Co-funded by the Erasmus+ Programme of the European Union

ISSES – Information Security Services Education in Serbia

Supported by the Erasmus+ Capacity Building in the field of Higher Education (CBHE) grant N° 586474-EPP-1-2017-1-RS-EPPKA2-CBHE-JP

PHYSICAL SECURITY

Computer Security

Lecture 2

Information Security Services Education in Serbia (ISSES)

2.1 Physical Security: The problem

Note on copyright

- Lockpicking-related images in this presentation are courtesy of Deviant Ollam of The Open Organization of Lockpickers and are used with permission.
- http://www.toool.us for more.

Physical security: purpose

- Focusing on computers, the purpose of physical security is to safeguard the hardware running the system we want to protect.
- Why would we want to safeguard the hardware:
  - We don't want it stolen, for one thing.
  - A direct attack on the hardware can impact system reliability: few server architectures survive explosions.
  - Physical access to the hardware seriously impacts confidentiality and integrity.

The peril of physical access

- At a fundamental level what we call computer security rests on the operating system (a lot more on this as this course progresses).
- The way the operating system makes a system secure is by rigorous protection of the hardware.
- Nobody gets to talk to the hardware directly, the interaction is always mediated by the operating system.
- This can't really be enforced if the adversary isn't running code on the system or sending network packets to the system, but is instead standing in front of the system with a screwdriver and an ominous expression.

Problem #1: Hard-drives

- The chief prize of a computer system is data.
- The data is generally on hard drives.
- The simplest way to steal the data is to physically remove the drive from the system and carry it away.
- True, if the data is encrypted this provides some level of security, but even so, there are significant risks as fragments of decrypted data may be present, and shadows of data long-deleted may persist on the drive.
- Further, unless whole-disk encryption is used, it is always possible to *alter* the data on a disk, and put it back, thus introducing security flaws into the system.

Problem #2: Local administration

- A lot of network security equipment has to be configured extensively.
- Lacking a dedicated interface, they are configured by connecting to them via specially designated ports: serial or network.
- This is perfectly secure against network attacks, but if your adversary has a laptop, a cable, and is standing in your server room, there's absolutely no protection left.

Problem #3: Targeted reconfiguration

- If the adversary is in the server room they can always change the hardware to make things easier for them or for others they are in collusion with.
- In the most sophisticated form, they can add surveillance and eavesdropping devices of disguised appearance in a corner somewhere and use them to mount complex attacks.
- In the least sophisticated form they can just unplug your expensive, highly-sophisticated hardware firewall making its purchase pointless.

Problem #4: Low-grade attack

- Even if the attacker is locked out of the server room itself, mere access to the facilities can have terrible consequences.
- Gaining access to workstation machines can allow attacks to be made from within the secure network and not from without.
- Gaining access, aside from all of the hardware-dependent attacks we just mentioned, can also be made considerably easier by trusting users to be… well, users.
- There's not a lot of offices where at least one computer isn't accessible via password written on a post-it note somewhere in the workspace.

Problem #5: Hardware attack

- A particularly sophisticated attack vector is to exploit vulnerabilities in the hardware itself to gain complete control with persistent remote access.
- An example is the recent vulnerability in the Intel Converged Security and Management Engine (CSME) which allows an attacker with physical access to the machine to, potentially, gain arbitrary code execution at the 0^{th} level of privilege which allows secure key storage and firmware integrity protection to be bypassed.
- See CVE-2019-0090 and related for more details.
- Simply put: *you do not want an advance persistent threat to have the slightest chance of having undisturbed access to your hardware at any point in its lifecycle.*

Information Security Services Education in Serbia (ISSES)

2.2 Physical Security Devices

Methods of physical security

The methods of physical security can be divided into those of:

- Monitoring
  - CCTV
  - Motion-detectors
- Control
  - Mechanical locks
  - Electronic locks
    - Keyed
    - Passcoded

CCTV

- A crucial component of any serious physical security system is an effective means of surveillance.
- CCTV is a *deterrent* and potentially an early-prevention tool.
- The biggest problem with CCTV is that it requires real-time human monitoring to be truly useful at preventing an attack.
- CCTV frequently works over existing network protocols and is, thus, susceptible to network attacks.
- Its deterrent function is defeated by a simple piece of cloth.

Motion detectors

- The most common type are passive infra-red detectors which detect a heat gradient by sensing mid- and near-infra-red light a human-body-warm object emits.
- Other types actively send some sort of signal and detect motion via heterodyning between the return and original signal.
- They can be exceptionally useful at raising the alarm if human motion is detected in sensitive areas.
- There is no ready way of bypassing motion detection by disguising temperature gradients.

Motion detectors

- The chief issue with motion detectors is that they are not discriminating: if something warm moves they will raise the alarm which makes it possible to have false alarms.
- False alarms are trivially easy to cause by an adversary by using nothing more elaborate than compressed air for basic motion sensors, and a balloon for more advanced ones.
- Even worse, this nature of motion detectors means that they can't be used anywhere where it is normal or expected for people to be since a motion detector can't differentiate between the night janitor and an intruder.
- Motion detectors are also electrical devices which makes them vulnerable to power-disruption attacks.

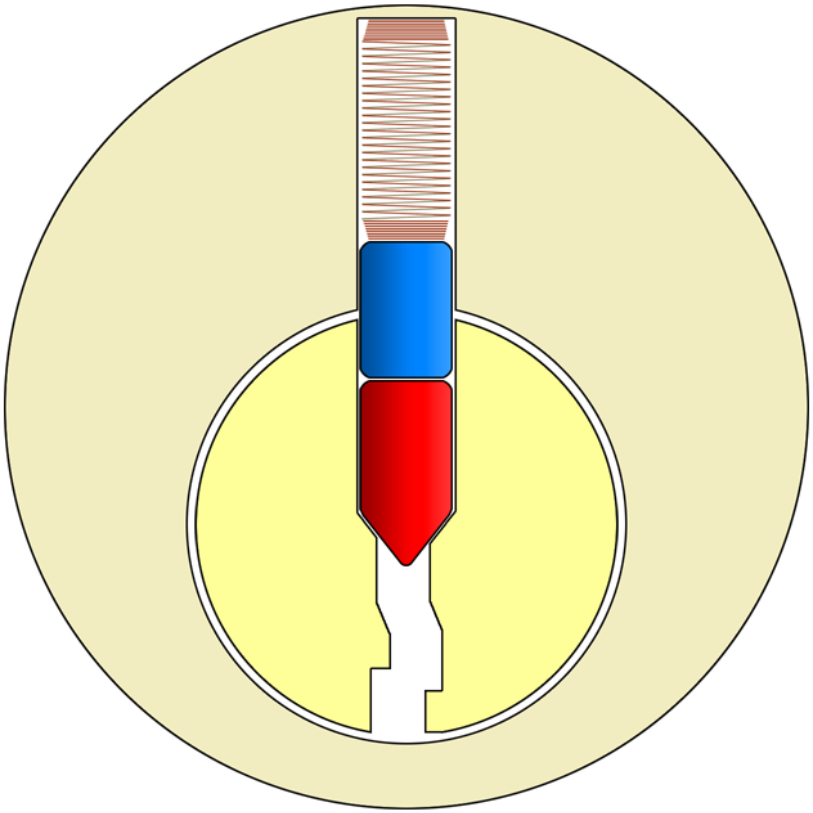
Mechanical locks

- Mechanical locks don't need introduction: they are the basic mechanism of control over whether someone can open a door or container currently used.
- On a surface level, what protects a lock is the possession of a physical object, but in truth, a key is merely an elaborately coded *passcode.*
- Each key is fully specified by its type and something called *bitting values* which are a numerical representation of the cuts made to a key blank by a locksmith to create the key.
- Mechanical locks come in various forms, the most common of which are pin tumbler locks and wafer locks.

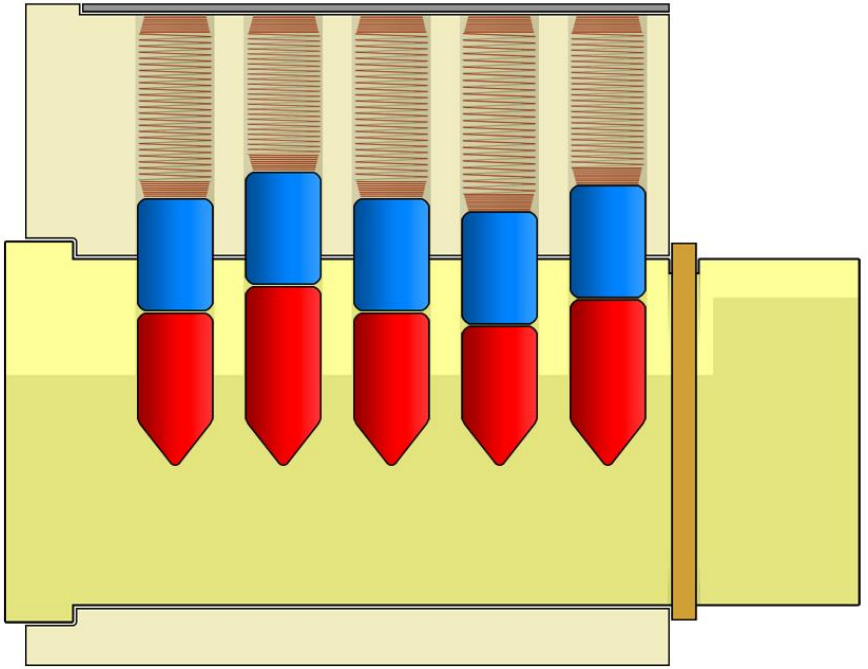
Pin tumbler locks

Diagram of a pin tumbler lock

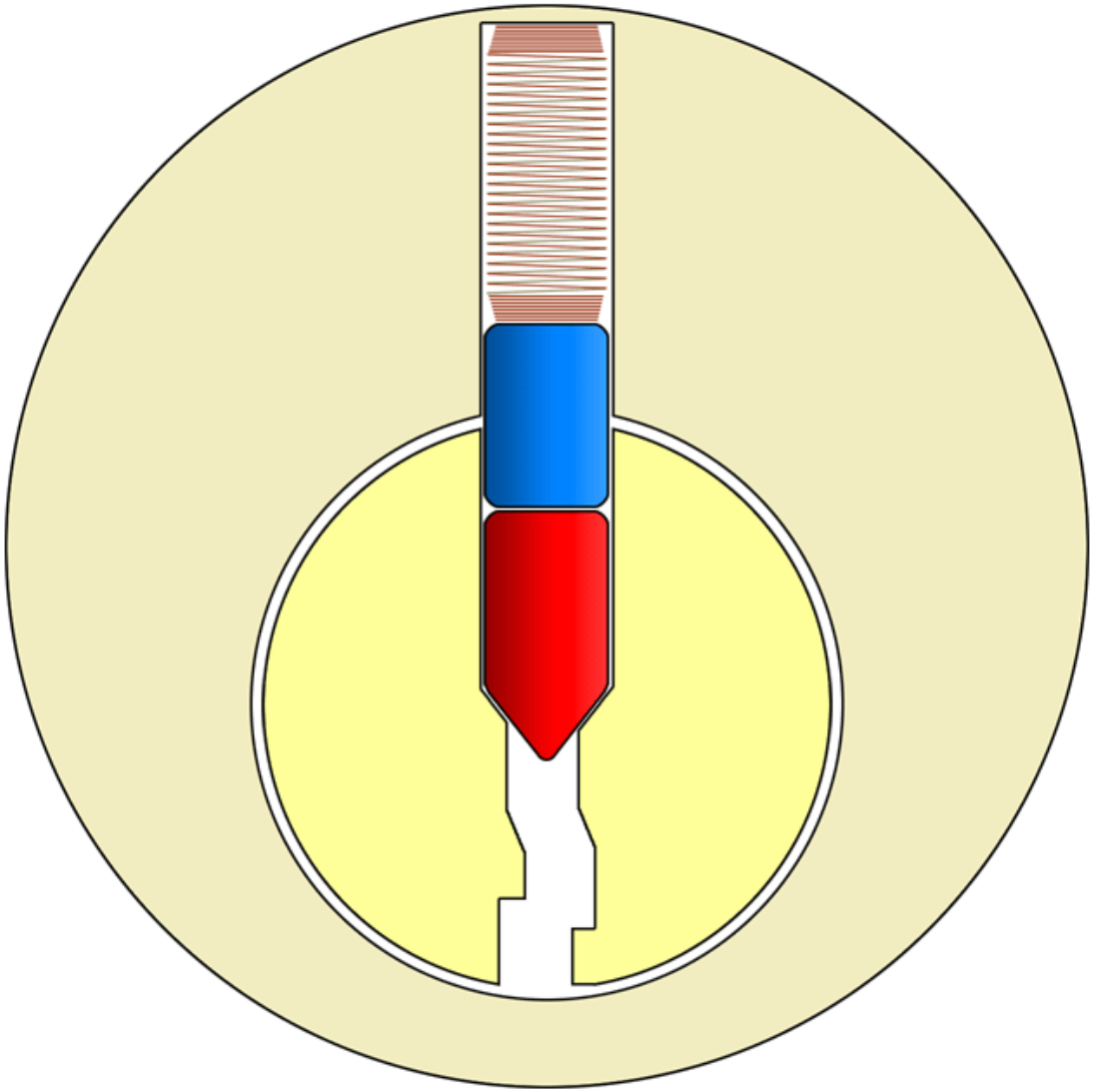
Front



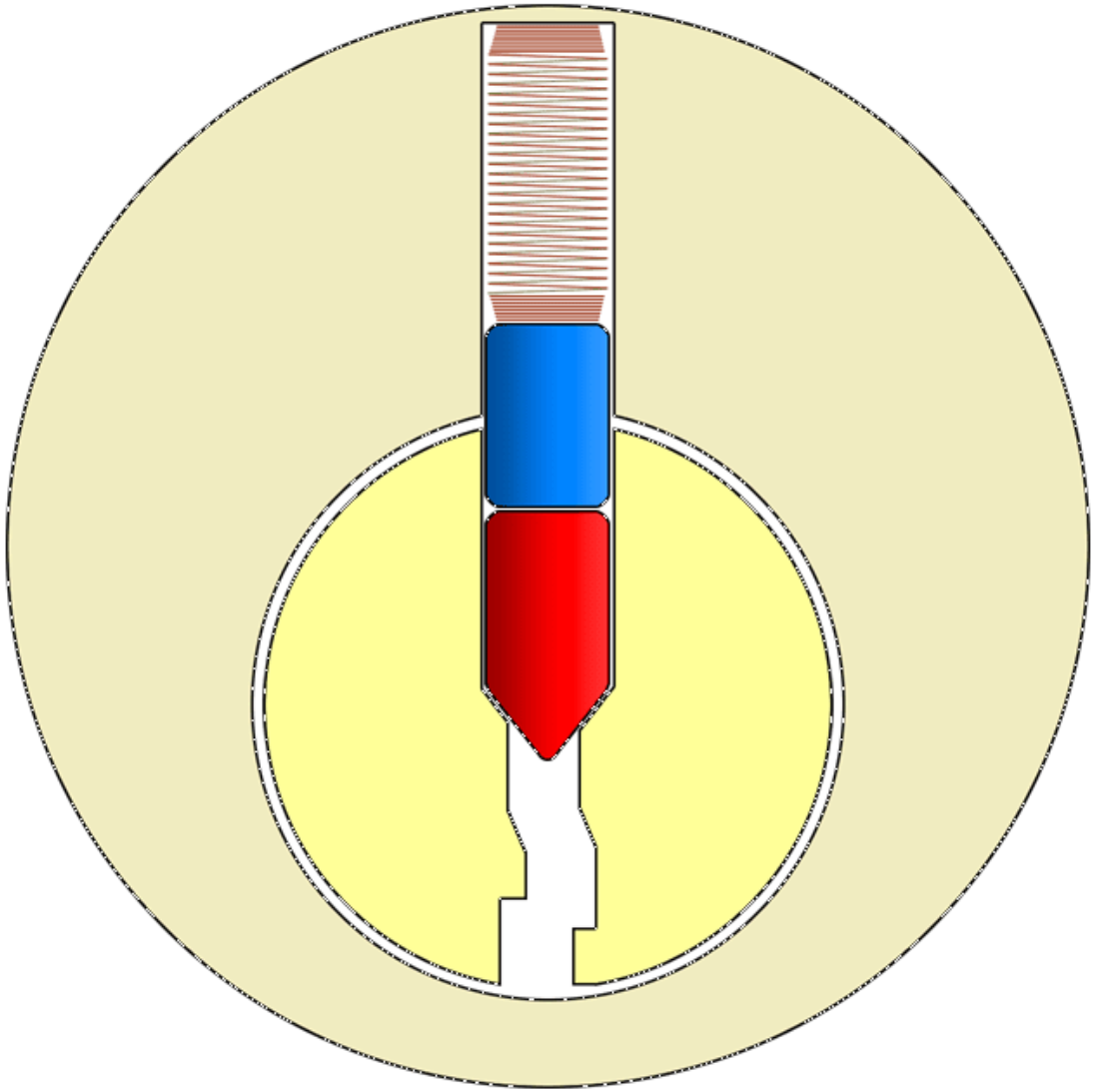
Side



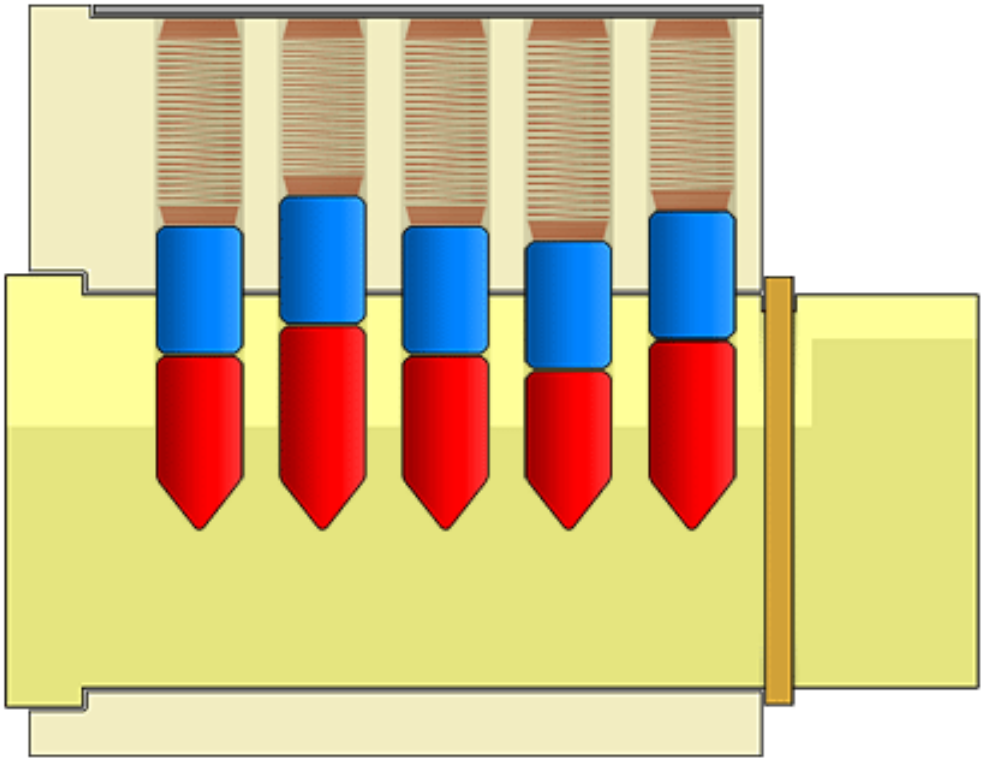
No key



With key

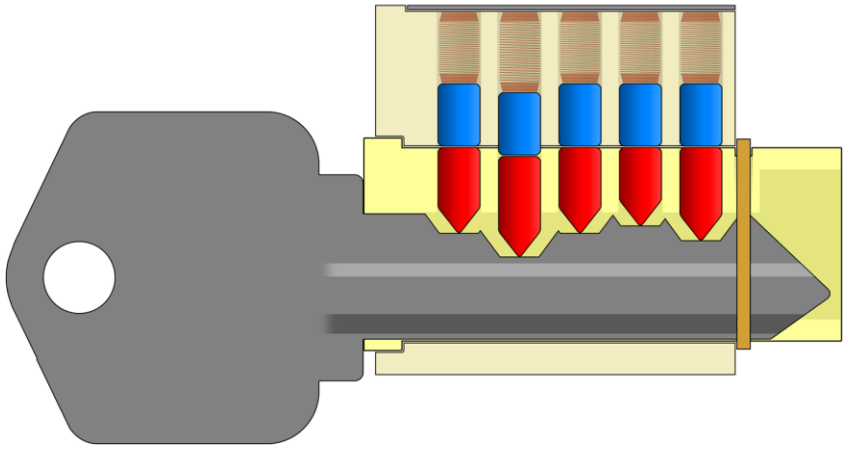


With key

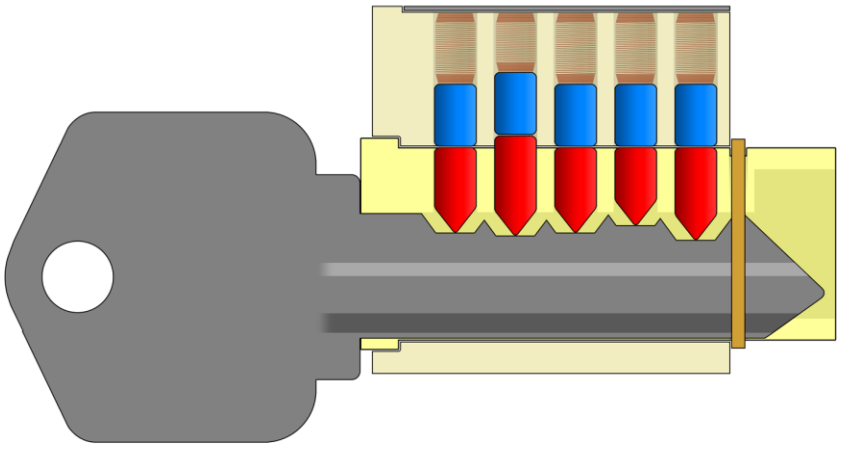


Wrong key operation

Low bitting



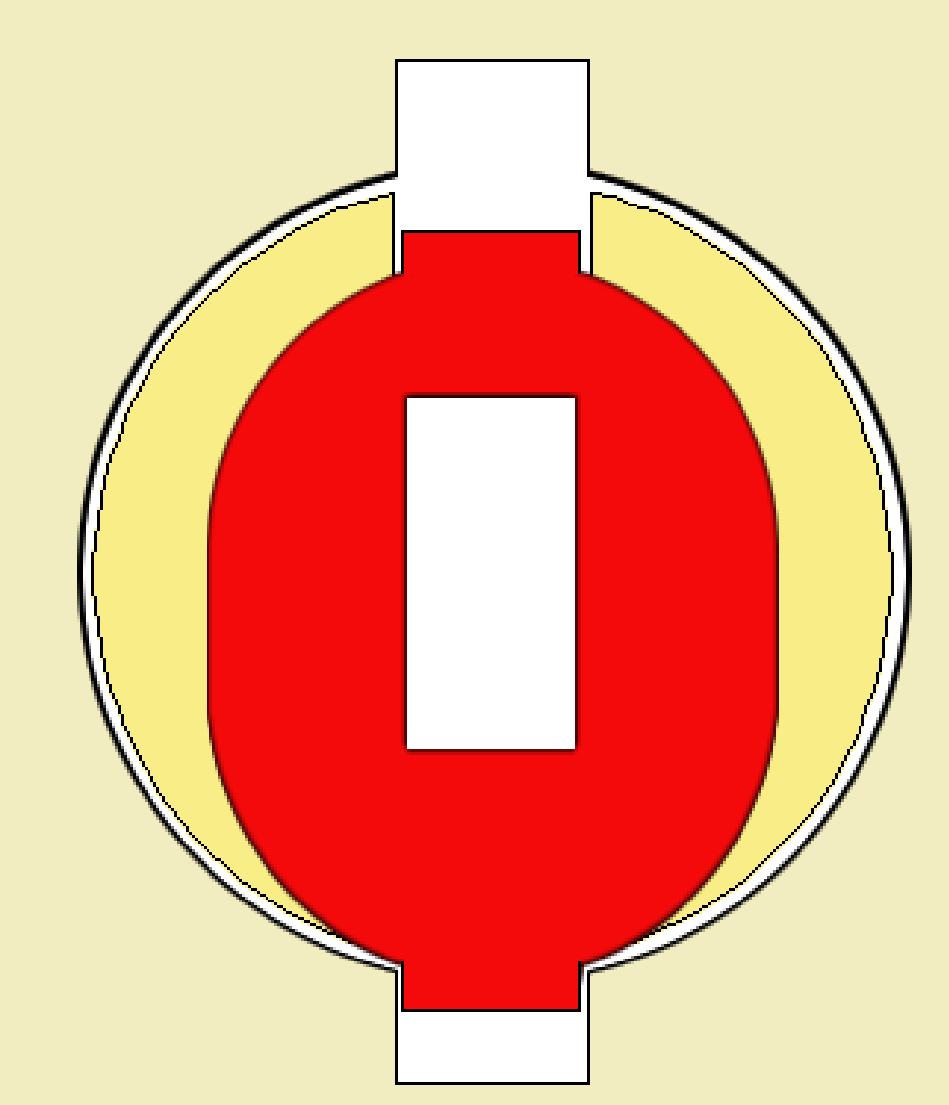
High bitting



Wafer locks

Note vulnerability: These numbers are almost certainly bitting codes for the lock, meaning that a skilled adversary could replicate the key in minutes, sometimes even with hand-tools.

How a wafer lock turns



Electronic locks

- Electronic locks are gaining traction more and more, often because of a greater perceived security.
- The locks are nearly all simple solenoid-actuated devices, what differentiates them is how they are opened.
- An electronic locked may be keyed using:
  1. An inserted electronic or magnetic card
  2. A 'contactless' card or passive fob
  3. A wireless active fob
  4. A passcode
- Options #2 and #4 are the most common
- They are also the least secure.

Power-off issues

- Electronic locks require power to be effective.
- This raises the question of what happens when the power is cut off.
- Some locks default to open: this means that 'picking' them requires only shutting off power.
- Some locks default to 'closed.'
- This is better, but this does mean that a power outage can leave someone stranded, possibly during dangerous circumstances, e.g. a fire.
- Therefore these always have backups: usually these are mechanical locks which have all the vulnerabilities of such, plus are likely to have keys be kept on-premises.

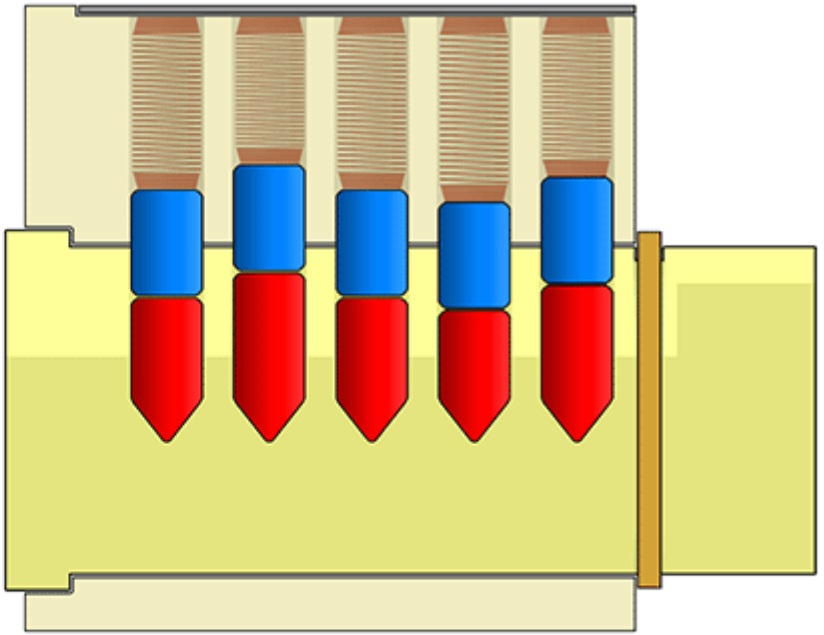
Information Security Services Education in Serbia (ISSES)

2.3 Physical Security Vulnerabilities

Vulnerabilities of mechanical locks

- Mechanical locks are surprisingly easy to pick, i.e. open without the use of the real key.
- Common picking attacks are:
  - Single-pin picking.
  - Raking
  - Machine-picking
  - Bump-keying
- Another attack vector is key duplication based on:
  - Information leakage
  - Faults in key-mastering techniques.

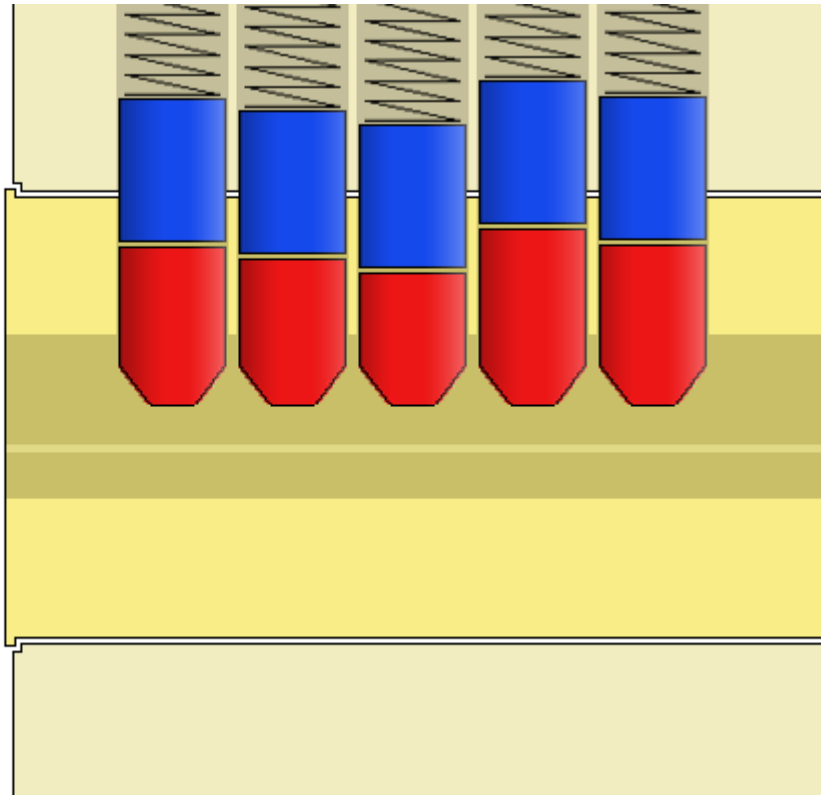
Single-pin picking



Why is this possible?

- Imperfections in key manufacture.
- The tolerances of locks, especially inexpensive locks can be shockingly loose.
- These imperfections are what causes pins to stick and allows someone to work through a lock pin-by-pin.

Raking



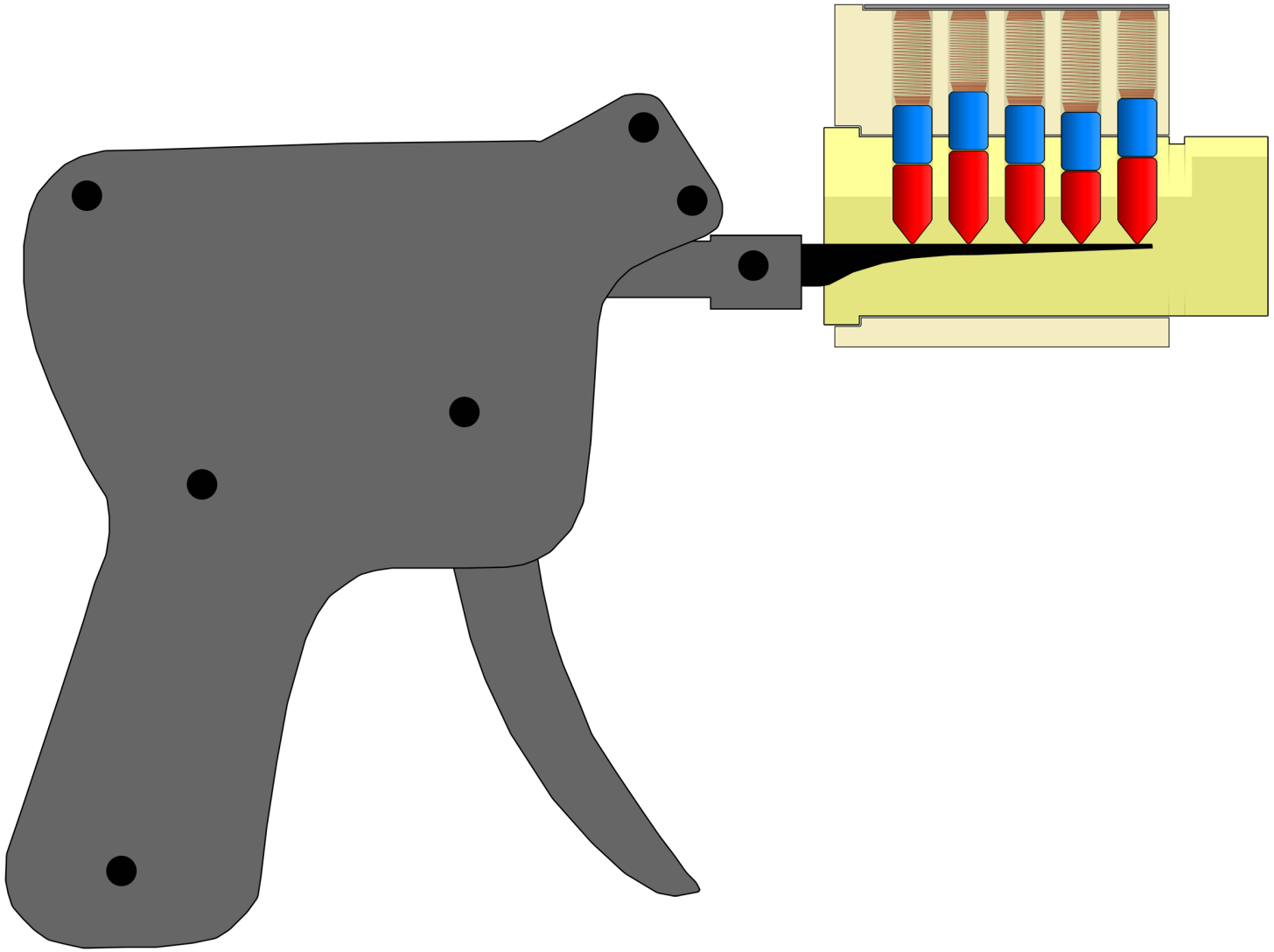
Raking

- Raking is *much faster* than single-pin picking
- This means that someone can open a lock nearly as quickly as with a key, so fast that it can look inconspicuous over, say, CCTV.
- And all that's needed for the task is two tools: a wiper-insert tension tool and a wave-rake, both thin pieces of metal which can be hidden nearly anywhere.

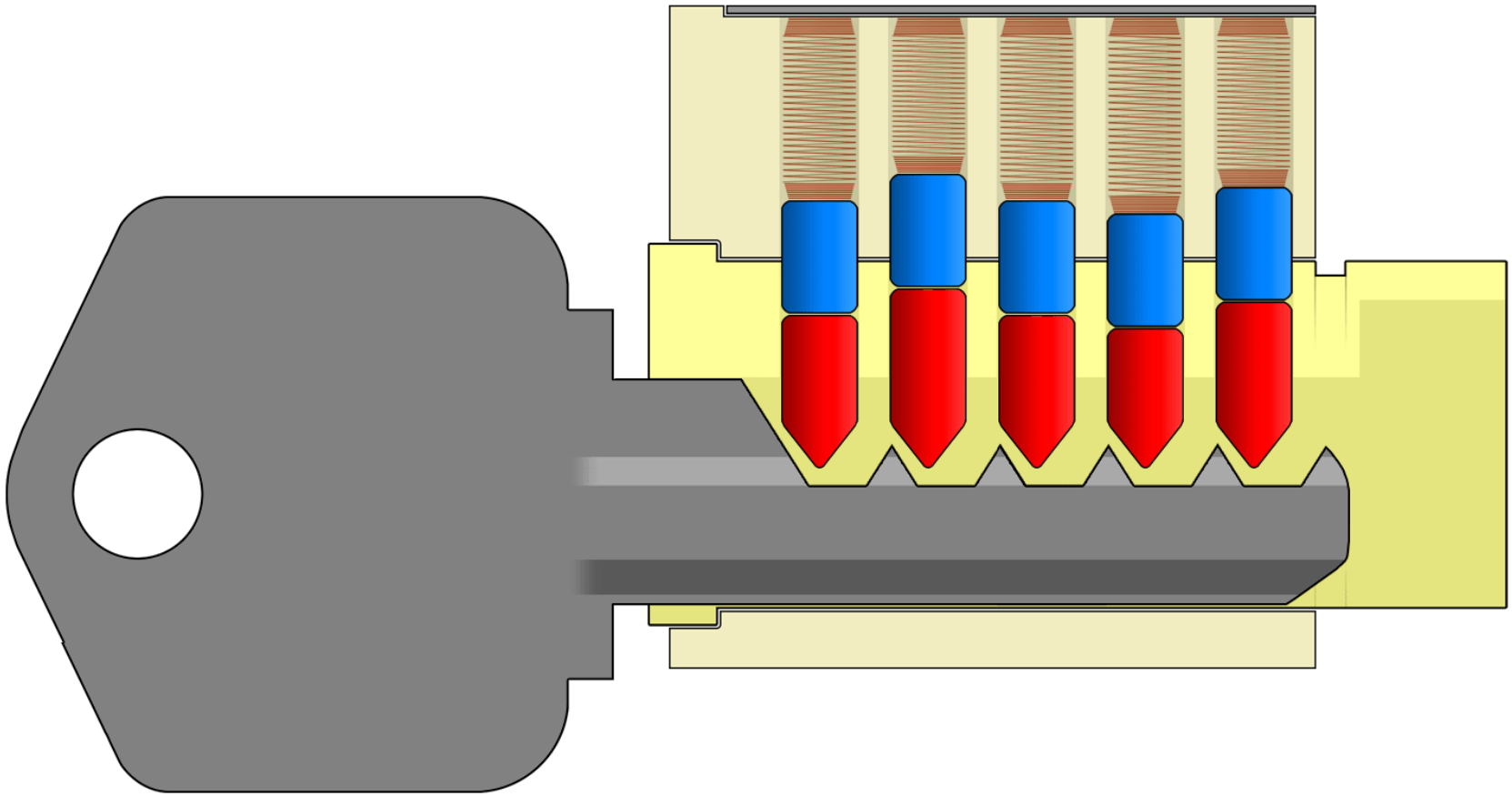
Bumping and pick guns

- Both techniques are based on a simple physical fact: the shear-line of the lock needs only to be cleared for a split-second for it to start turning.
- Once the lock has started turning, the motion itself stops the pins from resetting.
- Therefore, merely aggressively hitting the key pins repeatedly ("bumping" if done with a key or "snapping" if done with a pick-gun) causes many chances for this to happen.
- Keeping a lock tensioned enough means that it only needs to happen once for the lock to unlock.
- It's a *staggeringly* effective attack and not a very difficult one to pull off.

Snap gun picking



Bump key picking

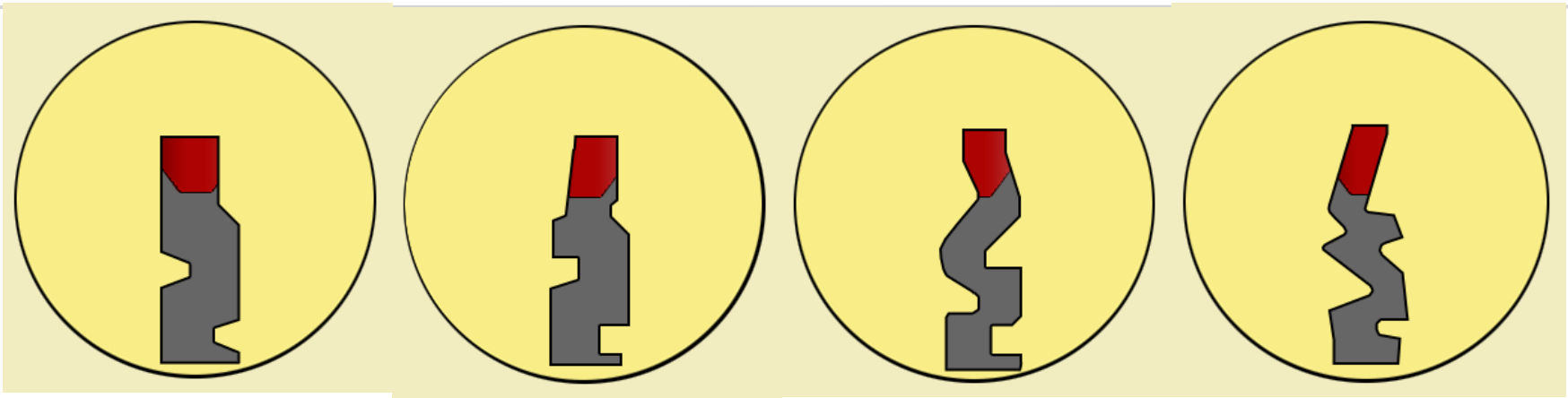


Bump keying is versatile

Pick-resistant locks

- It is possible to build locks with features which help them resist picks.
- These features include:
  - Tight tolerances and high-quality manufacture
  - Complex keyways
  - 'Tricky' pins.
  - Top-gapping and anti-bumping pins

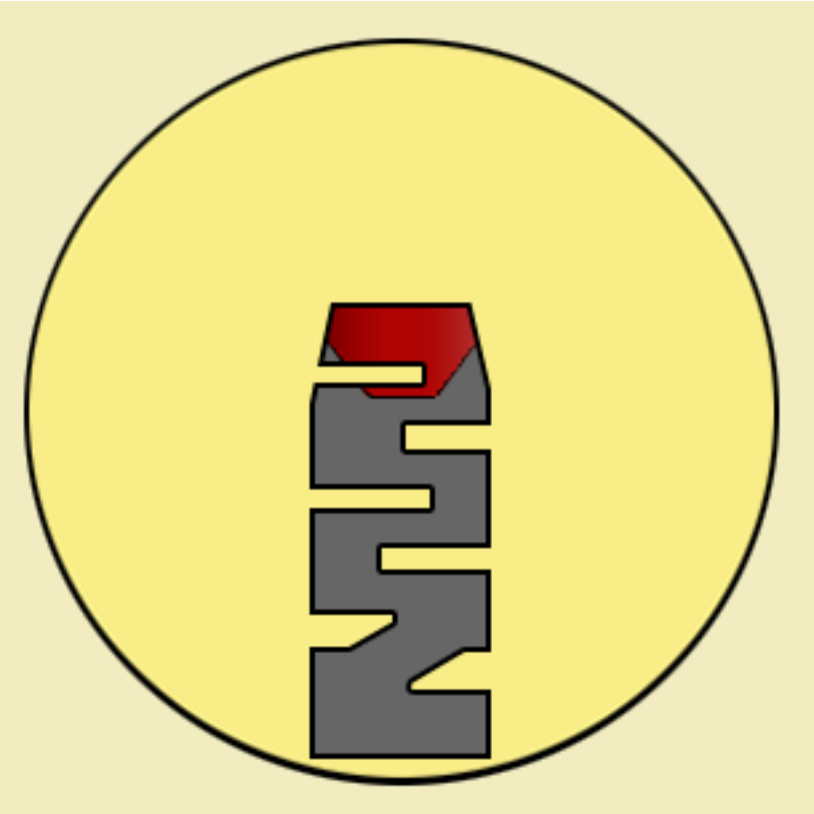
Complex keyways



Simpler

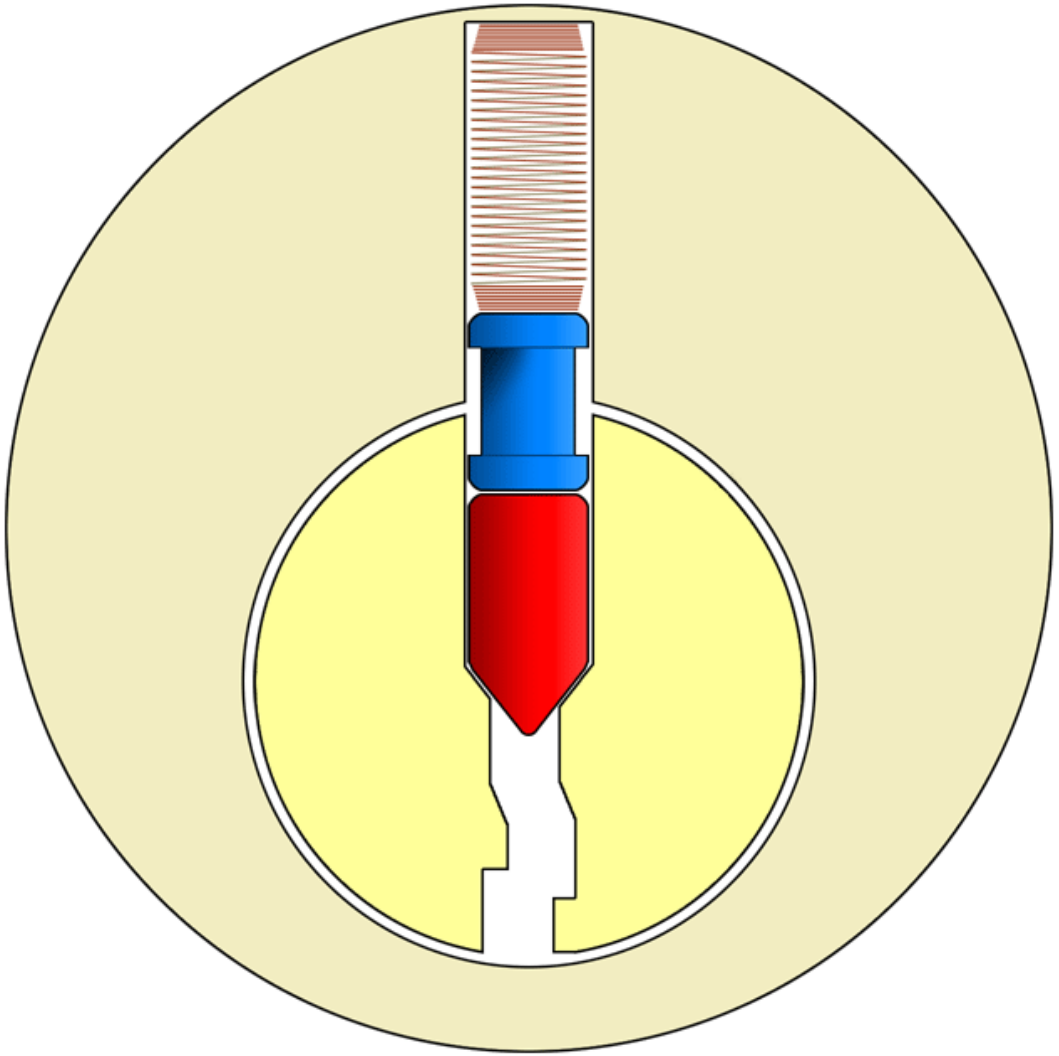
Complex

Complex keyways

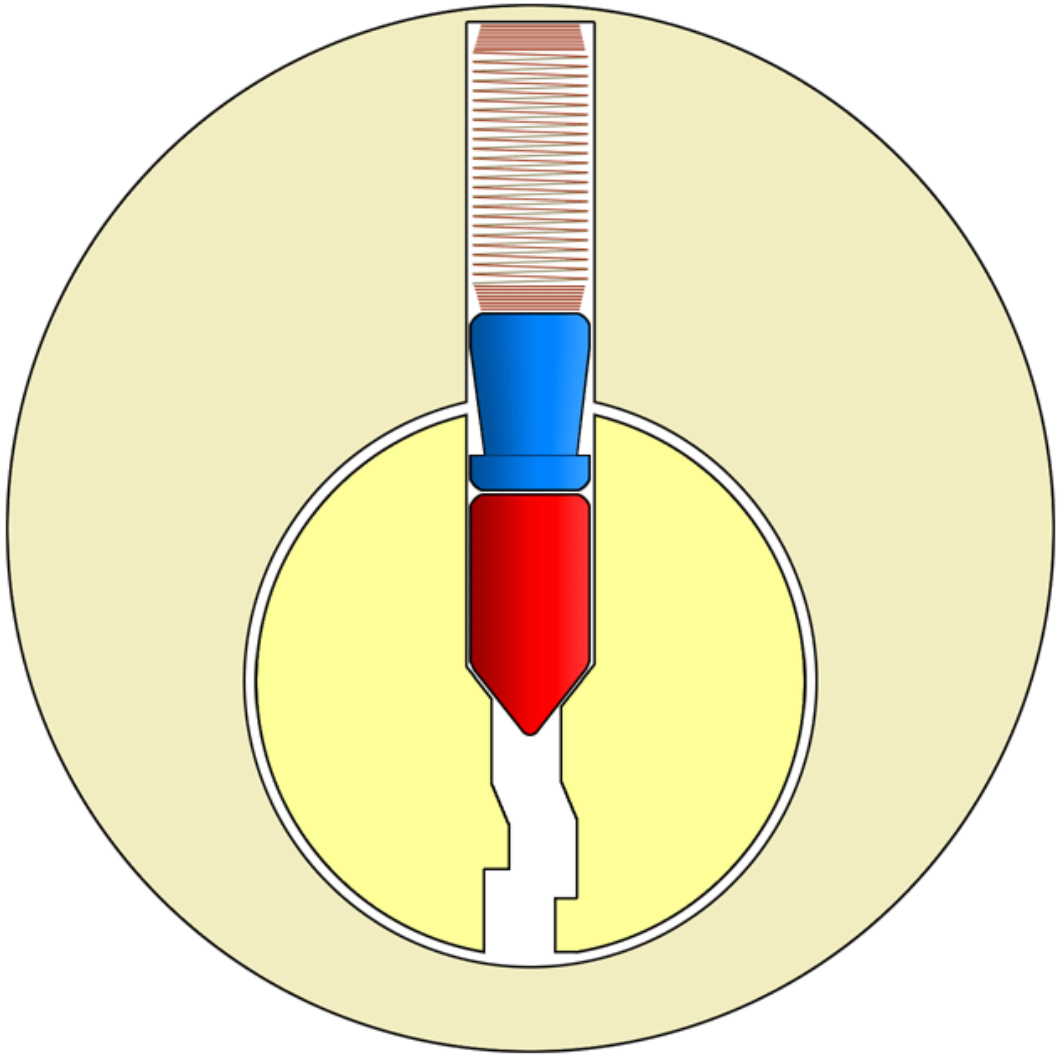


Unreasonable

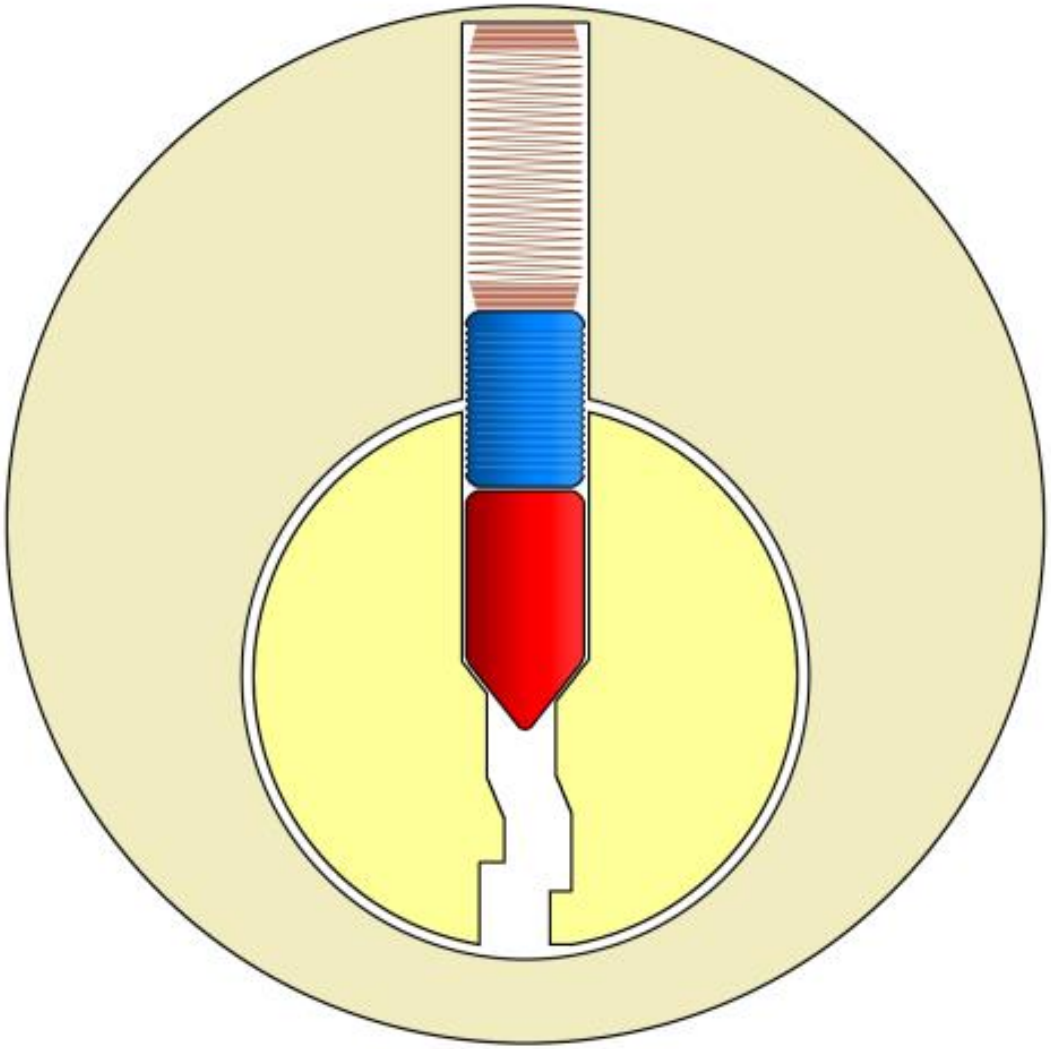
Tricky pins: Spools



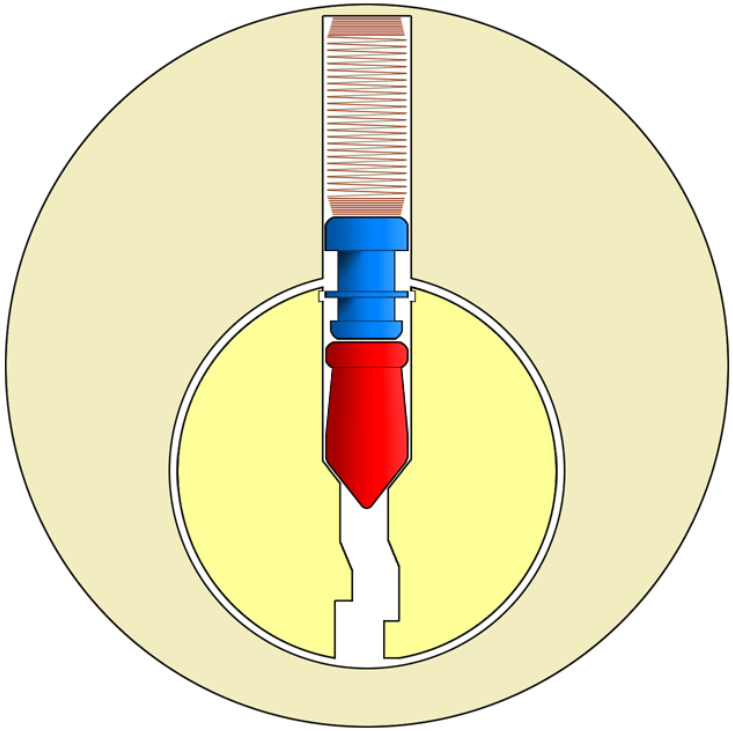
Tricky pins: Mushrooms

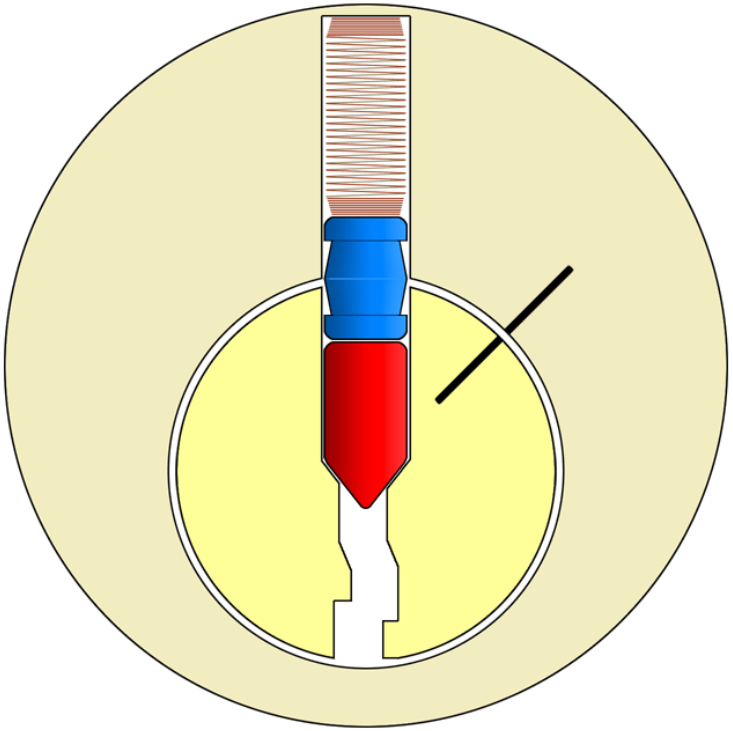


Tricky pins: Serrated



Tricky pins: Variations





Bumping/snapping protection

- Two methods work:
  - Anti-bump drivers
  - Top-gapping
- Anti bump drivers simply add a much stronger spring with an internal strengthening element to one pin.
- Top-gapping on the other hand, lift one driver pin (blue in our diagrams) upwards so that only a tiny amount protrudes beneath the shear line, and there's a substantial gap between it and its corresponding key pin (red in our diagrams).
- This renders it very difficult to get the knock-on hit-propagation effect that bumping or snapping require.

Information-leakage

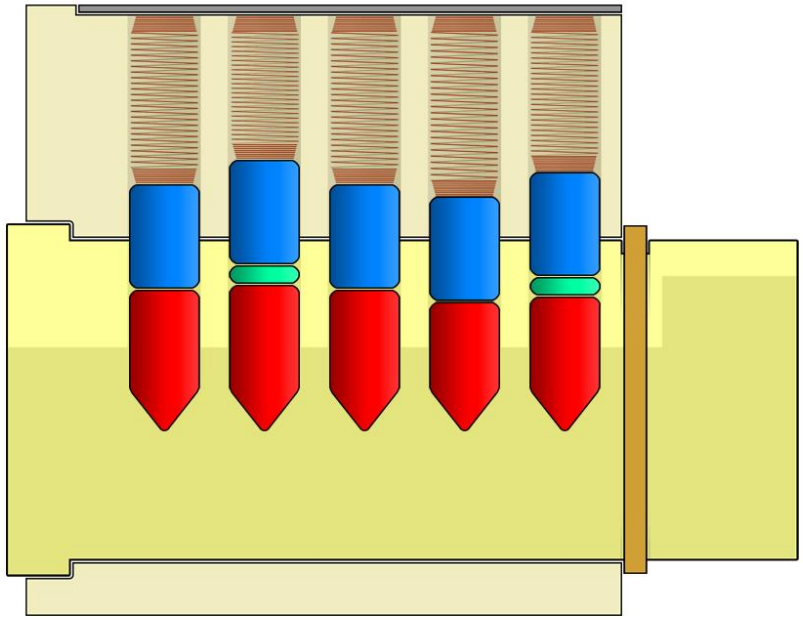
- If an adversary knows the bitting of our key, the adversary can copy it.
- How can bitting information leak?
  - Contractors
  - It's not difficult to extract bitting information from a photograph: a single side-view and edge-on photo is enough to reconstruct the key.
  - Impressioning of the key if the adversary has even momentary access to it.

Mastering key systems

- Large installations typically use key mastering techniques that allow certain keys to open all or a subset of doors.
- Such systems typically have a single 'master' key which opens everything and may have sub-levels of hierarchy beneath.
- Such keys are useful for custodial staff.
- However, such key systems are also a terrible risk since they allow for someone with access to *one* key or even just one lock (penetration testing teams sometimes cheat by simply stealing the lock out of a staff bathroom which nobody uses, disassembling it at leisure and using the information to extract vital secrets about how the system works) to reconstruct the master key.

How do such systems work?

- The only way you can have multiple keys opening the same door is by having multiple shear-lines.
- This is done by having key pins composed of multiple metal cylinders so that additional shear lines are created at the dividing line between cylinders.



Mastering key vulnerability

- In a seminal 2003 paper, security research Matt Blaze showed how by having access to *one* lock in a mastered system permits an attacker to escalate privileges and gain master locks in such a way that:
  - The attack can be entirely covert
  - It consumes negligible physical resources.
  - It requires no special skill or equipment: just about ten key blanks (available online), a metal file, and a Vernier caliper.
- This makes mastering systems unsuitable for high-security applications.

Electronic lock vulnerabilities

- Electronic lock vulnerabilities come in different forms:
  - Locus of control vulnerability
  - Remote-reading vulnerability
  - Human element vulnerability

Locus of control

- Every electronic lock has a reader, an actuator, and a locus of control.
- The reader accepts a request to enter and reads the user's credentials: it's the equivalent of the keyway.
- The actuator actually opens the door.
- The locus of control is the electronic system which verifies the credentials.
- Very frequently, for manufacturing reasons, the locus of control is in the reader.
- This means it is *outside secured space.*
- It also means that a surprisingly large number of locks can be picked open using a screwdriver and a 9V battery.

Remote-reading

- Electronic locks are frequently operated using RFID cards.
- These are passive devices which are read by active scanners *usually* from a short range.
- Usually?
- It turns out that RFID reading range is largely power-dependent, so if you use more powerful device you can read from a pretty extreme range.
- 10 meters is can be achieved with commercially available devices very easily.
- This means that all that's required to copy RFID credentials from someone is to be within 10m with a laptop bag.
- This can be defeated by carrying your RFID cards in a Faraday cage.

The human element

- If your system involves passcodes, they are vulnerable in the way all passwords are vulnerable.
- If they can pick them, users will pick ones that are easy to guess.
- If they can't pick them, users will write them down somewhere, usually somewhere an adversary can read them.
- More on this in section 2.4

Doors as points of attack

- Frequently, the adversary does not need to attack the lock at all.
- A door is a clear point of attack, and if the door isn't built right, then there's no point in fitting a fantastic lock into it.
- How can doors be vulnerable?
  - Build quality
  - Hinges
  - Fitment
  - Safe-side exploits
- Build quality is self-explanatory: if the adversary can simply break the door instead of picking the lock, they will.

Hinges

- It seems trivial but doors are frequently placed incorrectly with their hinges accessible from a side that's not necessarily secure.
- If the adversary has access to the hinges of your door, they can simply knock out their pins (a hammer and screwdriver suffice) and *remove the door.*
- This is a very low skill attack and highly efficient.

Fitment

- Fitment is how the door interacts with the door-frame, especially how the strike-plate is fitted, the element of the door-frame which is the 'dock' for the lock and for the latch.
- If the fitment of the latch is good, the door can't be forced open easily.
- If the holes are too large, however (and they frequently are because it's easiest to get the largest model available since it fits any door configuration) it is possible to use a thin flexible shim to open a door whose handle is otherwise disconnected from the latch mechanism.

Safe-side exploits

- Very frequently a door has a safe side and an unsafe side.
- This means that from one side you need a key and from another you need to just manipulate a handle.
- The fire code is often the cause of this, mandating crash-bars on one side of doors on the fire escape path.
- The problem is that if you can manipulate objects on the safe side of the door you can easily bypass the lock altogether.

Types of safe-side exploits

- Bypassing outside-facing double doors by fitting a shim in-between and hitting the crash-bar.
- Moving a wire under the door and hitting crash bars or handles.
- Spoofing safe-side Request to Exit (REX) electronic sensors by squirts of cold air or balloons forced under the door and then inflated and let go (this reads as motion to even the pickiest of sensors).

Physical security done right

- Correctly doing physical security is something that depends on requirements of the system at hand, on the budget, expected attacks, and many other factors.
- However, there are some general guidelines that generally help.
- These are not a recipe to success but guideposts to consider when planning security.

Guidelines

1. Physical security **is** a computer security issue. If there's no dedicated physical security person, then securing the software system also involves securing the space it must operate in.
2. Do not neglect basic things in favor of impressive technical solutions: there's no replacement for a good door.
3. Make sure doors are fitted in such a way that absolutely nothing can be slipped, pushed, or shimmied from the unsafe to the safe side.
4. Make sure all your door hinges face the right side.
5. Don't save on locks and look them up online as if it were a piece of software you were evaluating for possible security holes.

Guidelines

6. Do not use master-key systems, and if you must, don't use them for anything that's meant to be secure.
7. Anywhere that's not frequented (like the server room) should be alarmed with a motion-sensor and covered by CCTV. The only thing worse than an intrusion is an intrusion that went by undetected.
8. Assume that anything protected with an RFID reader is not, in fact, secure.
9. Make sure the building security holds in case of power being cut.
10. Copies of the keys of all the rooms in your facility should not be available in one place, and if they are, they must be protected by a top-quality lock at minimum.
11. There is no replacement for a good security culture

Information Security Services Education in Serbia (ISSES)

2.5 Operational security & the human element

The weakest link…

- The weakest link in any security system are the humans using it.
- Why?
  - Convenience is the opposite of security.
  - Good manners are the opposite of security.
  - Hierarchy is the opposite of security.

Convenience

- Security, by nature, is inconvenient.
- It requires that normal, everyday things, be done with a multitude of extra steps.
- It requires the following of tedious rules and procedures, wasting time better spent on other things.
- Simply put, security is *overhead.*
- Therefore, the impulse of any user is to circumvent security wherever possible.

Manifestations of convenience

- Doors kept open to make it easier to, e.g. get out for a smoke break.
- One handy place to store keys so that you don't have to go hunting for them.
- Setting passcodes to easy-to-remember dates and passwords to family member names.
- Writing down any other passcodes and passwords and leaving them lying around on post-its and scraps of paper.
- Keeping a master list of all the passwords in an excel file on the office manager's computer.

Good manners

- Consider this scenario: An elderly gentleman, clearly frail with age, is struggling with a big, heavy box festooned with 'fragile' and 'this way up' decals stands in front of the front door of the office. As you pass he asks you to, please, open the door for him. He has to get the package in right now or it's his job and he's got his hands full. Do you help him?
- Of *course* you do! To not do that would be to have a heart of stone.
- And yet this humane, human act is *precisely* the opposite of security.
- The security policy is clear: no card, no entrance, and yet here you are helping someone subvert it.
- This makes it a *great* way to gain entry, especially since there's very little cost to trying again and again.

Good manners

- Security practice demands that people act precisely in the way *opposite* to their natural instincts to avoid conflict at the workplace.
- Consider a bunch of guys walking down a corridor of an office building dressed in matching overalls bearing the logo of a maintenance company, talking to each other and joking around. They are carrying well-used tools but you don't see a security badge anywhere. Do you stop them?
- Who would? Who would want to be that guy? And even if you know that 'maintenance worker' is a favorite disguise for intrudes ninety-nine times out of a hundred you would just be a pompous, officious jerk.

Good manners

- The impulse to be helpful is astonishingly strong in the sort of well-socialized, nice people a company would want to hire in the first place.
- There have been cases of physical penetration testers just *asking security guards for help* and receiving it because, well, they seem nice and harmless and have asked really nicely.
- And, generally speaking, isn't this *precisely* what a company culture should be? Helpful? Welcoming? I mean, there's this new guy, just joined the company, and damn it, he lost his ID badge and he's terrified of being late, and could you help him not make a terrible impression his first day of work?

Hierarchy

- Sometimes it isn't about good manners so much as obedience to the signs of authority that's needed to make working in a complex organization possible without constant argument.
- If someone's in a conference room doing something inscrutable with laptops and they have an official-looking piece of paper (fakeable with a color laser printer, naturally) and are name-dropping your boss and explaining how he told them to be here do you leave them alone to do whatever it is they are doing? Or do you call your boss even though it's late? Do you do it *every time?*

Social engineering

- It's these factors that permit social engineering to work.
- Some adversary calls up your offices pretending and sounding as if they are someone of authority or technical savvy (hierarchy), they are warm and personable and friendly (good manners) and they ask for just this one password to save them a whole *mess* of trouble of going through the right channels because, well, we all know how tedious all those *procedures* are, right? (convenience)
- And if one worker refuses the adversary can move on to the next or just spam the entire company with a official-looking e-mail from tech support asking everyone to reset their passwords using this handy link… (phishing/spear-phishing attack).

Policies for human security

- A lot depends on context: rules for a tiny company are much simpler than a vast one. A lot of social engineering fails if everyone knows each other.
- However, the key insights remain constant and can be expressed in a series of simple guidelines which shape the formulation of security policies meant for members of an organization.

Guidelines

1. Establish clear rules and make them known in advance. You may assume that the 'default' behavior will always be low-security.
2. Establish certain things that *never* happen in official communication. A famous one is being informed that tech support will *never* ask you for your password.
3. Establish a clear method to verify suspicious circumstances and make it absolutely clear that using said method has no negative consequences. Make it painless to ask if someone is supposed to be there or not.
4. If at all possible, move away from passwords as a security measure. Prefer PINs and physical authentication tokens.
5. If passwords are unavoidable have a password policy and enforce it, especially when it comes to password reuse.

User-friendly security

- An important additional consideration is to try to implement security--both physical and operational security as well as the security you code--in such a way that it is user-friendly.
- If the user is doing everything right they should have as little interaction with security mechanisms as possible.
- Don't 'bug' the user with security
  - Consider the case of UAC in Windows Vista and the blowback it caused.
  - Every additional click/action/key you require increases the odds of users starting to develop creative workarounds.