Selecting locks for securing high-security premises (extended project presentation here, Lecture here)

An IT security professional's crash course to vulnerabilities of physical locks

Marek Šanta (433772) @ FI MUNI – Advanced Topics For Information Technology Security

1 Introduction

As a future Information Security professional, it does not matter if you will end up as a mere network administrator, manager, red-teamer, or (hopefully not) a black-hat. You should have at least basic knowledge of every security aspect – electronic, social, and physical. The devil, indeed, hides in the combinations[1].

IT professionals' perception of physical security is often limited to close attacks to the infrastructure alone and, possibly, electromagnetic and acoustic leakage. However, **the context in which an adversary can execute these attacks is ignored and considered "out-of-scope."** Why? Because it is not IT-ish enough. That part should be the job of locksmiths, security alarm integrators, and architects, you might think. But should you trust them? Even the standards they are supposed to obey (which they often do not) have a minimal viewpoint – EN 1627 is limited only to brute-force attacks.

Moreover, no public standard would truly consider any meaningful form of covert entry (even if they claim so). Even the Czech NBÚ[2] , as part of their certification process, considers only the most primitive form of lockpicking - bumping (1). So what kind of a security professional are you if you at least won't check that their job has been done correctly?

I bet that every one of you wants to know how to pick a lock or bypass it. And so do your adversaries. And it is an important issue. Why?

- It is much more accessible now than ever. For most locks currently being used, you can **easily buy tools[3], and their possession is not illegal here!**
- The information is **no longer exclusive to locksmiths** via special courses (2). You can learn how to use these tools thanks to videos on **YouTube,** and if you start now and take it seriously, your skills will be good enough in a while.

[1] There is a very interesting diagram from Chris Nickerson which should be self-explanatory (27)

[2] National Security Authority

[3] Among the best quality vendors are **Multipick, SouthOrd, Law Lock Tools, Sparrows, Peterson** and recently **Covert Instruments.** Classic locksmith tools manufacturers like **HPC** also have interesting picking tools. But you can find a great variety of much cheaper (and with considerable quality compromises) Chinese tools, especially from **Banggood's** "Locksmith Supplies" category. Some more tools can be found also on **AliExpress,** but the images are often censored for some reason.

- The manufacturing inaccuracies – the same physics that lets you pick the lock will allow other attacks we will talk about later and are **much simpler than picking**
- So-called “Locksport” is increasingly popular, and the community is vast and helpful
- The official percentages of household burglaries (1-6%) are probably **undervalued** because it is too **expensive to get forensic evidence**, and people would instead break their window to increase the probability of getting something from their insurance (opinion of myself)

2 KEYS

Before we start with locking mechanisms, there are a few important reminders about keys. These “tokens” are far from the cryptographic ones you know:

- Until there is an electronic element in the key[4], **it is always possible to copy** whether the profile is protected or not. With the magic of **casting**. **There are even specialized kits for this** (3)
- It is also possible to create a working key by measuring its **cuts** and determining the right **profile**. **Both can be derived just from a photo, and no, it is not complicated at all!** Then you can confirm the exact standardized values, profile, and cutting properties with locksmith software:
    - The most famous and complete is **InstaCode**. Full subscription with many useful information costs 30 USD per month, but older pirated version with older cracked database exists. (Just saying…) The same company has a great Android app **SnapDecoder** which makes decoding from a photo super-simple for everyone. It is limited to only a few types, but if you subscribe, you can decode almost every key. Anyway, Android app **ImageMeter** is a great free substitution if you can find the reference values somewhere. **KeyDecoder** is another possibility.
- Most locksmiths in Brno are not helpful when you provide them with all the information they need to cut the key. They either do not have the machines or are confused – they often know less about this topic than you will after reading this report. The only locksmith company that did not have any questions and was always able to fulfill my legitimate requests is H&B Group’s **Klíčové Centrum**[5] branch. Anyway, all the locksmiths **will always sell you the blanks**[6] , and you can make a working key by filing the cuts at home.

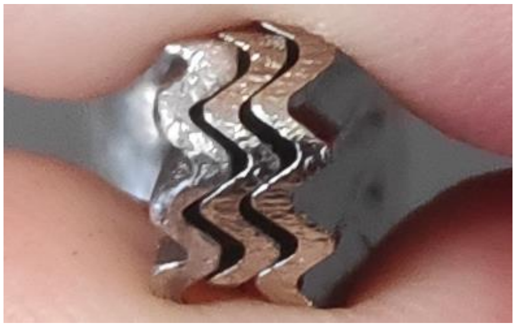

Figure 1: From left to right: Original restricted GUARD CPS master "C" profile key; Errebi TT14R modified to fit; TT14R without modifications

    - For the protected profiles this may be hard. But sometimes you can find a freely distributed blank that fits special profiles. One of the most famous companies, **Silca** has even a machine, called **Optika**, that scans the key profile and finds the most suitable unrestricted blank. For example, cross-compatible **Silca TN36R/JMA TIT-15/Errebi TT14R** or their reverses (i.e. in case of our faculty) seem to fit most **GUARD CPS** custom profiles with minimal and primitive modifications. And even for the worst-case scenario - **H&B** is

[4] It would still be mostly possible but it is out of scope of this project (it is too much IT 😉)

[5] The average retail price for a standard pin tumbler blank is 60 CZK and the cutting costs around 40 CZK

[6] The key of a particular profile without cuts. A working key is made by cutting it appropriately

  selling blanks without pre-milled profiles (28) and you can file these as well, although that might be more complicated. They will sell you these without any questions and the price is circa 350 CZK per piece.
  - Another interesting fact is that some locksmiths will copy basically anything without asking for the security card. You will just pay premium.
- The numbers on so-called **security cards** needed for copying protected keys are **just coded cuts** of a key. Unless these keys are part of a master-keyed system (see page 5) - then it often is a unique serial number, which is, however, engraved on the key most of the time. With all that, you can easily **botch a fake security card**.

3 Locking Mechanisms and their Vulnerabilities

The hunt for a perfect lock now begins. To understand the topic, we have to go over several locking mechanisms basics and discuss their vulnerabilities.

3.1 Pin tumblers

The largest and best-known group of mechanisms is a pin tumbler. That is any lock with multiple pins pairs: Spring-loaded from one side and key-interacting from the other. In the default state, the pins interacting with the spring prevent the cylinder from rotating. The cylinder is unblocked when all the gaps between the pin pairs are aligned at the boundary of the cylinder and the lock body. That boundary is called a **shear line**.

There are two basic types of pin tumbler locks. First is the well-known cylinder, where pins are perpendicular to the rotational axis. **Most existing locking mechanisms** are some form, modification, or an addition to the **cylinder pin tumbler**. These are mainly used for residential doors. The tubular locks with pins parallel to the rotational axis are primarily used on vending machines, bicycle locks, or cabinets.

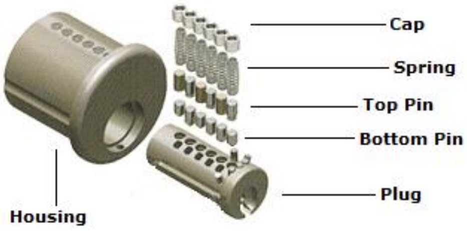

Figure 2: Cylinder pin tumbler

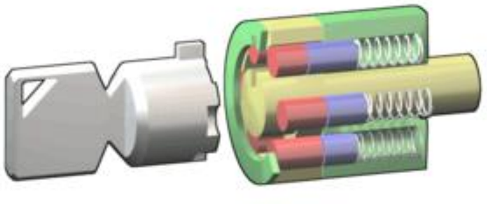

Figure 3: Tubular pin tumbler

The designed operation is that the correctly cut key pushes these pins to their correct levels. But we can do that **without the key** – with tools called **picks**. The only problem is **– how to find the correct depths?**

3.1.1 Pin tumbler bypassing

It turns out that it is nearly **impossible** to drill the holes for these pins so that they would be **precisely aligned**. That way, while applying **rotary tension** with a **tensioning tool** to the core cylinder, (mostly) only one of the pins is actually blocking the core. Because that pin will have greater friction, you can find it and try to level it. When that pin gets to the correct level, the core will **rotate a bit**, producing a “click” sound and leaving the pair of pins divided. Then the next pin pair will bind. You will find a ton of videos with animations on YouTube.

What I have just described is a "**single pin picking**" method. Oversimplified and idealized. But the physics behind this allows for many more attacks for which a minimal experience is needed:

- **Raking** – If the tolerances are too high, it is mostly possible to set the pins to a correct state by random fast movements of a pick
- **Snapping –** Is a term **I use** for various similar techniques that try to transfer the kinetic energy to the pins causing them to "dance" around a shear line, sometimes compared to the physics of billiard:
    - **Bumping** is using a special key and a hammer. The key is modified so that it's horizontal movement is transferred to a uniform vertical force applied to the pins. However, this is **not an effective method** for preparation because you need a special key for every profile, and it is hard to feel the correct tension because of the key being your tensioning tool.
    - **Snap gun** is much more universal because the force is applied directly through a thin rod and can therefore be used in most profiles. It also allows you to tension the lock however you want. There is also a primitive yet still very effective design of this tool made by a single piece of a spring wire (4).
    - **An electric pick gun** is a motorized snap gun that can produce fast periodical impacts, allowing a much quicker and more effective attack (5). **From my experience, this is the most effective attack for any cylindrical pin-tumbler lock. The only disadvantage is the noise. This attack needs little to no experience.** [7]
- **Impressioning** – with the right blank, file, and some time, you can create a working key (6)
    - **Self-Impressioning tools,** using the same physics, will set themselves to a correct setting. These tools are being made for **tubular locks.** (7) **This attack needs no experience whatsoever, and the tool changes into a working key that can be used anytime in the future immediately.**
    - Many more self-impressioning attacks (mainly using aluminum tape), some of them can be improvised (8). **These are also effective against so-called dimple locks** where the pins interact with a key's side instead of its bottom.

Also, If you thought that **multiple lock rotations** needed to unlock a door are a problem for a lockpicker, you're mistaken. Spinning tools can **spin the lock so fast** that the pins don't have time to slip into the core. (9) I also remember the old, poor's man attack from when I was a teenager: After picking the lock, you carefully fill it with wool so that both ends of the thread are still out of the lock, allowing you to pull it out later. That imitates an inserted key and lets you turn the core freely.

3.1.2 Securing the cylindrical pin tumblers

As You can see, **there is an effective attack that even a poor-experienced perpetrator can use for both types of pin tumblers.** Because the tubular locks are mostly still the same, vulnerable is almost every vending machine, poster cabinet in Brno public transport, washing machine coinbox, etc.

[7] A german company **Multipick** created a tool (called **ATT**) which eliminates the need for even the little skill needed to execute this attack (29)

But with the cylinder pin tumblers, there are a ton of modifications from different vendors creating new mechanisms, which are, supposedly, more secure:

- **Security pins** are special pins designed to mess with the feedback that a picker gets through his pick tools. A picker can recognize and overcome these pins with some experience. **However, these do little against the electric pick gun, which is, indeed, visible in the video** (5)
- **Multiple arrays of pins and sidebars** are increasing the number of pins needed to be picked. If done correctly, it can almost eliminate the possibility of picking with the electric pick gun by a novice.
- **Hiding the mechanism** is (in my opinion) a hype that allowed some companies to declare their locks as "unpickable." That is, however, hardly true. The most notable examples are the Bowley lock (10) and the Forever lock (11)
- **Crazy keyways – mostly paracentric** (profiles) are popular in Europe. These should make inserting and using the picks harder, but most of the time, leave the discussed snapping attacks possible.

To get a glimpse of how these and more advanced additions to the pin tumblers can be defeated, I recommend a video from Andre Vornbrock (12)

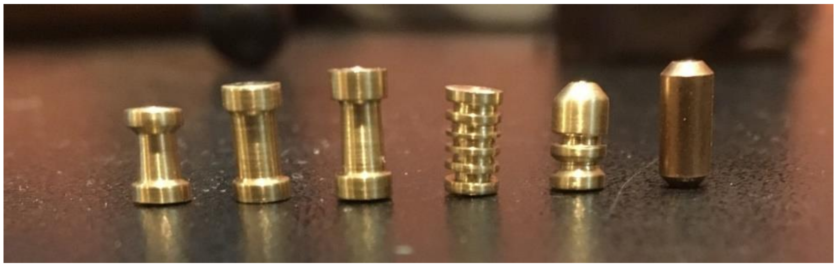

Figure 4: Some of the security pins used in pin tumblers

3.1.3 Master keying (or weakening the cylindrical pin tumblers)

In my experience, the most popular locking mechanism among companies and institutions in Czechia and Slovakia is a mid-level cylindrical pin tumbler lock with security pins. And most of the time, they come within what is here called a "**system**." The effect is pretty marketable: You can set access rights to different keyholders to open different doors. So there can be one key that opens all the locks and locks that can be opened by all keys. That is possible by inserting a so-called **master wafer** in between the two pins so that there are now two levels on which that pin "group" allows a core cylinder to rotate.

The cost is **much, much less pick-resistance.** Apart from the fact that there are now more combinations that can open one lock, the master wafers are rarely made as security pins. That together makes any of the snapping attacks more effective. Also, the **locks supposed to be working with all of the keys** are **effortless to pick**. These either have multiple master wafers in each pin chamber or have only a few chambers populated to make it work. Such locks' logical use is entrance doors or doors to common areas – making

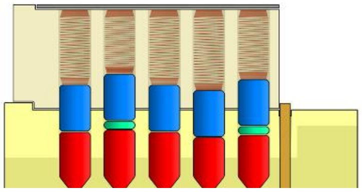

Figure 5: Master wafers (green) inserted between the pins

penetrating the perimeter insanely simple for an adversary. That is also the case for the heavily popular **GUARD CPS system used at our faculty and dormitories**[8].

On the contrary, master wafers can serve a different purpose; together with some cores, they allow your lock to block indefinitely (so that you have to dismantle it) almost every time somebody tries to pick it (13). *It is excellent protection with a bonus of providing unambiguous forensic evidence that the lock has been tampered with. However, this is probably* ***not something you should do when the secured premise's availability is essential****.*

3.1.4 Worthy examples

There are a few mechanisms that are currently very difficult to pick for even a mid-skilled picker (if there are no master wafers, of course). These are, for example, **ASSA Twin** family, **Kaba Penta,** or **FAB NZS3A**[9]**.** But make no mistake, I know of no pin tumbler lock that is currently unpickable for anyone with the right tools and publicly disclosed information! **That is why I would not use any pin tumbler lock alone for high-security premises**

3.2 Slider locks

Slider locks are relatives of the pin tumblers – but instead of pair of pins, only one **element** sits in each chamber, slides with various parts of the key, and tumbles directly against the outer cylinder. The most numerous representative is a **wafer tumbler** where that element is – you guessed it – a wafer. These locks are mainly used in **furniture**, **mailboxes**, and the rest of our favorite vending machines (that do not use tubular locks).

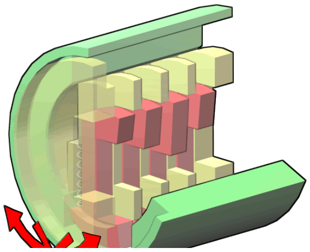

Figure 6: A Wafer lock in an incorrect state

3.2.1 Slider lock bypassing

The manufacturing **tolerances are always very high** – especially within wafer locks. I have never seen a wafer lock considered high-security**; almost all of them can be opened just by jiggling the wafers while applying moderate rotational force to the core. A child can carry out this attack successfully.**

But that is not all. **Most automotive locks**[10] **are slider locks**! And yes, the inferior properties hold.

The most notable example extremely popular in Czechia are **Volkswagen vehicle locks**[11] **(including Škoda)**. **Anybody** can open these with a recent specialized tool (14), fast.[12] And that is just an easier-to-use form of classic, also very much easy-to-use decoders from a Chinese master locksmith, Mr. Zhi Qin Li (marketed **Lishi**), widely available for a few years now, made for **almost every automotive lock**. These

[8] The geniuses from EVVA/GUARD also published a reference list of companies and institutions where these heavily master-keyed locks are being used. (31) Please, do not misuse that!

[9] The first video of picking this mechanism is from December 2020

[10] By the way, the locksmith software **InstaCode** also provides you with the information of how to unlock most of the cars without using the key – with simple tools. It also provides useful info about wireless transpoders you won't find anywhere else

[11] These are referenced to as **HU66** or **VAG** automotive locks. There are several generations!

[12] Yes, your old Felicia without immobilizer will not be stolen because nobody wants it, definitely not because of the lock.

tools allow You to pick and measure (decode) the lock immediately. I presume that my favorite locksmith branch would also help create a working automotive key just from these measurements.

This mechanism does not deserve any more extensive description. You really can open it almost by thinking about it 😉.

3.2.2 Worthy examples

EVVA ICS might be considered one of the better slider locks, certainly harder to pick than most others. But a hypothetical Lishi-type tool for this would make it fairly simple, and I believe it will come.

3.3 Lever tumbler locks

We are slowly approaching better mechanisms. Lever locks have a bolt fixed to a specifically shaped part – I call it a **block**[13] (remember that for later). Next, it has a set of (usually) spring-loaded levers blocking the block to move towards them. These levers have cut-outs (called **gates**) in a specific place so that when all the levers are at the correct height, the block can move inside them with the bolt retracting.

I have seen this kind of locks on the doors to the elevator machine rooms and the roof on most socialist prefabricated buildings (blocks of flats or “paneláky”) in Slovakia[14]. I have no clue why it was used there - in our countries, lever locks are being used almost exclusively in **vaults** (safes). That’s why the Czech name is literally a **safe/vault lock** (trezorový zámek).

As for the previous mechanisms, there are **many tools available that will help you open most of them.**

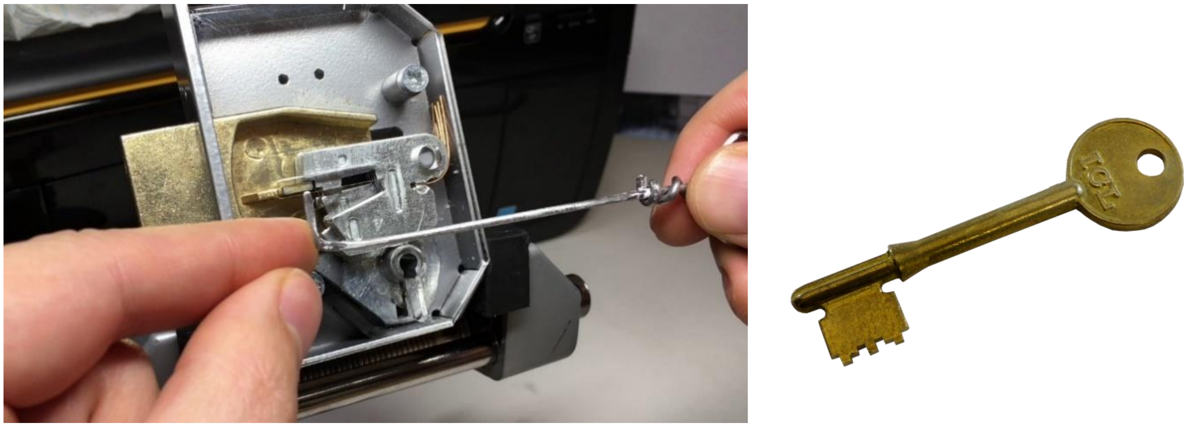

Figure 7: On the left: A basic lever lock with the bolt and springs of a brass color and levers of a silver color. On the right: A typical lever lock key.

3.3.1 Lever tumbler bypassing

The basic picking method is as follows: while applying tension to the bolt – trying to push the block inside the levers – you lift the levers one by one. There will be at least one lever rubbing against the block (binding). When that lever is raised to the correct height, the block will partly get into that gate, and you will feel a movement.

[13] Czech word for this would be “závorník” or “závorníček” in case of smaller, especially disc detainer locks. This is borrowed from firearm vocabulary. But in this case you might encounter a word “fence”

[14] These are being replaced by pin tumblers anyway

Of course, **attacks similar to bumping are not feasible here**[15]. But because this mechanism needs a lot of space, tampering with its other parts with long tools is possible. That way, **you can decode the lock by feeling the gates directly** without picking the lock and then creating a correct key.

3.3.2 Securing a lever tumbler

There are multiple ways to make a lever lock more pick-resistant:

- **False gates** are an analogy to the security pins. They mess with the feedback, giving you a false sense that you have that lever picked correctly.
- **Multiple level sets** that can make picking without specialized tools into an acrobatic stunt (15)
- **Single spring** common for all the levers makes setting one step back harder (needing to reset the picking) and also mess with the feedback
- **Shieldings** that should prevent the picker from accessing different parts of the mechanism

3.3.3 Worthy examples

I have very little hands-on experience (only the machine rooms) with these locks, but these are very discussed among the community. Mainly because of the legendary **Western Electric 30C.** That lock has been securing American payphones since the 1970s, and **only one person could ever pick it**[16]. Until this very year, after much effort from multiple community members, one lockpicker finally showed a way it could be picked (16).

A good example of actually available locks could be the **Ingersoll 10-lever** (15)**. Matt Smith**, a locksmith I am mentioning multiple times here, uses this mechanism (of course in a different form) to secure his front door.

3.4 DISC DETAINER LOCKS

The last group of mechanisms I am going to describe in more detail is disc detainers. They are similar to the lever locks – but do not use any springs and are much more compact. They consist of **multiple discs with gates** for which a small pin-shaped block, also called a **sidebar.** This block rests in a lock body cut-out and prevents the core from turning until it is "absorbed" by it. That can be done if all the gates are aligned so that the block can sink in.

That could be hard to imagine, and because there is no good enough image on the internet, I will help myself with animation from Schuyler Towne (17)

These locks are very popular in Scandinavia but are slowly conquering the world.

3.4.1 Bypassing a disc detainer

For most mechanisms that exist, you would want to **rotate the discs as far in the direction of picking as they will go**. Very similar to the lever lock, after applying rotational force, **the block is pushing against some of the discs, trying to get into the core**. Like in the previous mechanisms, you will find these discs

[15] Bumping a pin tumbler works by actually expanding the free space between the two pins. But a lever is just one part.

[16] In the 1980s a guy by the name of James Clark has stolen ofer half a million USD from Bell System payphones. He was even featured on America's Most Wanted twice (30)

thanks to the difference of friction. You then try to rotate it until a distinct “click” notifies you that the block has found a gate.

For this, however, using standard or homemade picks is almost impossible**. You have to use a specialized tool.** Currently, probably the best on the market is a *Silver Bullet* designed by Matt Smith (18). But there are other tools.[17] Because it is far from the most used mechanism, not much about all the possible attacks is known. It is, therefore, **believed to be the most secure** now. But in **the last ten years, there was significant progress**, either on the side of lock manufacturers and lockpickers. And the details of successful methods are mostly being kept secret so far. However, these are other ways to defeat disc detainers I know of:

- **Decoding:**
  - **By wire**: Sometimes, It is possible to slip a wire in between the disk and the spacer and find the true gate.
  - **By pressing the disc against the block directly:** Metal is a flexible material, and the discs are wobbly, so it is possible to press any of the discs so that it scratches the block without actually tensioning the core. I was able to observe this on the Czech **TOKOZ PRO** mechanism. It is also probably the way that decoding sets from Dimitar Ivaylov[18] from Bulgaria work for **Abloy** locks (19)
- **Impressioning and self-impressioning** The same guy – Dimitar Ivaylov, has uploaded a video ten years ago that probably showed the self-impressioning attack on **Abloy Protec**. The video is not to be found anymore, and it was largely disputed back then (20). Matt Smith has confirmed recently that this is possible.
- **Much more to come!** The disc detainers are currently in a state where **many 0-day vulnerabilities** are possible, but most are not disclosed. Matt Smith (yes, the same guy again) claims that he can now open Abloy Protec 2 in under 2 minutes (21) with one method after six years of research. And that other five methods could defeat it. Given his record, there is no reason to doubt. **Other people in parallel could have discovered these vulnerabilities[19]**

3.4.2 Securing a disc detainer

This is how the lock manufacturers are securing the disc detainers:

- **False gates -** As always, messing with the feedback and until the picker develops an exceptional sense for the particular mechanism, it is relatively hard to pick.
- **Return bars –** align the discs with a pair of sidebars. These are bound to the core’s rotation – if you return the tensioning parts, all the discs will reset. They also enable the **Disk Blocking System** by Abloy – when the core is tensioned, the sidebar slides into the discs, blocking all of them in place. That, in theory, makes the lock unpickable. There are, however, ways to bypass that.
- **Disc controller arms –** makes navigating the pick inside without turning the controller harder

[17] The most notable and known is the tool that LockPickingLawyer and BosnianBill made (google that!) and the classic chinese one you will find on AliExpress. These are, however, very limited to front-tensioned mechanisms.

[18] By the way, the guy makes some of the most advanced and easy-to-use decoders for automotive locks. They are not cheap though.

[19] This has been done previously. Matt Smith was also the first who designed and published a tool for Abloy Classic. Only to discover that some secret services have ben using basically the same tool for years before.

- **Shielding –** makes some of the bypass attacks impossible

3.4.3 Worthy examples

The most popular and considered as most secure by many is **Abloy Protec 2.** It definitely is the most advanced disc detainer locking mechanism that currently exists. However, it's popularity automatically attracts many lockpickers, either good, controversial (government), or the bad.

A Czech company TOKOZ makes a **TOKOZ PRO** mechanism and markets it as virtually pick-proof. It is a very nice lock, but the patent is basically about making the original Abloy Protec (the first one) as cheap as possible. It does not have false gates, the discs are too wobbly, it does not have the disk blocking system, and reduces the possible key cut combinations to 65536. I am sure that it can be opened or decoded fast with the silver bullet, but it is a nice try, and it is Czech. However, it has recently become popular in China, so I am waiting for new cheap tools.

3.5 Magnetic locks

This category is here just for completeness; I won't go into details. **These are not unpickable at all!** You can find **EVVA MCS** videos all generations picked, and the magnetic key might not be something you would want to get near some of your electronics accidentally. The key and the lock might also be magnetized in a different way if it encounters a strong field – making them unusable. Finally, I can imagine self-impressioning tools that could be available for them in a few years.

4 Selecting the right lock

I have promised You that you would be able to select the appropriate lock for the premises you are responsible for. For that, the most important part is **awareness** about the essential basics of locks and their vulnerabilities.

Well, this is relatively challenging. Until you make it your hobby, you will never contain it all. But gladly, there is the **magic of Reddit**. The **lockpicking subreddit** has a "Karate Belt Ranking System" that allocates the belts to the members according to the locks they were demonstrably able to pick (22). In there, You will find a link to a fresh **Google Docs sheet.** That contains all the possible locking mechanisms classified by the "wisest" community members.

Now, all the locks you will find in the **Brown belt and lower - You may forget about them**. Next, when you find a lock that is available on our market, just google search: if there is a video where somebody **picked it under 2 minutes, or if there is a special tool for it. If yes, you can forget about these locks too.** Right now, the Bowley lock is pretty much not worth the Black belt.

With what you are left, try to select two very different mechanisms – preferably a disc detainer and a lever lock. I would also accept pin tumblers with many arrays (such as Kaba Penta). Whatever you choose, it should be **exotic** to our market so that **the chances of finding a person with the exact skillset and tools required to open both of them are low.** If possible, you may also gather very special locks such as the WE 30C or **NATO Mersey** and incorporate them somehow.

Use this combination of two locks on your door to a high-security premise. That's it.

I had initially planned to provide you with particular tips, even a cheat sheet for different purposes. **But then I realized that some of You might start practicing to gain the skills for my combinations.** And that is unwanted attention. Also, it might be that if you read this paper when it is released, **my tips might already be obsolete**. My goal is to increase the diversity of locks used to protect all the premises – that won't be achieved if you will just accept what the locksmith offers you**.** So never settle down with your locks for a long time! The community is continuously growing, and the number of persons able to pick them will always be higher as time progresses.

Anyway, keep yourself educated. Closely watch the new information from the sources provided, and I hope you will stop ignoring the locks you are passing by every day. Also remember, that physical penetration is far from being just about locks. Please read the appendix to get a glimpse of that.

5 References

1. **Národní Bezpečnostní Úřad.** Metodika zkoušení odolnosti cylindrických vložek proti bumping metodě. [Online] 2008. https://www.nbu.cz/download/aktuality/prohlaseni-tiskove-zpravy/metodika-bk.doc.

2. **H&B Group s.r.o.** HB TV H&B ACADEMY - školení otevírací techniky. *YouTube.* [Online] 2014. https://www.youtube.com/watch?v=LM0_r2wlq8s.

3. **Multipick.** Quick-Key Easy Pro - Key Duplicator. [Online] https://shop.multipick.com/en/locksmith-tools/key-copier/quick-key-easy-set.

4. **Šanta, Marek.** Homemade snap pick slowmo. *Youtube.* [Online] 2020. https://www.youtube.com/watch?v=R2WmPPnE9uU.

5. **Multipick.** Lockpicking Elektropick - Multipick MHP. *Youtube.* [Online] 2012. https://www.youtube.com/watch?v=qO67Tdy3D0g.

6. **Bosnianbill.** How to Impression a Key. [Online] 2016. https://www.youtube.com/watch?v=jciQpGdAVtc.

7. **LockPickingLawyer.** Banggood/HUK 3-Piece Tubular Lock Impressioning Tool Set Review. [Online] 2017. https://www.youtube.com/watch?v=4rCUK5K6wwY.

8. **(huxleypig), Matt Smith.** Self Impressioning; the Locks That Pick Themselves. [Online] 2020. https://www.youtube.com/watch?v=BFTIbAvtvak.

9. **Šanta, Marek.** Spinning tool - demo. *Youtube.* [Online] 2020. https://www.youtube.com/watch?v=L67UhsyxBRs.

10. **(huxleypig), Matt Smith.** Bowley Lock Opened Quickly and Easily. *Youtube.* [Online] 2019. https://www.youtube.com/watch?v=KS0FSzamUzc.

11. **Ollam, Deviant.** Foil Attacks - 02 - Foiling the Forever Lock. *Youtube.* [Online] 2014. https://www.youtube.com/watch?v=UGHjW3ZbCT8.

12. **Andre Vornbrock, OzSecCon.** Andre Vornbrock - High Security Lockpicking - OzSecCon 2018. *Youtube.* [Online] 2018. https://www.youtube.com/watch?v=1UDSqioshDo.

13. **LockPickingLawyer.** Pickproof your Kwikset For Less Than $1. *Youtube.* [Online] 2017. https://www.youtube.com/watch?v=7JlgKCUqzA0.

14. **Lock, Beginners.** New type Hu66 Kwik decoder. [Online] 2019. https://www.youtube.com/watch?v=hEEoFIQZHs0.

15. **LockPickingLawyer.** U.S. Military “Miracle Lock” with Ingersoll 10-Lever Core Picked and Gutted. *Youtube.* [Online] 2018. https://www.youtube.com/watch?v=FCY5iXqPOUc.

16. **NØthing.** DEF CON Safe Mode Lock Picking Village - NØthing - How I defeated the Western Electric 30c. *Youtube.* [Online] 2020. https://www.youtube.com/watch?v=wHpXsmnd-XA.

17. **Towne, Schuyler.** Disc Detainer Lock Animated. *Youtube.* [Online] 2011. Disc Detainer Lock Animated.

18. **Smith, Matt.** Silver Bullet tool. *Silver Bullet.* [Online] https://silverbullet.tools/.

19. **Ivaylov, Dimitar.** Abloy Novel Decoder. *Youtube.* [Online] 2019. https://www.youtube.com/watch?v=TkjLhnaYJn.

20. **“self impressioning” attack on the Abloy Protec? *blackbag.toool.nl.* [Online] https://blackbag.toool.nl/?p=1359.**

21. Smith, Matt. Adventures in Discworld - OzSecCon 2018 - Matt Smith. *YouTube.* [Online] 2019. https://www.youtube.com/watch?v=GBaihzVxs5Y.

22. Pearson, Cliff. Lockpicking Karate Belt Ranking System. *GitHub.* [Online] https://github.com/crpearson/lockpicking.

23. Ollam, Deviant a Wild West Hackin’ Fest. I’ll Let Myself In: Tactics of Physical Pen Testers. *Youtube.* [Online] 2017. https://www.youtube.com/watch?v=rnmcRTnTNC8.

24. Šanta, Marek. Challenges of securing a custom embedded system. *santomet.eu.* [Online] 2018. https://santomet.eu/2018/11/26/challenges-of-securing-a-custom-embedded-system/.

25. —. Triggering microwave REX. *santomet.eu.* [Online] 2020. https://santomet.eu/2020/02/07/triggering-microwave-rex/.

26. Ollam, Deviant. The Search for the Perfect Doors. *Youtube.* [Online] 2016. https://www.youtube.com/watch?v=4YYvBLAF4T8.

27. Nickerson, Chris. Quora. [Online] Lares Consulting. https://qph.fs.quoracdn.net/main-qimg-ba1e957cab0d0076c29a48640d0aa152.

28. H&B Group s. r. o. Speciální polotovary klíčů Verze 2. [Online] https://www.hbgroup.cz/images/stranky/katalogy%20a%20ceniky/Katalog%20speciálních%20klíčů/Katalog_specialnich_klicu_v2.pdf.

29. Multipick. Brandneu! Multipick ATT mit MHP II Plus Elektropick - Digitales Öffnungssystem. *Youtube.* [Online] 2017. https://www.youtube.com/watch?v=n4htPAD1MKc.

30. 20th Television. America's Most Wanted (1988) - FBI's Most Wanted List & Fugitives. *Youtube.* [Online] 1988. https://youtu.be/e56gA8NBXuQ?t=1250.

31. GUARD – Mudroch spol. s r.o. GUARD Produktový katalog. [Online] https://web.archive.org/web/20191223211730/https://files.oivancic.cz/js27pjiatt01/GUARD_KATALOG.pdf.

6 Appendix: Bonus - Other Forms of Covert Entry

For completeness, let's discuss other ways one could enter the premise. **Because even if you find a perfect unpickable lock, it won't matter if you first do not take care of the following**:

6.1 Social

A human factor is most prone to error. Everybody knows this. **Try to come up to our faculty reception** when COVID restrictions end **during the work hours, tell some name, say that you are a fresh employee of some company with an office in the "S" building and that they did not give you the key yet.** What do You think will happen? **You will get the key!** Physical pentesters also like to pretend to be a contractor and would gladly dig through your trash cans only to gather the needed details. Most of the physical-social-engineering tactics are known for years. Yet, somehow, the companies and institutions are often reluctant to put a process in place. Also, the eligibility of employees is next to impossible to check; the right to execute a security clearance in which one can use every resource[20] is exclusive to government organizations. **So, first of all, set a comprehensive policy and enforce it.** Adversaries can think of millions of tactics; Deviant Ollam's talk (23) might be helpful to remember that! **However, white-hat red-teamers would never try everything possible!** Imagine a scenario when an adversary breaks into an employee's home to copy all of the keys and chips he could find. That is impossible to do legally, but a black-hat does not mind. I'm sure you all can imagine the consequences.

6.2 Electronic

Another essential vulnerability is a reliance on electronic access control systems. You probably know about the dumb EM MARINE chips used at our university and their weaknesses. But even the "top-secret" certified systems we are using have childish vulnerabilities. One[21] is being used in our dormitories. And I managed to get the chip data by a simple MiTM attack and pair them to a particular person thanks to our information system (24). The (of course, purely hypothetical 😉) outcome is apparent. Also, try to notice other ways these systems can be bypassed, like Request-To-Exit sensors (25). Another problem is all-in-one embedded systems with all the electronics outside – leaving relays vulnerable to magnet attacks or circuitry with which you can interact. Even LockPickingLawyer had a

[20] The security clearance process of Czech National Security Authority (NBÚ) for the "přísně tajné" (top secret) level has only one limit according to the law: human dignity should not be touched. Otherwise, during the one-year period it is supposed to be running, they can use the secret service and do absolutely everything you can think of. Legally.

[21] Honeywell NetAXS-123 has a top secret certification by NBÚ.

series of videos regarding some of these systems. And remember that tampering detections won't be useful if an adversary knows about them. So, **do not trust the access control systems entirely, isolate them, and do not use backdoors like REX.**

6.3 Physical

Before buying the locks, you have to think about where do you put them. Integration and structural vulnerabilities are much more common than lockpicking. With brute-force attacks considered in the mentioned standard, we are left with many potential soft attacks. To get a glimpse, I would recommend watching another talk from Deviant (26). There are, of course, many more. So **select the door, and it's elements properly.** Also, remember that doors are not the only openings in the building! Many burglars are using the window. Opening a classic tilt-and-turn window from the outside is relatively easy with various (slightly) destructive and non-destructive attacks that won't be detectable with your acoustic glass breaking detector. There might be many other entrances you even do not know about, especially on older buildings – emergency exits from bomb-shelters, coal lift shafts, coal holes, loft doors, etc.

6.4 Mind your security levels

There are some very prevalent bad habits, such as storing your high-security key in:

- A lockbox – most of the time locked by a terrible wafer lock or a combination lock[22]
- The room which itself is secured with a much cheaper and easier-to-pick lock[23]
- Hung up on a notice-board[24] or anywhere else visible where it could be photographed or remembered – sometimes the even lockboxes are from a transparent glass
- Inserted with the whole keychain in the lock from the outside – photographing the keys is one thing, but I especially love to copy keyfobs

[22] Mostly the companies like these little boxes

[23] I have noticed this in my dorm: The central key has been kept in a room locked by old FAB cylinder, providing absolutely no pick-resistance.

[24] That is the case of an unnamed professor at our faculty