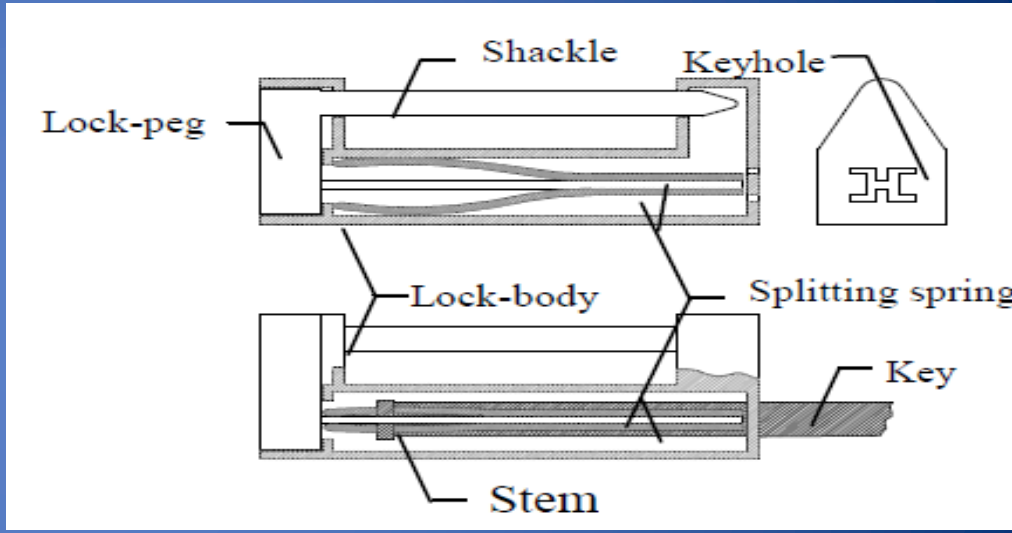
History of Locks Vs. Encryption

- Very easy to break
- Very few physical keys
  - The width and the length of the key
- Few combinations C^S
  - Difficult to use with a large number of cylinders (C) and symbols (S)
- Effective because people were not good at casting iron or algorithms

- Very easy to break
- Very few possible encryption keys
  - i.e. 1-26 letter shift
- Effective because people were not able to read (illiterate)

Splitting-spring lock

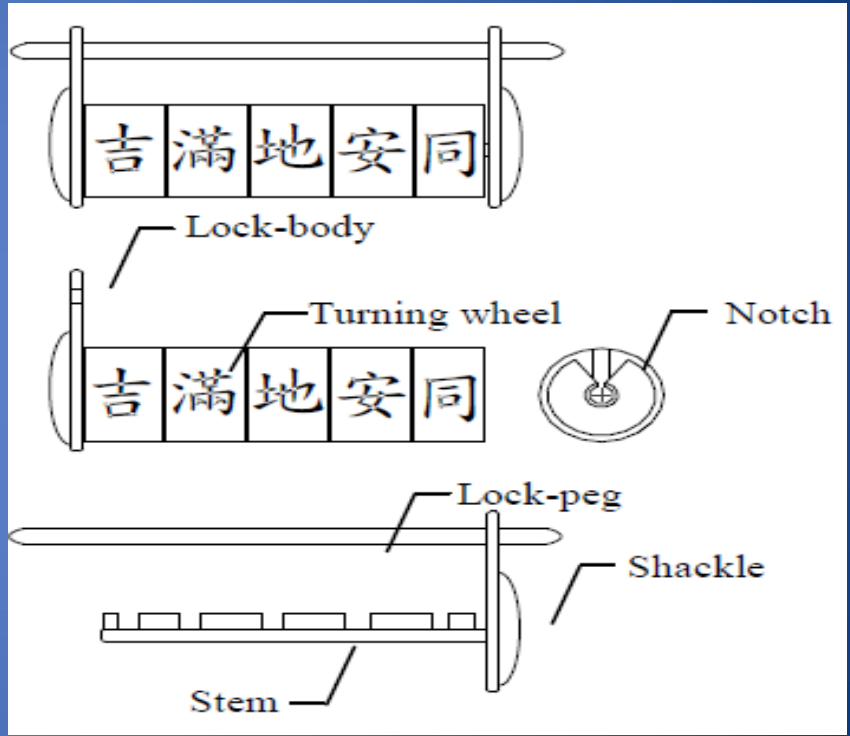
- Lock body has a Keyhole
  - key to insert
  - supporting guide for the sliding bolt to move
- Sliding bolt
  - a shackle for hanging the lock
  - a stem for bonding one end of the splitting springs
  -
- If locked: sliding bolt is trapped by the opening springs against the inner wall of the lock-body.



•For opening, key is inserted and its head squeezes the opening springs so that the sliding bolt can exit from lock-body.

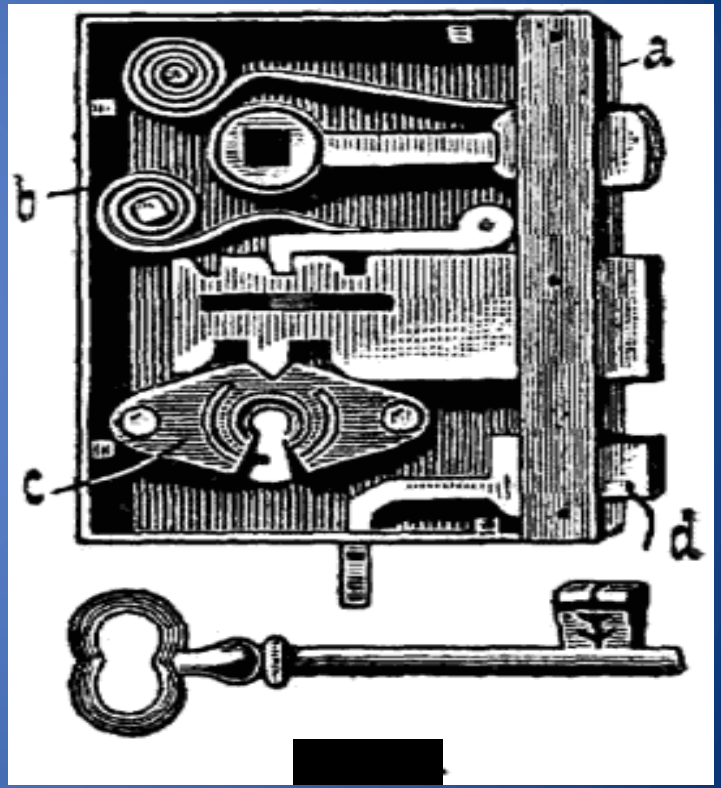
Letter-combination lock

- Lock-body has an axis with rotating wheels for guiding the movement of the sliding bolt
- Rotating wheels have same size with four letters engraved on the surface
- When all letters are in the correct position a channel is formed that allows the stem to slide apart from the lock-body



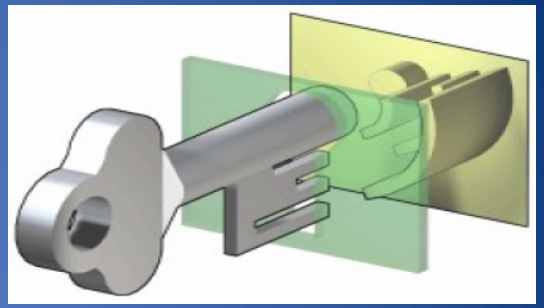
Warded Locks

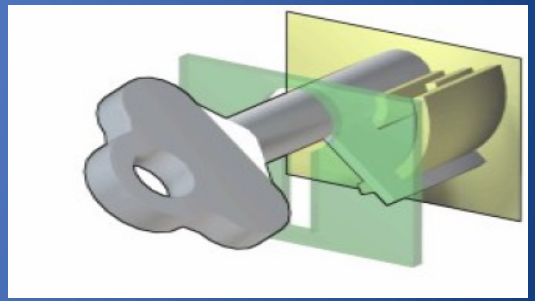
- Locks of this type were used in ancient times
- The key moves the bolt assisted by a support spring
- Security relies on the fact that not all keys pass through the key hole

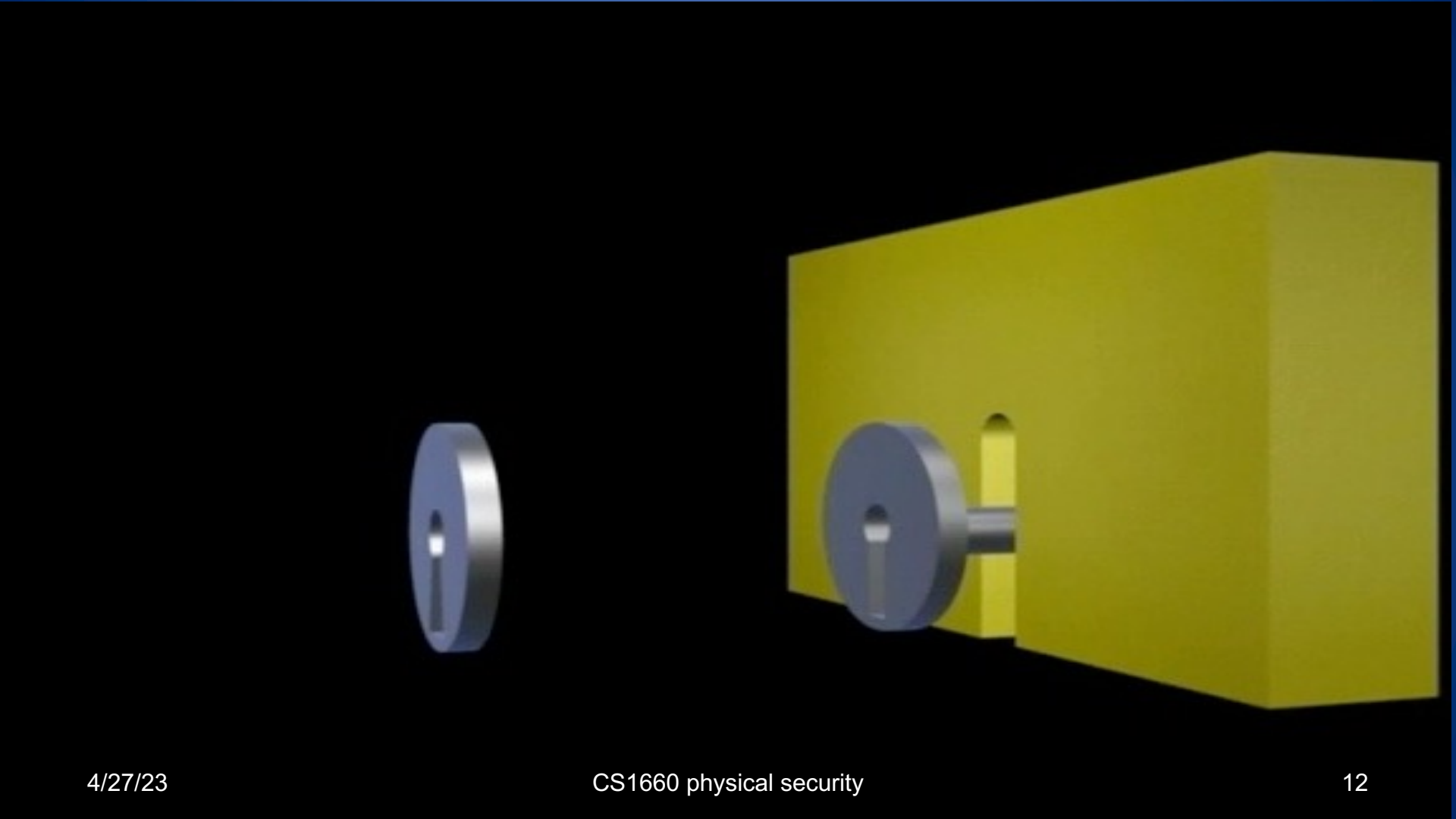


Skeleton Key

- Usually in old style doors or desks
- Different concentric obstructions
- Easy to lock pick with Skeleton keys
- They come from ancient Rome



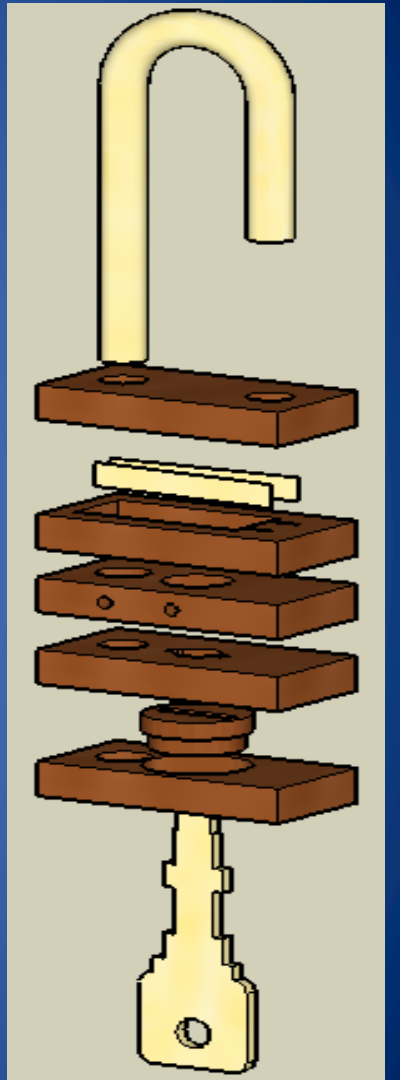




Warded Picks

- Warded padlocks have a number of elements that are superimposed to determine the profile of the key

- Easy to "break open" with a set of key samples



CS1660 physical security

Pick vs. Bypass

Break open a lock in a nondestructive manner can be achieved either through:

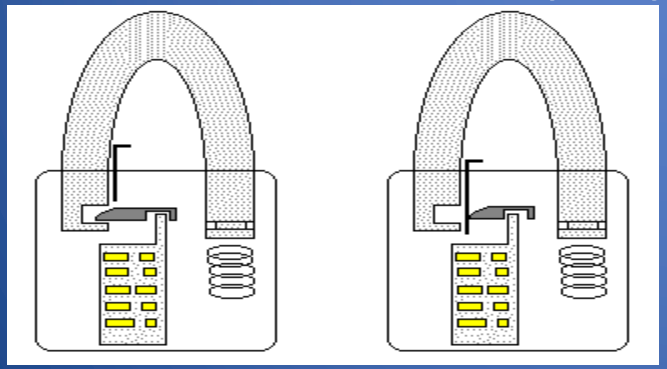
- Pick: acting on the lock mechanism simulating the operation of the key
- Bypass: manipulation of the bolt without using the lock

TSA Lock

- The U.S. government has established a set of rules for the inspection of baggage without the presence of passengers
- Special TSA-approved locks allow both inspection and protection against theft
- An important element is that the inspection must be easily verifiable by the user

Shims

- It is often possible to open a padlock by slipping shims in between the shackle and the lock's casing
- No need to defeat the actual locking cylinder where the key is placed



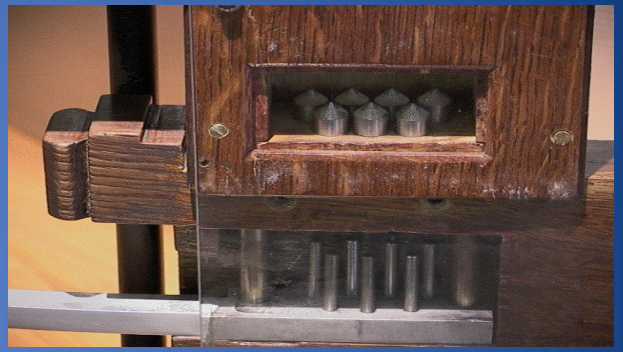
The key to remove the block that allows the lever to open

Handcuffs typically use locks Warded

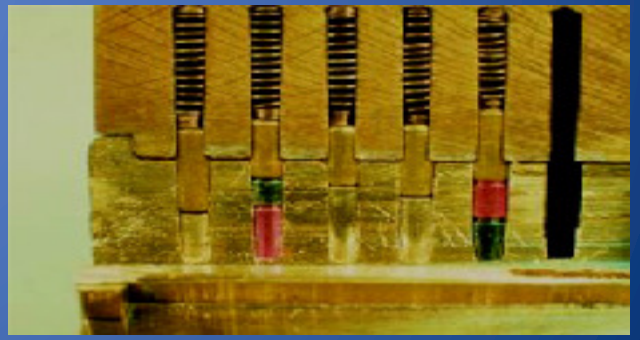
Opens the throttle inserting a shim between the rack and lock

1860: Yale Pin Tumbler Lock

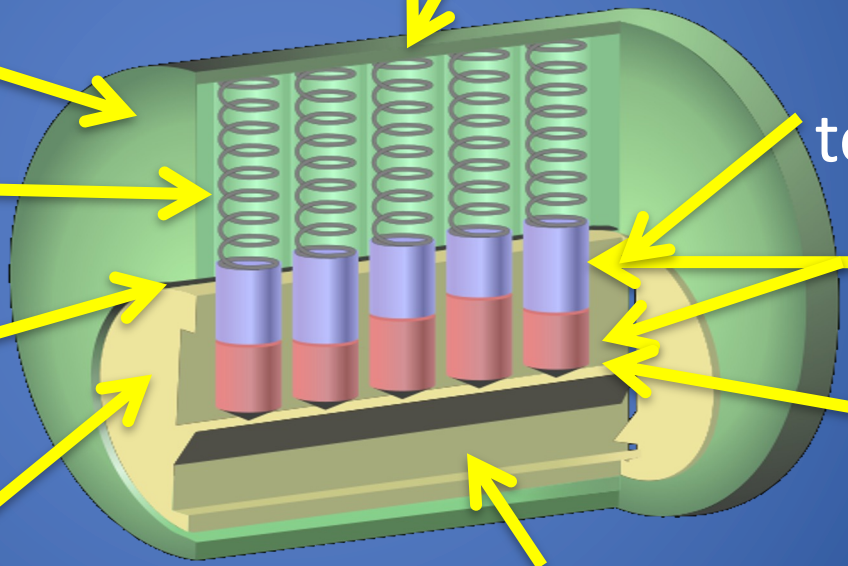
- Modern version of the Egyptian single-pin design
- Utilizes two pins for locking



- Double-detainer theory of locking
- Created shear line



Terminology



How Does a Lock Work?

LOCK PICKING

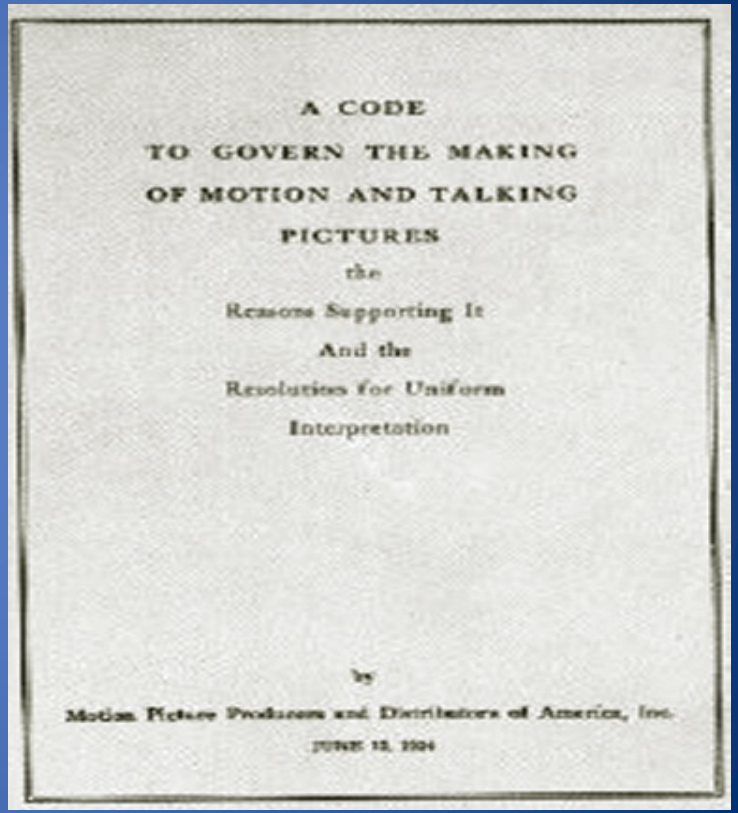
Lock Picking

- Lock picking had been the exclusive art of locksmiths, professional thieves, spies and magicians for hundreds of years
- However, with the advent of the Internet, information about lock picking methods and tools has become readily available
  - E.g., YouTube has many lock picking videos


Press Esc to exit full screen mode.

Lock Picking in Movies

- Genuine lock picking in movies used to be prohibited
- Before 1967, the Hays code (Motion Picture Production Code) required censorship of Hollywood movies
  - "All detailed (that is, imitable) depiction of crime must be removed, such as lock picking or mixing of chemicals to make explosives"



A CODE
TO GOVERN THE MAKING
OF MOTION AND TALKING
PICTURES
the
Reasons Supporting It
And the
Resolutions for Uniform
Interpretation

by
Motion Picture Producers and Distributors of America, Inc.
JUNE 13, 1934

Lock Picking

Physical object

- Lock on door, safe, etc.
- Key to the lock
- Access to room, safe, etc.

Cryptanalysis

Equivalent crypto object

- Unbroken cipher text
- Cryptographic key
- Plaintext

These techniques are based on the same principle, overcoming an obstacle that is in between you and something you are trying to access

Lockpicking Tools

- Feelers
- Scrubbers
- Tension tools

Image credit: southord.com

Picking

- It is all about exploiting mechanical defects
  - Better locks = less defects
- Conceptually a $O(n^2)$ problem lifting all pins to the correct height
  - Misaligned pin stacks reduce it to a O(n) problem or better

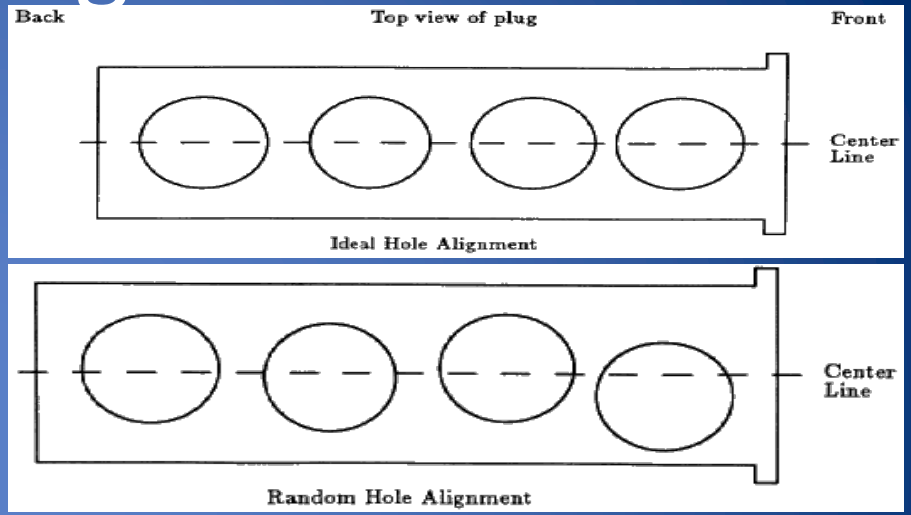
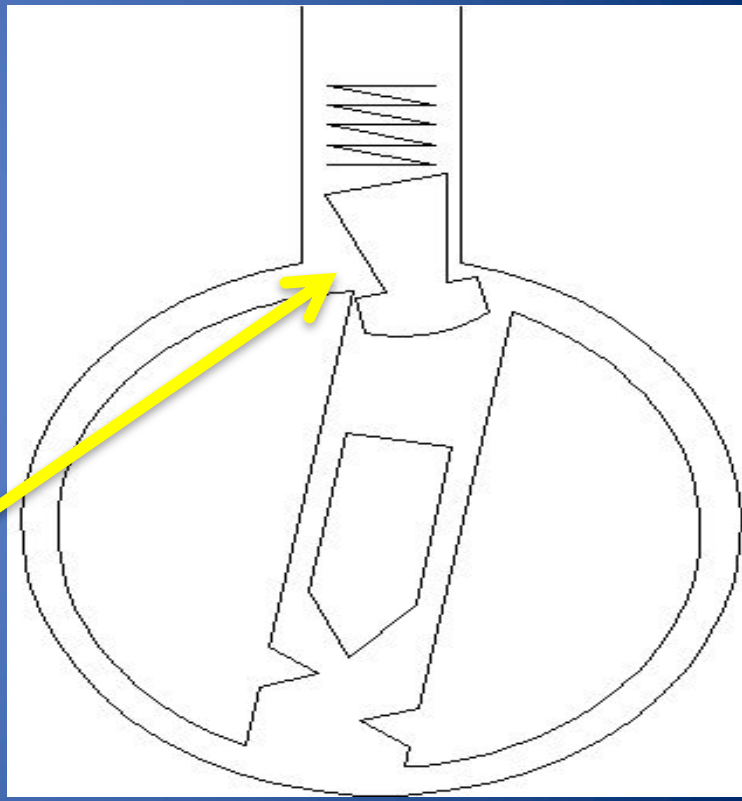


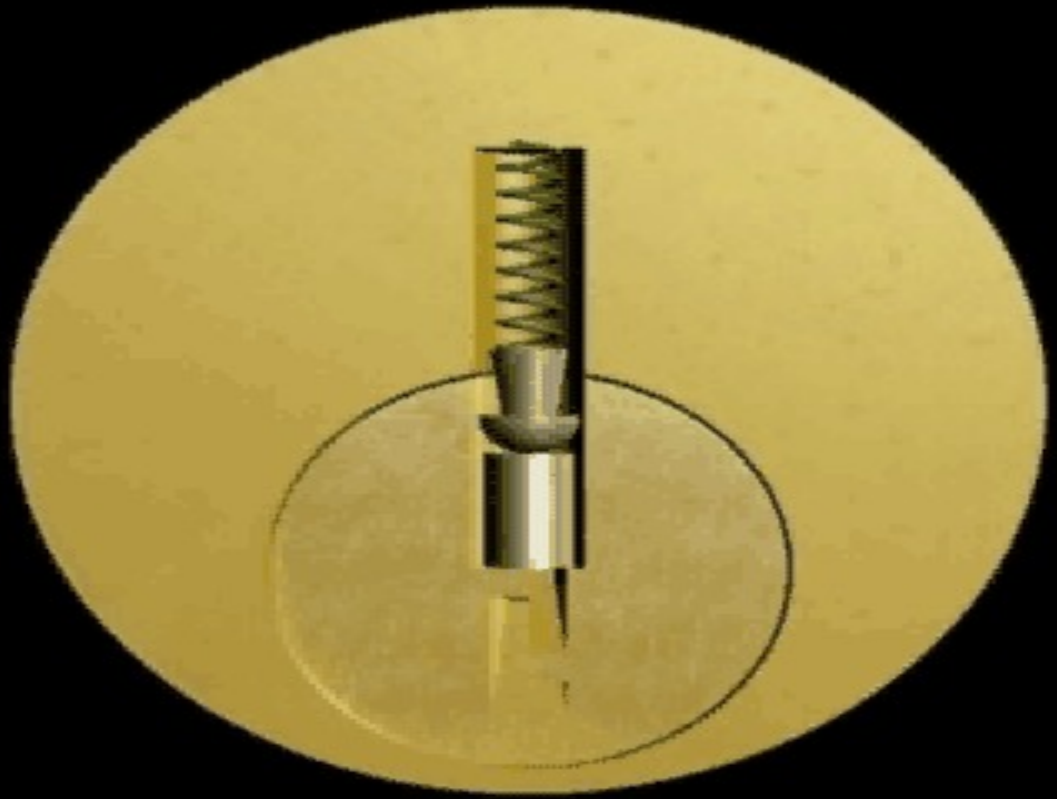
Image credit: MIT Guide to Lockpicking

High Security Pins

- Special pins can complicate a lot the task of picking

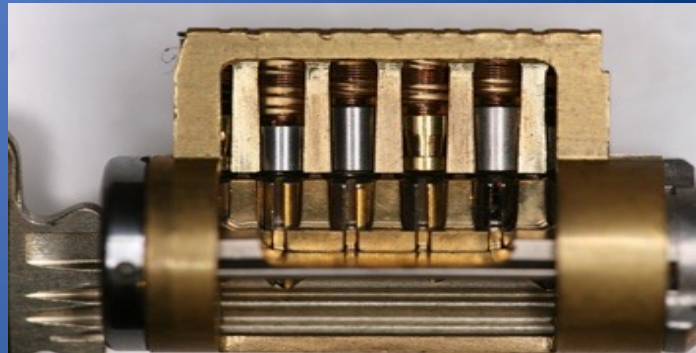
Top pin is placed in a position similar to that on sheer line but that does not allow opening



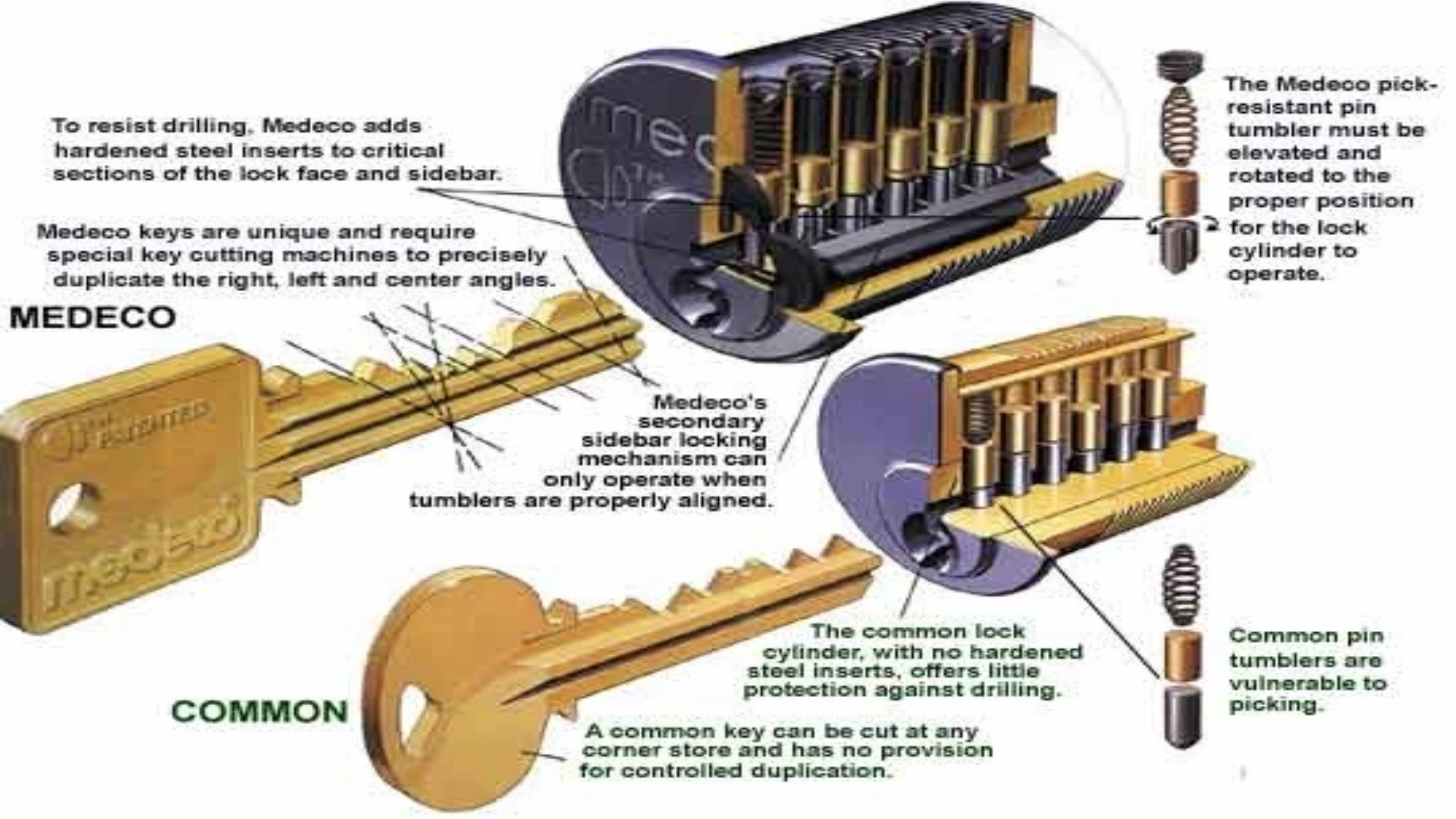


Locks for Critical Infrastructures

- Which locks protect these places?
- What characteristics do they have?
- What are they?



Medeco


To resist drilling, Medeco adds hardened steel inserts to critical sections of the lock face and sidebar.
Medeco keys are unique and require special key cutting machines to precisely duplicate the right, left and center angles.
MEDECO
The Medeco pick-resistant pin tumbler must be elevated and rotated to the proper position for the lock cylinder to operate.
Medeco's secondary sidebar locking mechanism can only operate when tumblers are properly aligned.
The common lock cylinder, with no hardened steel inserts, offers little protection against drilling.
COMMON
A common key can be cut at any corner store and has no provision for controlled duplication.
Common pin tumblers are vulnerable to picking.

CS1660 physical security

Statistics

- 4-6 pins, 4-10 levels
- $10^6 = 1{,}000{,}000$ possible keys!
- The angular positions of the cylinders allow to obtain about 180 different positions $(180 \cdot 10)^6 = 3.4012224 \times 10^{19}$
- (Un) fortunately there is a need for some tolerance in locks

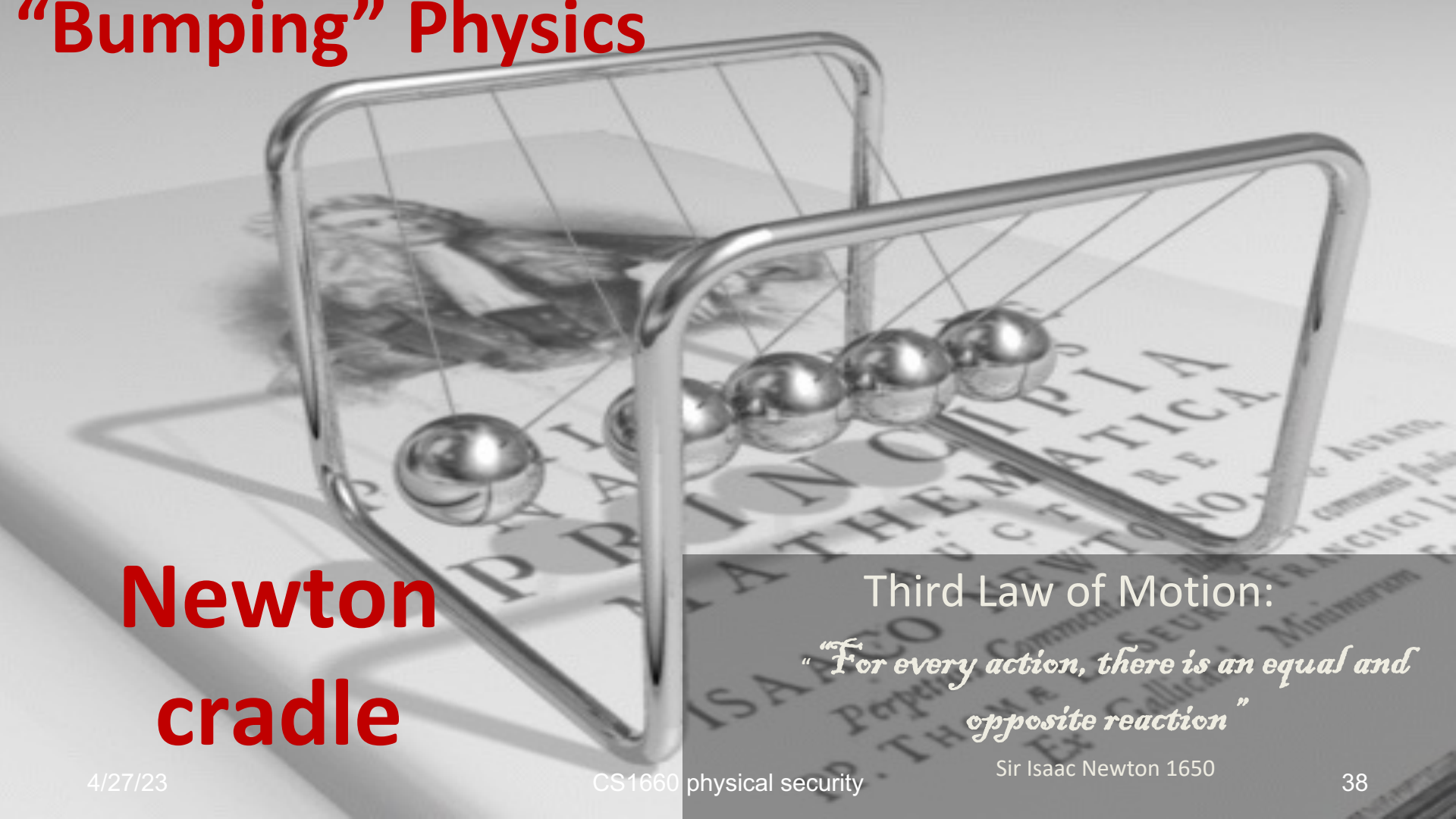
Typical enhancements

- Sidebar
- Drill-proof pins
- Slide
- Biaxial rotation
- Magnets
- Non-uniform top pin (more combinations)
- Strict chain of custody on key controls
- Electronic audit trails

Bumping

- A different way of picking locks
- Virtually all traditional Yale and similar locks can be opened by bumping
- What lock pickers say about bumping:
  - RELIABLE
  - REPEATABLE
  - SIMPLE TO LEARN

"Bumping" Physics



Newton cradle

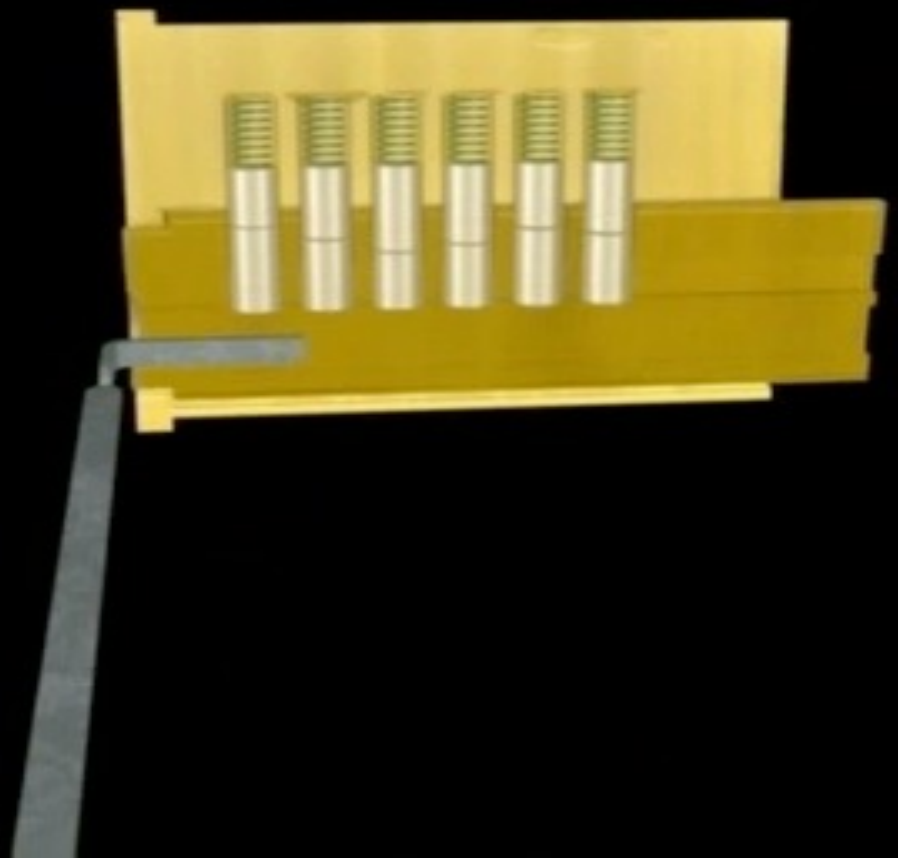
Third Law of Motion:

"For every action, there is an equal and opposite reaction"

Sir Isaac Newton 1650

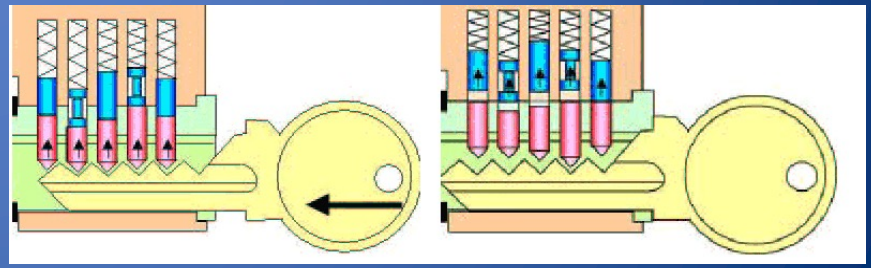
Pick Gun

- Manual and electronic pick guns are a popular method for quick and easy ways of opening up doors
- The pick gun is used in a similar way but usually has a trigger that creates an upward movement that must be repeated rapidly to open the lock



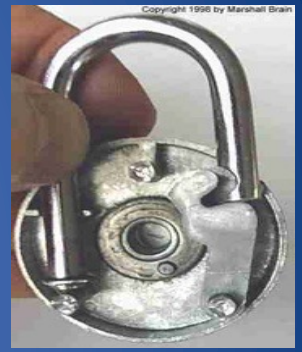
Bump Keys

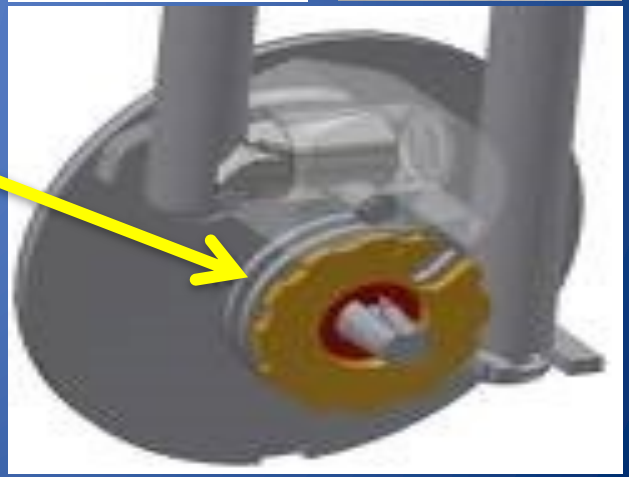
- Driver pins “jump” higher than the cylinder just for an instant
- If a light rotational force is applied, the cylinder will turn
- Lock bumping is a very fast method for opening the lock
- The lock is not damaged in any way
- Few key-pin locks cannot be bumped



Combination Lock

- There are locks that do not require a physical key to be opened but a code
- Combination locks allow attacks based on reducing the space of possible combinations to try
  - The gears have a higher tolerance of the external disk combination





Biometric padlock

- Usability
  - No need to worry about forgetting the password.
  - No need keys and mobile phones with you.
  - No need multiple steps to open the lock.
  - Easy touch solve any trouble
- Unfortunately not always secure
  - Shimming andWeak materials
- ‘Ontogeny Recapitulates Phylogeny’
  - A biological theory on evolution of the species similar to the evolution in the computer industry
  - Pay attention to avoid the repetition of old mistakes

Credits

Video:

- **Richard Edwards, Mirko Jugurdzia**
  Visual Guide to Lock Picking DVD
  Standard Publications, Inc.

Image:

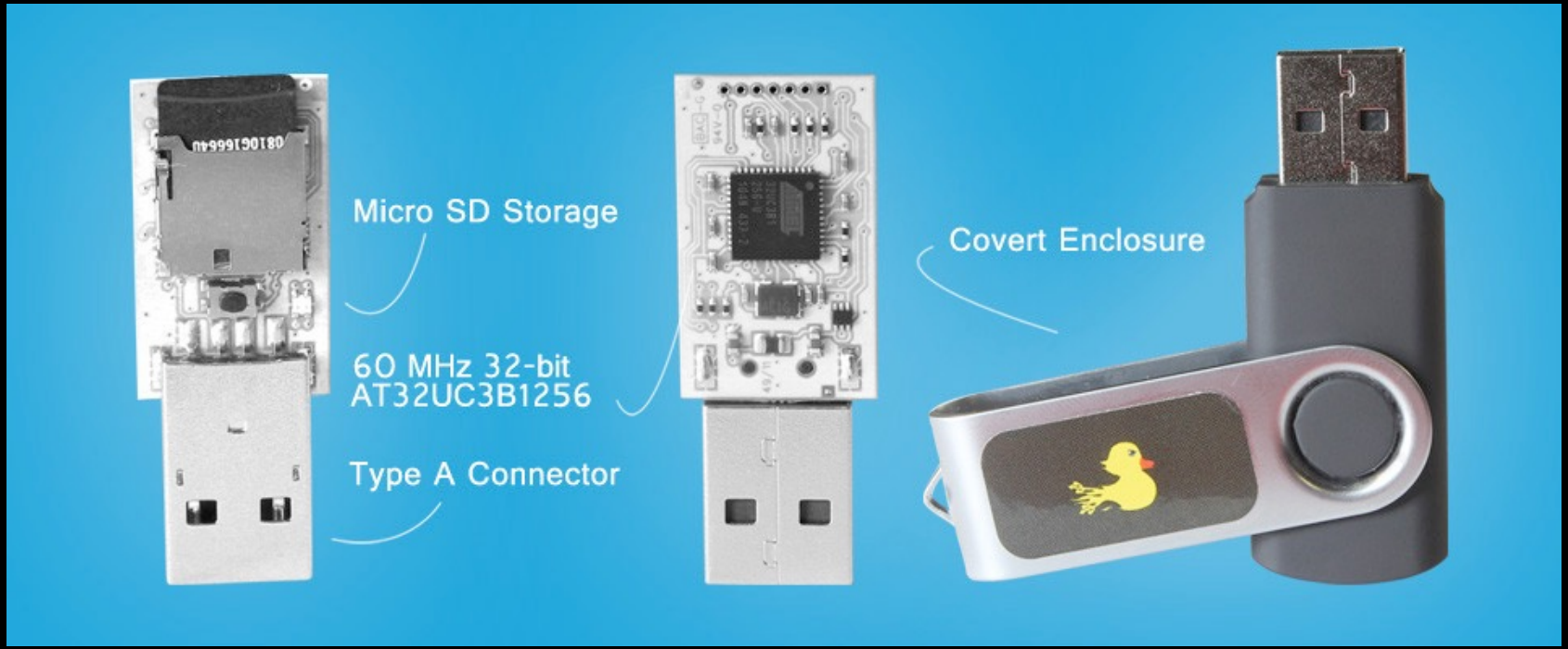
- Southord.com
- Medeco.com
- MIT guide to Lock Picking
- www.clksupplies.com
- Wikipedia: lock picking,
- bumping, etc.

USB attacks

USB Rubber Ducky

- A penetration testing tool It is not an ordinary HID (Human Interface Device)
- A powerful 60 MHz 32-bit processor
- A simple scripting language to craft payloads capable:
  - changing system settings, opening back doors, retrieving data, initiating reverse shells, or basically anything that can be achieved with physical access
- All automated and executed in a few seconds

USB Rubber Ducky



USB RUBBER DUCKY

THE MOST LETHAL DUCK EVER TO GRACE AN UNSUSPECTING USB PORT

Write

payloads with a **simple scripting language** or online payload generator including

- WiFi AP with disabled firewall
- Reverse Shell binary injection
- Powershell wget & execute
- Retrieve SAM and SYSTEM
- Create Wireless Association

Encode

the Ducky Script using the cross-platform open-source duck encoder, or download a pre-encoded binary from the online payload generator.

Carry multiple payloads, each on its own micro SD card.

Load

the micro SD card into the ducky then place inside the generic USB drive enclosure for covert deployment.

Deploy

the ducky on any target Windows, Mac and Linux machine and watch as your payload executes in mere seconds.

Ducky Script Syntax

- Each command resides on a new line and may have options
- Commands are written in ALL CAPS
- Most commands invoke keystrokes, key-combos or strings of text, while some offer delays or pauses.

Ducky Script Syntax

- **REM** will not be processed.
- **DELAY n** wait in the ducky script - in milliseconds * 10
- **STRING** can accept a single or multiple characters.
- **GUI** Emulates the Windows-Key,
- **MENU** Emulates the right mouse button
- **ALT** or **CTRL** accepts Single Char
- Arrow Keys: **DOWNARROW**, **UPARROW**, **LEFTARROW**, **RIGHTARROW**
- More Keys: **PRINTSCREEN**, **ESC**, **TAB**, **SPACE**, **PAGEUP**, etc.

Simple-Ducky Payload Generator

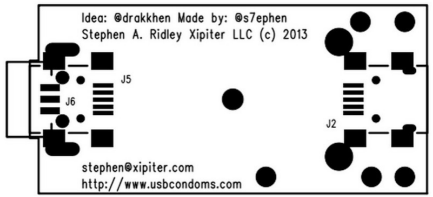
- The simple-ducky is designed to quickly create reliable payloads and launch listener's.
- Create your evil executable (its automatically placed in your web directory)
- Create your inject.bin
- Launch a listener (meterpreter or netcat)
- Generate custom password list's
- Crack extracted passwords
- code.google.com/p/simple-ducky-payload-generator/

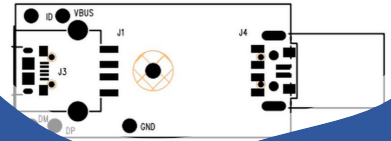
USB kill

- The USBKill classic is a "plug-and-zap" device.
- As soon as it is plugged in, it will continuously deliver pulses to the host device.
- Output voltage:-215 volt
- Advanced versions offer single/continuous pulse and different trigger modes:
  - Remote
  - Smartphone
  - Timed
  - Magnetic

How to protect ?

- USB protection
- syncstop.com



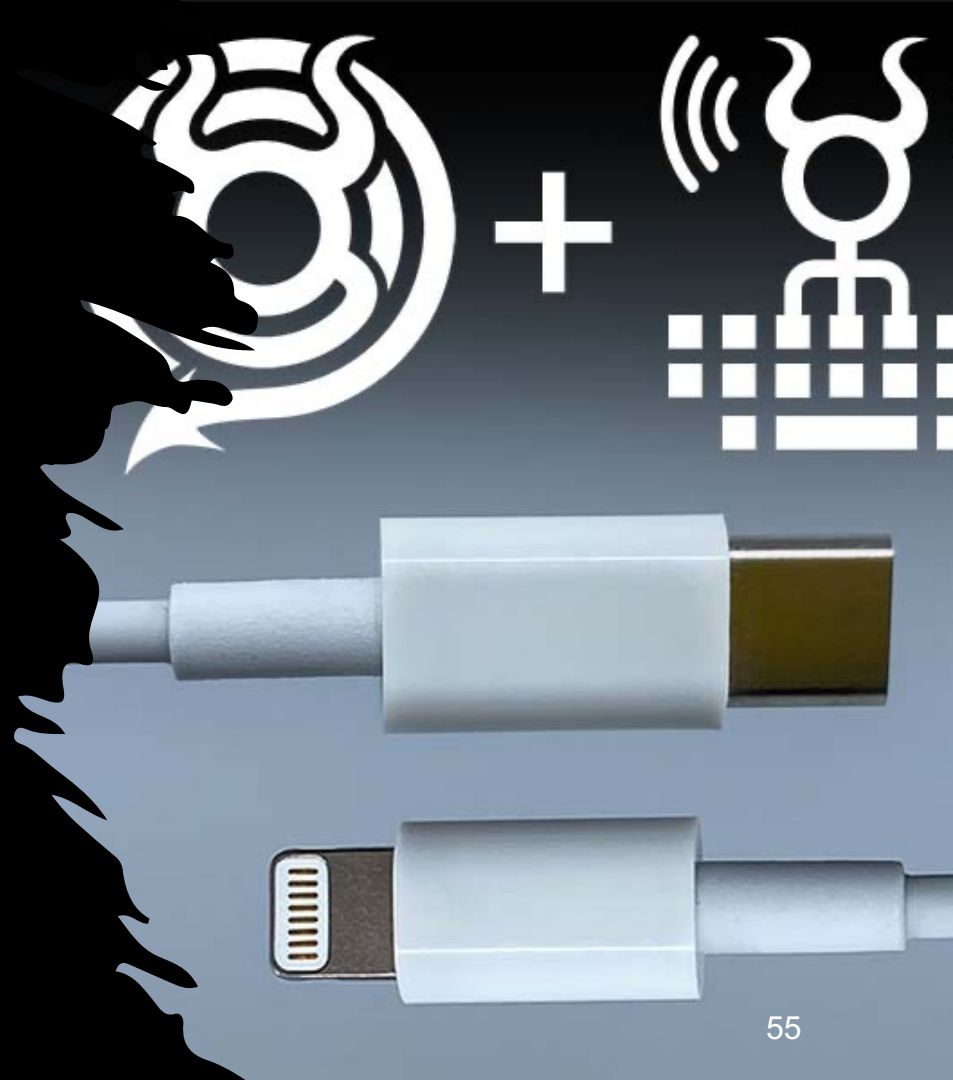


After rubber ducky?

O.MG Cable

A Rubber Ducky inside a cable phone with wifi transmitter

- Interface: USB
- Radio: 802.11b/g/n (2.4GHz)
- Payload Syntax: DuckyScript,
- Capacity: ~650,000 keystrokes



CS1660 Farewell

- And now before the course will be over …
  - Thanks to all!
  - A journey lasted 23 lectures…
  - This is an intro course just the tip of the iceberg
  - Transmit the security mindset and the passion
  - Stay in touch
- And now the course is over ☺