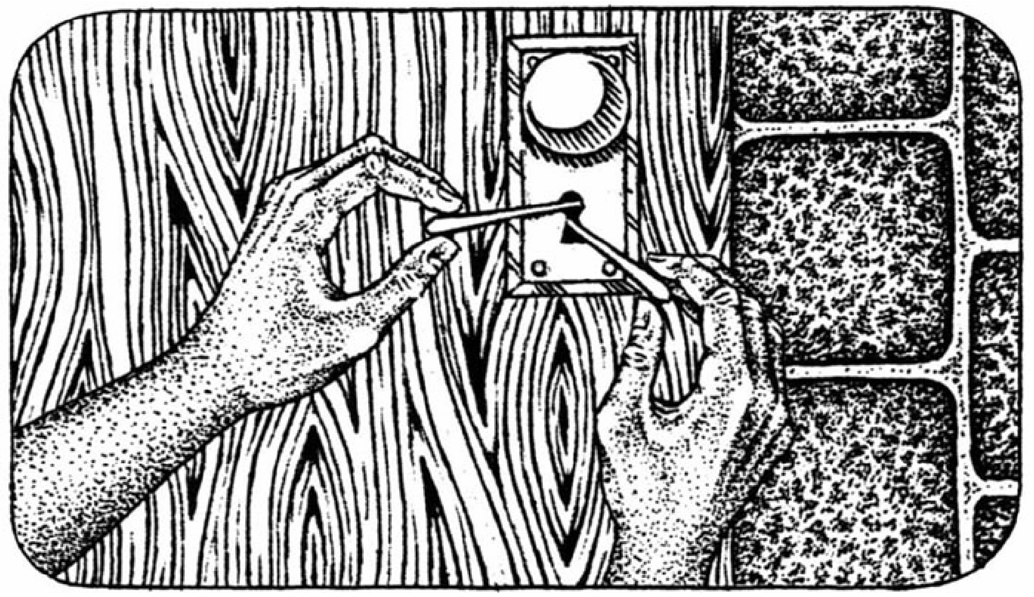
Ten Things Everyone Should Know About Lockpicking & Physical Security

Deviant Ollam



Physical security is an oft-overlooked component of data and system security in the technology world. While frequently forgotten, it is no less critical than timely patches, appropriate password policies, and proper user permissions. You can have the most hardened servers and network but that doesn't make the slightest difference if someone can gain direct access to a keyboard or, worse yet, march your hardware right out the door.

These ten general points will give you a solid overview of the weaknesses in many security designs as well as an understanding of how certain (often very small) changes to how locks operate and are utilized can make a huge difference in the security of your facilities as well as your data.

1. Locks are not complicated mechanisms

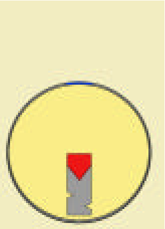
In general, locks are very simplistic devices that are employed to address very a straightforward problem. When areas or objects require security (which is most often defined as "keeping unauthorized people out") there is a very simple and ideal solution… installing them within an ultra-hardened structure constructed out of reinforced concrete and metal cladding with no doors, windows, or other openings.

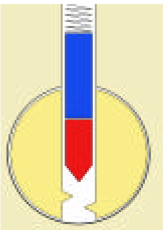
This is impractical in the real world, however, because in life our goal isn't simply "keeping unauthorized people out" but also "occasionally allowing authorized people in." A hallway can have a huge wall of stone stacked from floor to ceiling. This will prevent unauthorized passage. If constructed without mortar it can be disassembled to allow the periodic travel of someone with permission to pass through. However, again we see a flaw requiring a refined definition.

What we really want, of course, is a way to keep unauthorized people out while letting authorized people in "with a minimum of hassle, cost, and effort" in the process of securing or opening such clearance. That is, at its most basic, the purpose locks serve in our lives… they are a way to provide (in theory) rapidly-deployed and easily-removed barricades that alternately restrict or allow easy passage or access to a sensitive resource.

All locks (even the bad ones) do this with amazing efficiency. Their designs are not complicated, and by looking at some internal diagrams we can take a lot of the mystery out of these devices.

When viewing a typical lock from the outside, this is often the perspective that we can see. Within the lock's main body housing there is a round plug. This plug is what turns during the successful operation of the lock. On a the most conventional locks, there will be a hole called a keyway, into which a physical token is inserted by the user. Often, if you peer directly into the keyway, it is possible to see at least the tip of one of the many pins that sit within most locks.

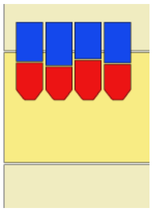




If viewed in a cut-away fashion, this is how most locks would appear. There is, in fact, not a single pin but rather there are *two* pins sitting atop one another. The bottom pin (also called the "key pin") appears in red in this diagram. The top pin (also called the "driver pin") is shown in blue.

As you can see, when the pins are at rest and hanging fully-down (springs atop the pin stack apply pressure keeping the pins down unless something specifically lifts them) the plug cannot be turned, since the driver pin is "binding" and in the way.

If the correct key is inserted into the lock, however, the pin stack will be lifted to the right amount and the space in between the two pins will be at the height of the "shear line" which allows the plug to turn.

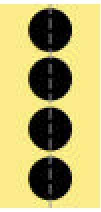


Now, in an actual lock there is not just a single key pin and driver pin. There are multiple pin stacks, each of which needs to be raised to the proper height in order to prevent the drivers from binding. When the blade of the proper key is inserted, the bottom pins will ride along the cuts on the key (known as the "bitting") and lift the stacks correctly.

2. Most locks are wildly easy to pick

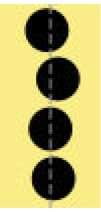
In theory, the more pin stacks a lock has, the more secure it should be. More stacks means more possible key variations and greater difficulty in getting all the pins to raise properly.

This is not entirely the case, however. Basic flaws that are present in nearly all lock designs make it possible to attack the pin stacks *one at a time*, allowing someone to compromise the lock regardless of how many pins it contains.



If pictured from above, most people would assume that during its construction, the pin chambers are drilled in a very regular pattern... evenly-spaced and in a straight line. This would result in perfectly-aligned pin stacks, and if someone attempted to rotate the plug without using the correct key, all the driver pins would simultaneously "bind" and prevent the plug's movement. This is the goal, but manufacturing processes are often less than perfect.

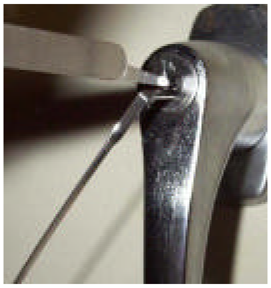
In reality, there are almost *always* imperfections in the alignment of the pin chambers. While this diagram is perhaps a bit exaggerated, the misalignment can be *very* profound in locks manufactured on a low budget. The machine tolerances at some factories are very poor.



In situations like this, attempts to rotate the plug will still fail, but it is only *one* of the pin stacks that is holding the plug in place. Because only one pin is ever really binding at a time, it is possible to attack the lock one pin at a time.

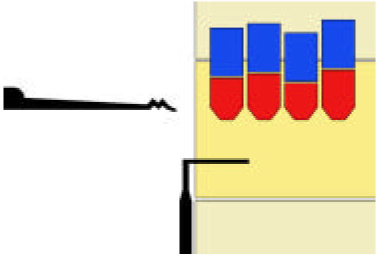
Lockpicking is performed by applying a bit of torsion pressure on the plug (typically with a tool called a wrench) which causes at least one driver to bind. Then, the whole pin stack can be gradually lifted (using another tool, simply called a pick). If the lifting is done precisely and methodically, eventually the stack will be at a height where the pins are perfectly aligned at the shear line.

When this happens, the driver pin will no longer be binding. If there is still pressure being applied with the wrench, the plug will rotate slightly. Then the lifted driver pin will typically "hang" on the lip of the lower pin chamber and *another* pin stack will be in a position to bind. The process can then be repeated with other pin stacks.



A lockpicker can apply some torsion with a wrench and then methodically lift the pin stacks, sometimes finding binding stacks and setting them to the appropriate height. When all stacks have finally been lifted correctly, the plug is free to fully turn.

The two biggest errors that people make when attempting to pick involve the use of too much force. Too much torsion pressure with the wrench will bind the pins too hard and make lifting the stacks difficult. Lifting the pins too high will raise the *bottom* pin up into the shear line and not allow the plug to rotate. If this happens, the only way to proceed is to release torsion pressure (allowing all pins to fall back down) and start over.



In addition to the methodical "pin by pin" picking technique, there are other ways to attack the pin stacks. A less sophisticated, but often no less effective, technique is "raking" or "scrubbing". A different pick tool (called a rake) is inserted in and out of the lock while light tension is applied. Unlike lifting tools (which are often hook shaped) rakes tend to be wavy or have multiple points. The idea is to jiggle and pop the pin stacks into position very rapidly.

Raking works best on locks with *very* loose mechanical tolerances, where sometimes multiple pin stacks can become properly "set" almost simultaneously.

3. Unpickable doesn't mean invulnerable

To impede traditional picking attacks, some manufacturers have redesigned the internal mechanisms in their locks. However, in many cases, this has been a process simply of *re-arranging* the same, basic pins that common locks possess. The same weaknesses are often still present and can be exploited just as easily, simply by using new tools or new techniques.

Dial Combination Locks

Just about everyone has seen or used a dial combination lock. These locks are everywhere, particularly in the North American market. They are so ubiquitous because they are inexpensive, simple to operate, and do not require the user to keep track of a key or any other physical token.

Unfortunately, these locks provide almost zero security. The mechanism within is highly simplistic. The shackle has a single notch cut and this interfaces with a small locking bar within the lock body. The primary flaw in this design is the manner in which locking bar operates. While dialing the appropriate combination will mechanically retract this bar, all users of this lock know that the bar can also be "pushed" back out of the way… this is what happens when the shackle is closed. A user doesn't need to re-enter the combination to close the padlock, they simply snap it shut. The locking bar is spring-loaded. This convenience to the user is also a critical flaw, however, since the locking bar will slip backward and out of the way when *any* force is applied to it. The bar doesn't know *what* is pushing against it… it just acts as if the shackle is coming down and springs back.

The primary tool used to bypass the latching mechanism inside of a padlock is called a shim. As seen here, shims come in a variety of sizes (in order to accommodate various lock sizes and shackle thicknesses) but their overall shape remains consistent. Manufactured typically from spring steel, retail shims are inexpensive but sturdy. At a little over a dollar per shim, a user can often get a dozen or more uses successfully out of such a device before seeing the metal start to fail. For even cheaper (and yet still weaker) shims, it is possible to fabricate this exact same design using the aluminum metal of beverage cans. Googling for "beer can shim" or some other similar query will yield a number of results, including guides published online by this very author, complete with step-by-step photos.

While the locks shown in this shimming section have been dial-combination style, it is possible to shim many popular padlocks, including those that operate with a key. The primary difference pertains to one versus two internal locking bars. Dial combination padlocks almost *always* have just one locking bar, and in every single such lock I've ever examined, it is on the left side of the shackle as you face the lock. Keyed padlocks have two locking bars and thus have notches cut into *both* sides of the shackle more than half the time. Such locks can often still be shimmed just as easily, but of course two shims are required. This requires significant wiggle and play to be present where the shackle inserts into the lock body. On locks with very tight gaps, the best advice is to try shimming with thin (albeit weaker) material such as aluminum from a beverage can.

Tubular Locks

When tubular locks appeared on the scene they were immediately popular on the grounds that traditional picking tools and picking methods would not be applicable to such a mechanism. Unfortunately, while older tools and techniques do not apply to this style of lock, it is still constructed with the same types of pins and mechanisms that you see in traditional "blade key" hardware. The same weaknesses and physical attacks apply, they simply are carried out with small variations.

In fact, there are those who could say that the tubular lock design is even *weaker* in some ways due to the fact that each of the pins stacks is clearly visible and easily manipulated independently. Tubular pick tools are made to accommodate the two most popular styles of tubular locks: 7-pin and 8-pin. It is worth pointing out that the *vast* majority of tubular locks are 7-pin. I have never personally encountered an 8-pin tubular lock in my life.

Some exceedingly poor tubular locks can actually be bypassed by inserting any round object into their keyway… this attack gained notoriety for Kryptonite brand bicycle locks in years past. That company has since updated their design, and other manufacturers have made advances in higher-security tubular locks. The ACE company makes tubular locks popular with the vending machine and gaming machine industries. These locks (called the ACE and ACE II) employ springs with varied pressures in each chamber, which helps defeat many tactics.

Dimple Locks

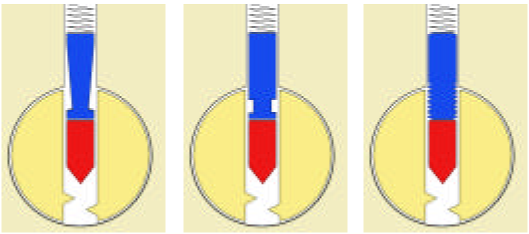
Dimple style locks and keys are another example of manufacturers attempting to thwart lock picking by making designs that do not lend themselves to the use of traditional pick tools. These locks are given their name by the fact that the keys do not have bitting cuts on the side of the "blade" but rather have small holes drilled to various depths along their flat side. These holes are called dimples.

The horizontal keyway of a dimple lock is very small and makes the insertion and use of traditional pick tools very difficult. However, even though they cannot easily be picked, dimple locks are susceptible to a number of other attacks, impressioning and bump-keying chief among them. Bump keying will be covered later. Impressioning is a tactic where some kind of soft or malleable material is inserted into the lock and worked into shape by the pins. In many cases, the plug is wiggled and pins will rub and jostle as they bind. This minute movement is enough to make impressions in the soft material. Gradually, these impressions deepen until a specific pin stack is at its "proper" height. When that height is reached, the stack is no longer binding and therefore will cease impressioning deeper into the soft medium.

It is possible to perform impressioning attacks against "blade key" style locks but the tools and methods used are more precarious. Dimple locks, with their nice bowl-shaped cuts supported on all sides by flat metal surfaces, are easier to impression than almost any other type of lock.

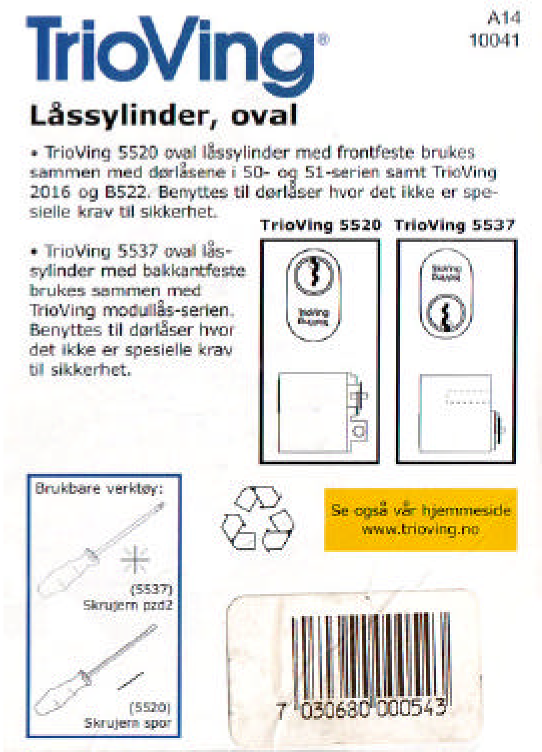
4. Minor changes make a big difference

There are some very minor changes in the components of a lock that can frustrate traditional picking attacks immensely. These changes in design often contribute very little to the cost of the lock and are a great way to achieve security in an economical package.



Specially-shaped top pins (a.k.a. driver pins) can frustrate typical picking and raking attempts. Top pins with a "mushroom" or "spool" shape can catch on a side lip during picking and not lift high enough to clear the shear line. Spool pins are particularly insidious because they give the "click" feeling and resultant slight movement of the plug associated with a successful setting of a pin without actually clearing the shear line. There are also serrated pins, whose multiple grooves catch and bind almost everywhere making the lifting process nearly impossible.

These specialized security pins are much more common in European locks than those seen in the American market. Note this packaging from the Norwegian brand TrioVing.



TrioVing®

A14
10041

Låssylinder, oval

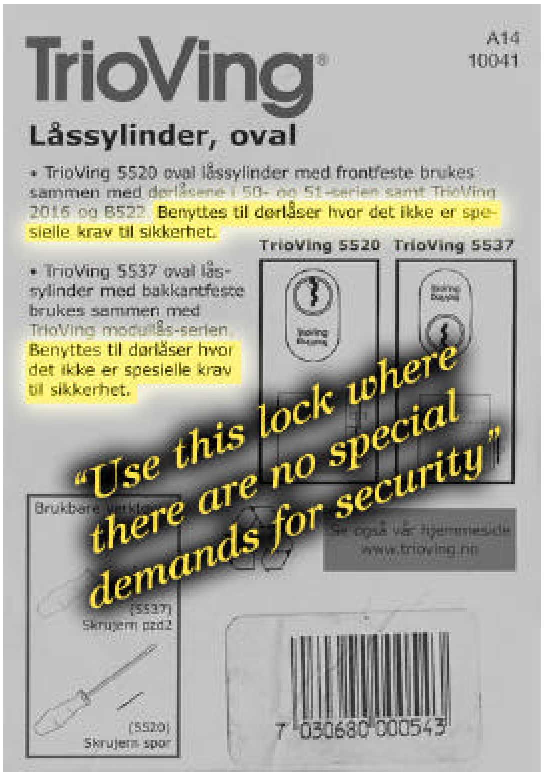
- TrioVing 5520 oval låssylinder med frontfeste brukes sammen med dørlåsene i 50- og 51-serien samt TrioVing 2016 og B522. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.
- TrioVing 5537 oval låssylinder med bakkantfeste brukes sammen med TrioVing modullås-serien. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.

TrioVing 5520 TrioVing 5537

Brukbare verktøy:
(5537)
Skrujern pzd2
(5520)
Skrujern spor

Se også vår hjemmeside
www.trioving.no

7 030680 000543



TrioVing®

A14
10041

Låssylinder, oval

- TrioVing 5520 oval låssylinder med frontfeste brukes sammen med dørlåsene i 50- og 51-serien samt TrioVing 2016 og B522. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.
- TrioVing 5537 oval låssylinder med bakkantfeste brukes sammen med TrioVing modullås-serien. Benyttes til dørlåser hvor det ikke er spesielle krav til sikkerhet.

TrioVing 5520 TrioVing 5537

Brukbare verktøy:
(5537)
Skrujern pzd2
(5520)
Skrujern spor

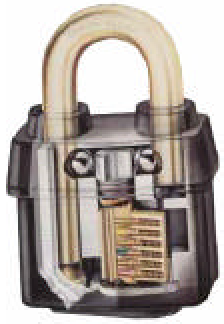
Se også vår hjemmeside
www.trioving.no

7 030680 000543

"Use this lock where there are no special demands for security"

For those who can't read any Scandinavian languages, the text here clearly states that this is far from a high security lock and that it should not be used in any sensitive installations. And yet, *every single chamber* of this lock (which is a six-pin lock, by the way) has a double-mushroom style spool pin in the top slot. That's how they do *base model* security in Europe.

Many padlocks (on both sides of the Atlantic) contain protections against shimming. The most common is something known as a "double ball" mechanism. High security padlocks will often mention their "double ball" or "ball bearing" feature on their prominently packaging. In such a design, there is no spring-loaded retaining bar as seen with the dial combination locks before. Instead, a pair of solid steel balls retain the shackle. These balls can only fall inward if the "control cylinder" between them rotates. Such control cylinders are almost always connected to core consisting of a plug that interacts with a traditional key.



It is also possible to achieve shimming protection in a dial combination lock, however. Those who (for example) visit a gym or simply don't want to contend with keys can look for Sargent & Greenleaf model 8088 or 8077 padlocks. These locks (the 8077 is actually the more modern variant) are used by the Department of Defense on file cabinets. They are of good quality and will resist shimming and manipulation attacks very well.

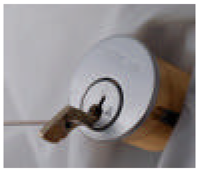
5. Advanced features aren't a panacea

There exist even higher-security features than the specially designed pins described above. Many of these provide excellent protection from nefarious attacks. Others have some weaknesses that should be understood.

Schlage's Side Pin

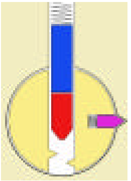
One of the first well-known and popular attempts where we saw the lock industry designing features that went *beyond* mere pin stacks was the Schlage Everest. On this lock, the plug contained an additional pin. The "check pin" will impede plug movement unless an appropriate key is inserted into the plug.

The Everest key has a long groove down the side. This channel catches and then raises the check pin. While this is an interesting and rather nice system, there is no variation in the size, position, and functionality of the check pin. It is the same size and operates the exact same way in all Schlage Everest locks.

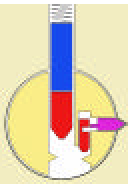


Because of this, it did not take long for specialized tools to be developed for the Everest. Specially-designed torsion wrenches can lift the check pin. Also, some industrious people just cut down Everest keys and used them *as* to apply torque force to the plug.

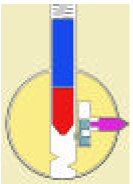
Side Bars



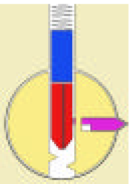
Better than the check pin (or "side pin") technique, is the type of mechanism known as a "side bar" which can be found in many high-security locks. Side bars run the entire length of a plug and will prevent rotation. Side bars will not fall inward unless any number of specific conditions are met.



Some side bars interact with tiny sets of "finger pins" seen here on an Assa V-10 twin lock. These smaller pins are operated by a set of cuts milled into the side of this traditional blade key.

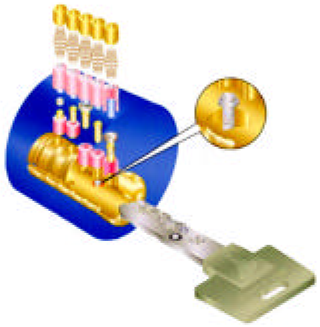


Other sidebars interact with small plates of metal known as "sliders" which maneuver along tracks cut into the side of a key, as seen on this 3KS lock by Evva.



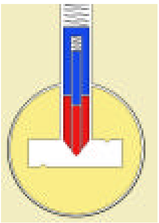
The Medeco high security lock has a unique sidebar. On these locks, the bottom pins actually rotate within their chambers, exposing a groove in their side into which part of the sidebar can insert.

Mul-T-Lock's Telescoping Pins



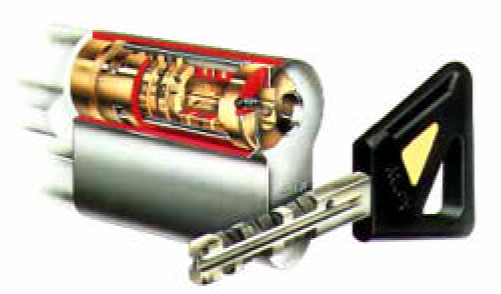
The Mul-T-Lock company (who has been acquired by the Abloy group, a conglomerate that has bought out *many* high security lock manufacturers, including Medeco) has developed a specialized dimple key system that uses pins within pins. This "telescoping pin" design prevents the impressioning attack described above in the traditional dimple lock section.

The Mul-T-Lock company (who has been acquired by the Abloy group, a conglomerate that has bought out *many* high security lock manufacturers, including Medeco) has developed a specialized dimple key system that uses pins within pins. This "telescoping pin" design prevents the impressioning attack described above in the traditional dimple lock section.



What many people do not know, however, is that the top pins (both inner and outer) do not operate independent of one another. It is possible, at least in theory, to over-lift the inner pin stack and in the process take the entire top pin array up and out of the way. Eric Michaud published proof-of-concept attacks against older versions of the Mul-T-Lock. The manufacturer has since updated their designs a number of times, however, and newer Mul-T-Locks are considered very secure.

Rotating Disks



The Abloy company (particularly in their line of Abus products) offers a type of lock mechanism called the "rotating disk system". These sorts of locks perform very similarly to how safes operate. A set of wheels must all be rotated into the appropriate position, allowing notches on their sides to align and accommodate a sidebar's inward motion. These locks are *very* secure and cannot be picked without specialized tools and great skill.

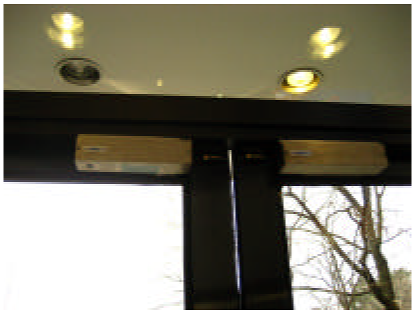
The tool used to manipulate the inner disks of an Abloy lock is manufactured by John Falle. It is expensive and takes time to use properly. Newer revisions by Abloy make the use of this tool even more difficult, if not practically impossible in some instances.

6. Adding electricity isn't magical

It should be noted that many lock systems incorporate electronic components. Many safes, particularly small models in hotel rooms, are electronic. Some "high security" deadbolts have electronic elements within them. And, of course, access control systems with keypads or proximity card tokens are electronic systems.

There are a number of ways that electronics can fail to protect secure areas as intended. The accompanying videos show some of the faults of hotel safes and a crypto-powered deadbolt by Winkhaus. A better electronic system (that also employs crypto) is the CLIQ system by Mul-T-Lock.

Here we see a typical building's front door with a number of design flaws. This door is secured with magnetic locks. If the wires for these locks are susceptible to compromise, they can be made to fail almost instantly. Also, instead of a "push to exit" button, this door relies on a passive infrared sensor to detect the presence of an individual attempt to leave the facility. There is a significant gap in between the doors, however. A person outside can insert an object through this crack and, given the right amount of movement, quite easily trigger the sensor and unlock the door. Since the IR sensor is also in plain view through the windows of the front façade, it is conceivable that someone could direct a beam of light upon this sensor. A tactical flashlight or perhaps a laser pointer could, in theory, provide enough interference or heat to trip the sensor and possibly unlock the door.



With access control systems, the biggest problem pertains to backwards compatibility. An older system, using a technology called Wiegand, had weaknesses in its protocol. Many new systems that use high-tech elements like biometrics or smart cards still communicate with their back end using the Wiegand Electronic Protocol. Zac Franken has done a great deal of work exposing the flaws of these systems. His "Gecko" device is an ingenious attack that can compromise site security in a myriad of ways. Google his name for more of his materials, or even better… invite him to speak to you personally at your next security event.

7. Safe locks vary as widely as door locks

Safes are used by many people to protect specific objects, documents, and other valuables. Safes vary as much as any other type of lock in terms of good and bad designs. Fortunately, safes are very well studied and inspected by respected parties whose findings are reported publicly.

Nearly all mechanical safes operate with a system of wheels that spin. These wheels have notches, or "gates" cut into them. By operating the dial on the face of a safe, the wheels can be worked into alignment, allowing internal mechanisms to drop into these gates and operate a component called a "fence". The history of safe designs chronicles a number of variations on the "fence" mechanism, making for more secure model that will resist manipulation attacks.

All modern safes are inspected by the Underwriter's Laboratory and given a specific certification. Most safes are rated with a number following the letters "TL". This refers to the number of minutes that it would take a skilled person to open the safe using basic tools and manipulation techniques. Safes whose rating includes the letter string "TRTL" also provide resistance to cutting torches. Safes whose rating number is preceded by the letter string "TXTL" represent a safe's resistance to tactics, tools, torches, and *explosives*.

Perhaps the most amazing safe lock with which I am familiar is the X-07 and X-09 electronic dial by Kaba Mas Hamilton. This dial exhibits none of the weaknesses associated with mechanical imperfections and loose tolerances present in mechanical locks. They also operate in ways that will completely frustrate both human and robotic brute-force attacks and elegant manipulation techniques. Safes with Kaba Mas electronic locks and adequate steel wall construction are all but impregnable.

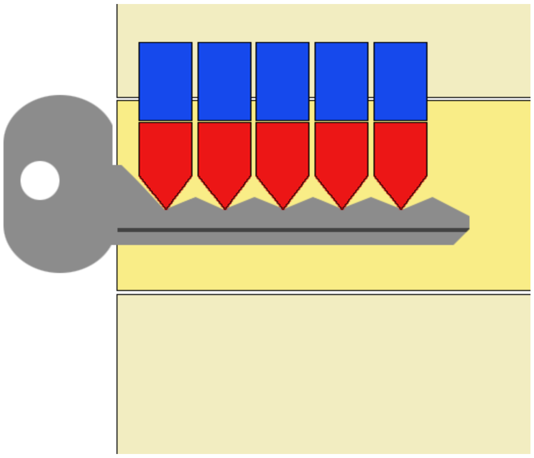
8. Bump keying is a real problem, but one with real solutions

The bump key attack is one of the biggest risks that locks face today. It is getting attention, however, and now both expensive and inexpensive locks are being designed to thwart this risk.

Bump keying requires little more than a specialized key. Skill and training are rather immaterial to successful execution of this attack. To understand what is happening within a lock during bumping, consider the movement of billiard balls...

If the white cue ball is shot towards the three and the two ball (which are touching) the three will likely remain stationary and all the kinetic energy will transfer straight through to the two ball, which will roll away.

This is how locksmith's pick guns operate. A spring-loaded blade is snapped against the bottom pins in a lock, with the resultant blast of energy traveling up through the pin stacks, making the top pins jump up while the bottom pins remain relatively stationary.



The bump key attack involves the insertion of a specially-cut key into the lock. If the head of this key is struck with appropriate force, the ridges of the key will all simultaneously smack against the bottom pins and the energy of this strike will cause the top pins to all jump upward. The resulting gap leaves the shear line without any binding force. If the plug is turned at the exact right moment, often the lock will open.

It should be noted that many mechanisms designed to make locks more secure have little to no effect against the bump attack. Specialized anti-pick pins, for example, will bump just as easily as traditional cylindrical pins.

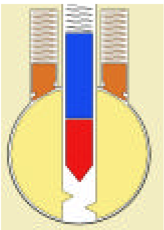
The Dutch chapter of The Open Organization of Lockpickers published a paper detailing the bump attack. It can be found here: http://www.toool.nl/bumping.pdf

Some of the advanced high-security mechanisms discussed above can significantly frustrate the bump key attack, even going so far as to prevent it entirely. Other very similar mechanisms have little to no effect. Sidebars (or, more accurately, the sidebar *locking mechanisms*) found in the Schlage Primus, Evva, and Scorpion locks cannot be bumped. The Primus uses a very unique set of rotating side pins, while the Evva and Scorpion models incorporate sliders. Newer Mul-T-Lock models featuring pins within pins as well as what is known as an "interactive pin" are often very difficult to bump.

However, the sidebar systems in Assa Twin locks and many Medeco locks are, at least in theory, susceptible to bumping. Typically, this cannot be done without some knowledge of the sidebar code. However, Assa (whose sidebar cuts are factory-milled and not cut by local locksmiths) divides most geographic regions into specific territories and distributes key blanks with a very limited set of sidebar codes to each territory. It is therefore possible to make an educated guess as to what sidebar could be in a door with an Assa Twin lock.

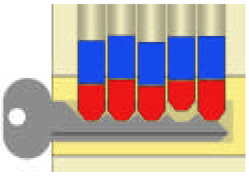
Also, both Assa and Medeco locks can "leak" information if installed in a mastered arrangement through out a facility. We will speak about mastering of multiple locks with various user permissions later, but for now understand that a typical user in a facility with a mastered configuration will likely bear a key that has the same sidebar codes to all other locks in the facility. Using this key as a starting point, it could be possible to create a bump key that opens many (if not all) of the doors in a specific office or campus.

Trap Pins



Some manufacturers are experimenting with ways to make basic pin tumbler locks resistant to bumping. One such technique involves the use of "trap pins" which will remain off to the side when a lock is operated with a key but which will fire downward and seize the lock in place if it is bumped (or picked) open.

If trap pins fire, however, there are no reliable and easy methods for restoring the lock to normal operation. It must be drilled out and replaced. A somewhat more elegant and less destructive method of preventing bumping is the "shallow drilling" method.

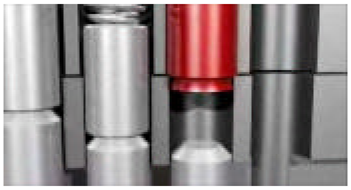


By drilling one of the pin chambers in a lock to less than full depth, the pin stack in that chamber will not hang low enough to contact a bump key inserted into the lock. Now, this will make the lock out of spec and prevent a full range of pin sizes from being loaded into that specific slot (and thus prevent the lock from being re-keyed to all possible combinations) but it will do a decent job of frustrating the bump attack.

While a shallow-drilled lock exhibits no easily discernable evidence of its unique construction, there are ways that a person could conceivably probe for and discover a shallow cylinder. What would the next course of action be, however? Are people going to carry a key ring with 50 or more bump keys? (And such an assortment would only be useful if just *one* pin chamber were drilled shallow.)

Top Gapping

American locks are likely going to see bump resistance via a technique known as top gapping. In this design, the top (driver) pins are fabricated in a way that they do not drop all the way down into the plug. This resulting gap between the bottom pins and the top pins makes the physics of bump keying fail.



Master Lock published extensively on this topic and is now producing locks that incorporate a special “bump stop” pin in at least one chamber. Such locks can be distinguished by the letter “N” being appended to their model number. Also, these products feature Master’s “bump stop” logo on the packaging. A number of years ago, Master Lock acquired American Lock, the makers of a number of heavy-duty padlocks and hasps. Having an American Lock with bump-prevention technology (which would be accompanying their usual array of anti-pick serrated pins) would make for very nice security in the face of “typical” low-tech attacks.

I also like to describe how the Kwikset company is developing locks that are specifically designed to resist the bump attack. When a company like this is taking notice of a security issue, you can be assured that the industry is finally waking up to the problem in a very real way.

Despite all these developments, there are not a wide range of locks that have these countermeasures at the present time. Trap pins are only present in the Mitche & Collin “Antiklop” (or “Anti-bump”) model. The Shallow drilling method is used by the manufacturer Carl Eduard Schulte on their VA5 and VB7 models. Master Lock / American Lock is offering the top-gapped “bump stop” design on some new models, and locksmiths could re-drill and re-pin some existing locks from this company. Kwikset’s new “smart series” not only includes some rudimentary biometric options but also specifically incorporates mechanisms that cannot be bumped.

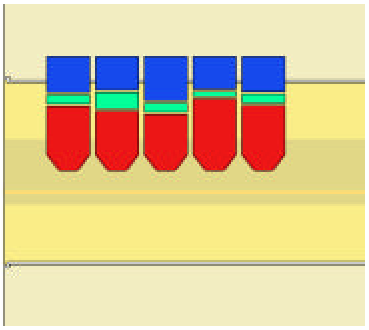
BUMP STOP

One other proposed way of addressing the problem of bumping is the use of specialized fluids or gels. Perhaps the best known product in this vein is *Pickbuster*, a thick grease developed by Mark Garratt which is distributed by the Almore company based in Pontypridd, Wales. It is squirted into locks and impedes normal pin movement, thus frustrating bumping. However, free and easy pin movement is the reason that *traditional* lubricants are used on locks. One typically does not *want* pins to stick or travel with difficulty. A product like Pickbuster can attact dirt and fouling and harm the lock in the long run. Perhaps on an internal door this product could have beneficial results, but I would not recommend it on an exterior door exposed to the elements. Ultimately, you must weigh the costs and benefits yourself.

9. Large facilities have their own unique concerns

Large facilities tend to have their own unique set of concerns and considerations. Often, multiple users are granted specific permissions to a variety of areas. Many times lock cores can be removed, facilitating management. Also, methods are often put in place to prevent unauthorized duplication of keys once they are issued.

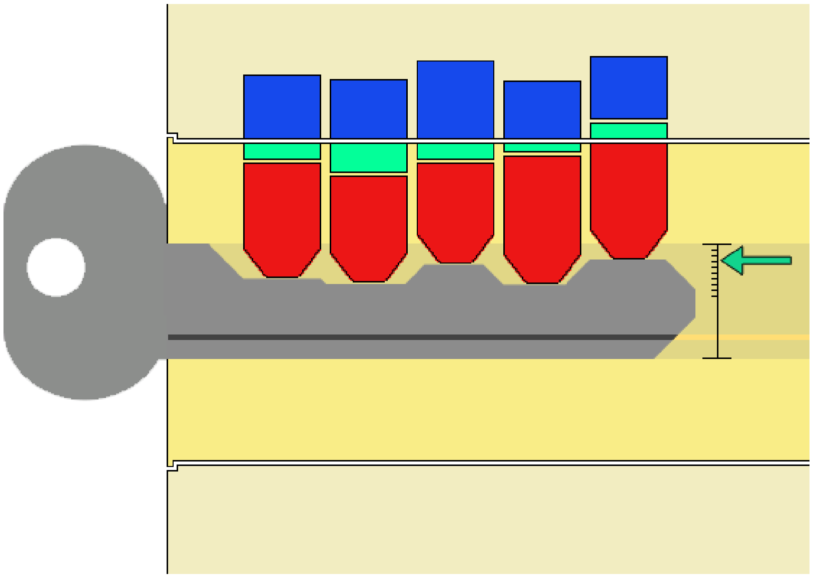
Master Keying



Mastering of locks (the issuance of multiple levels of permission) is achieved by the insertion of an additional pin (often called a “wafer” because of how thin it is) into the stacks. This allows for multiple levels of clearance at the shear line… and while that makes for more functionality, it also can make the lock easier to pick.

A mastered system will typically have the same set of bottom pins in all locks. Atop them will sit different sized wafers in every lock.

Typically, a user will be issued a key that only operates the door to their room or office. This key, called a "change key", will raise the pin stacks slightly, aligning them at the plug's edge to the higher shear line. There is also a "top master key" which will raise the pin stacks much higher, lifting the stacks to the second shear line... a line shared by all the locks.



There are a few possible security problems, however, with a mastered setup. In addition to the ease of picking that mastering sometimes creates, a crafty user could take their issued key and attempt to extrapolate out the mastered bitting. If someone has new keys made and in the process continually adjusts the bitting depth on just one chamber of the lock, eventually they may discover a *new* height for that pin stack at which the lock opens. The user has now discovered the "master cut depth" for that one chamber. They can repeat the process on the subsequent chambers.

Indeed, this is how "intermediate" master keys are created. Often someone who has been granted access to a particular floor or specific building will be issued a key where *some* (but not all) of the bitting cuts are at the master depth.

It is also important to consider that in a mastered system, *all* doors and locks will contain the master pins. If a single door is stolen or compromised in some way, it is possible for a nefarious party to plainly see the master bitting and create their own top master key.

Matt Blaze, a professor at the University of Pennsylvania, wrote a terrific paper discussing this phenomenon. It can be found here: http://www.crypto.com/papers/mk.pdf

Small Format Interchangeable Core

Some of the easiest methods for managing many locks in a large facility is the use of interchangeable cores. Companies like BEST, Yale, and some others have an interchangeable core design called "Small Format", or SFIC. In addition to being very difficult to pick, these locks can be installed and removed very easily with the use of a special control key.

SFIC locks have not just a plug that rotates, but also a control sleeve that can either expose or retract a retaining bar. These two components result in multiple, distinct shear lines. Picking attempts with traditional tools will almost always fail since tension will bind across both shear lines.

When a basic user's operating key is inserted into the lock, the control sleeve and lock body are locked together by the pins up in the top shear line. When the control key is in the lock, pins bind at the lower shear line, locking the control sleeve and the plug together into a single unit.

There does exist a specialized wrench tool, by the way, that can reach down with thin "fingers" and apply pressure exclusively on the control sleeve, potentially allowing someone to pick the stacks to a single shear line. Picking is still very difficult due to the tight tolerances to which BEST locks are manufactured and also the extreme designs of their keyways.

Matt Blaze experimented with ways to modify the control sleeve so that the specialized torsion wrench has nothing to grab on to. I believe that BEST now manufactures SFIC locks where the control sleeve is completely impervious to this style of attack.

Key Control

One of the primary considerations for people in charge of overseeing many users is the prevention of unauthorized copies of keys. Often, this is achieved with what are known as "restricted" keyways. This does not mean that they are legally designated as off-limits per se… but simply that a company has copyright control over their design and therefore can restrict the supply of key blanks. With no free supply of key blanks, there is little to no chance that a small hardware store or local key cutting shop can make a duplicate of a user's key.

There are other ways, however, that keys can be duplicated… even with restricted keyways. In Europe, there are *so many* various manufacturers and keyway designs that locksmiths often cannot keep adequate supplies of key blanks, So a machine was designed in Germany…. the E-Z Entrie machine. This device can, through a variety of means, duplicate the shape and pattern of many keyways. It can fabricate fresh blanks on the fly for numerous locks.

The best way to defeat even an E-Z Entrie machine if you are concerned about illicit duplication is to employ a system of keys that use side cuts or other customized milling that cannot easily be duplicated in a local shop. The Schlage Primus, slider systems, and rotating disk locks are all examples of such hardware.

10. Security in the Real World

Finally, it is important to bear in mind the fact that most physical security risks are not from elegant finesse tactics but rather from brute force attacks. Expensive, high-security locks are worthless if they are installed in cheap, weak doors. Solid-core doors, hung on heavy hinges with all hardware mounted using deep screws is essential. Also, deadbolts that contain round bars in their core will impede cutting.

Consider the risks that glass windows introduce. Security glass (with wire mesh running through it) or shatterproof film can be used to prevent window breakage. Motion-sensing lights and lots of open space in outdoor settings goes a long way toward preventing nefarious parties from creeping around and being where they do not belong, particularly at night.

I'm often asked what locks I prefer. There is no single, clear winner overall but this is a list of specific makes or models that impress me, along with the reasons why.

SCORPION

Scorpion locks employ a slider-based sidebar. They cannot be bumped and are monsters to pick.

EVVA

Evva locks, like Scorpions, have an advanced slider system.

SCHLAGE

While Schlage produces a number of low of low-grade "hardware store" products, their high-security Primus series incorporates a very unique sidebar system that cannot be bumped. Picking a Schlage Primus may be possible in theory, but I couldn't image it being done by anyone but the *most* skilled individual under very controlled conditions.

BEST

BEST is one of the foremost manufacturers of Small Format Interchangeable Core locks. They utilize high quality parts and machine to tight tolerances. Additionally, they produce a number of various keyways, all of which are copyrighted for key restriction purposes.

ABUS

The flagship line of the Abloy company's heavy-duty hardware, Abus locks are built to resist loads of brute force as well as finesse attacks.

ABLOY

Any current locks incorporating the rotating disk system are all but impregnable. The Protec series by Abloy is the cream of the crop and suitable for use securing the most sensitive environments.

AMERICAN

The American Lock company makes something known as a "shackle-less" padlock. It is their model 2000 lock, solid steel, and with the appearance of a hockey puck. Coupled with the heavy-duty steel hasp that is often seen on store fronts and contractor vans in every big city, the American 2000 is one of the locks most suited to resist brute physical force. These locks almost always feature serrated pins, and with the addition of Master Lock's new Bump Stop protection, they are all but impregnable… particularly to the types of attacks you see at the unsophisticated "street crime" level.

TrioVing

I love every visit I make to Norway. And as long as folks there keep inviting me back to give more talks, I'll happily pick up one or two TrioVing padlocks each time. Their double-mushroom spool pins make for terrific security in an inexpensive package.

KABA MAS

If you have a safe that you want to protect from here to eternity, the electronic X-07 and X-09 dials by Kaba Mas are they way to go. There are *no* known workarounds, bypasses, or attacks that can compromise these beauties.

SG SARGENT AND GREENLEAF

One of the exclusive distributors of locks to the Department of Defense, Sargent & Greenleaf makes a number of outstanding locks. While not always available retail, checking eBay or military surplus establishments can often lead you to discover 830-series padlocks (used on munitions stores and armories), 8077 or 8088 combination locks (used on D.O.D. file cabinets), and safe deposit box locks (which incorporate old "lever lock" style technology in new and highly secure ways.)