Contextual Physical Security

A Practical Attack Methodology

Eric Van Albert, A Vicki Crosson, Zachary Banks

May 19, 2013

Presented here is a collection of frequently overlooked vulnerabilities in mechanical key based systems, which we synthesize into an attack methodology. First, we exploit unlocked or poorly secured doors to gain knowledge about the system. We remove locks from these doors and take them off-site for decoding. Then, we analyze the information gathered to produce the master key(s) to the building.

Our attack minimizes the need to actively bypass security measures on-site. We avoid picking, bumping, and impressioning when possible, instead investigating latch manipulation techniques. Although we use Schlage, Best, and Yale pin-tumbler locks in our examples, our attack is generalizable, even to high security locks. We conclude with a hypothetical case study where an attacker uses our methodology to to completely compromise two separate lock systems in one week, leaving no evidence

1 Introduction

This attack is designed for use on a building secured by traditional mechanical locks, which prevent doors from opening. Rather than considering how to open just one door, we make a key to open all of the doors on a given system. Our attack will leave no trace.

The exact vulnerability we are attacking is the existence of a master key in an imperfect system. Anybody familiar with computer security knows that passwords should not be stored in plain text and that the ability to execute code as root should be carefully guarded. Traditional mechanical security systems suffer from analogous vulnerabilities: every lock which can be operated by the master key contains the master bitting. Therefore, if a single lock is left unsecured, it can be reveal its bitting, from which the master bitting can be deduced.

Here we also provide practical considerations for how such an attack might be executed, as well as a novel bypass attack with regards to latch manipulation.

We assume the point of view of an attacker, in order to uncover more vulnerabilities. It is the small details in this attack that make it so powerful, and these are exactly the details which would be easily overlooked by a building security manager. We assemble minor vulnerabilities into a coherent system of attack constituting a major threat to security. This is a recurring theme: rather than attacking just the latch or just the lock, we will attack the entire system as a whole. We will walk into a building knowing nothing, and walk out with the master key(s).

2 Reconnaissance

The first part of any attack is to understand what you are attacking. Where possible, examine the face of various locks for useful information. Determine what brand and model the locks are to learn important details about the type of keys they take, as well as any high-security features. Things to consider when choosing the key blanks include the shape of the keyway, and whether it is tip-stop or shoulder-stop. Both of these are easily seen by a quick glance at the lock's face.

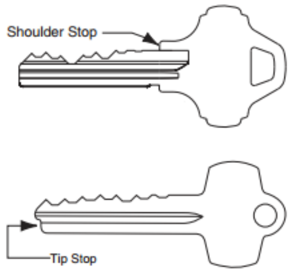


Figure 2.1: Shoulder-stop versus tip-stop keys[1]

This is made easier in that most manufacturers use a small set of stock keyways, with custom keyways available on request. It may help to photograph the keyway and compare it to drawings in the technical manuals. Many manufacturers also have an "all-section" key which fits many of their keyways. Having common all-section keys with you will be useful in choosing a blank that fits.

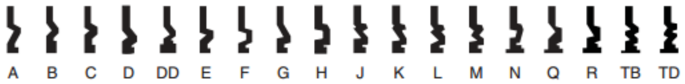


Figure 2.2: Set of SFIC keyways shared across multiple manufacturers [1]

If a system uses a custom keyway, all is not lost. Generally, custom keyways are very similar to stock keyways, so a stock key (especially an all-section key) will fit into them with little to no modification. Note that a bench grinder can often be used to thin down keys until they fit.

Lastly, by looking at multiple doors, you can determine whether multiple keyways or key systems are in being used. Large institutions may use multiple brands, models, and keyways. Higher security locks are generally used on higher value assets. There are cross-keying opportunities across keyways, and occasionally across models, but never across brands.

When examining locks, note any markings you may see on or around them. Sometimes, designations are even printed or handwritten on locks, which can help you to find patterns.

Make your best guess as to how the systems are organized and what keys exist. For example, many institutions have different systems for external and internal doors. They may also segregate facilities doors (janitorial closets, mechanical rooms, and roofs) from offices or other rooms. You will have to do some experimentation, as your first key may not open the set of doors that you expected. Start with a goal in mind, and design your attack to begin at a related point in the system.

3 Opening the first door

The first step of this attack involves gaining access to an open door with a lock in it. The door does not need to be particularly "interesting", it just has to be on the same lock system as an interesting door. For this reason, you should choose a door that's not frequented so as to minimize awkward questions about what you are doing. The goal is to extract the lock for decoding.

If a suitable door is found left open or unlocked, the steps involving opening that door should be skipped. Before you get going, look at multiple doors that could be relevant; it is highly unlikely that every door in a given system is closed and locked. However, we will still entertain the possibility that every door is closed and locked.

At that point, one must be opened. The door does not necessarily have to be unlocked–just ajar. Any method can be used to open the door, but we'll focus here on latch manipulation because it is fast, surreptitious, and applicable to many doors. Opening a door by picking the lock is rarely necessary, and increases risk because it is so slow. Keep in mind that any door may be used, so choosing a poorly installed door, or one with a broken latch is recommended.

3.1 Latch Manipulation

Spring latches are particularly vulnerable to manipulation. In a spring latch, the latch bolt is held extended by a spring and will retract due to end pressure. The sloped face of the latch transforms lateral pressure into end pressure. This causes the latch to retract momentarily as the door swings shut.

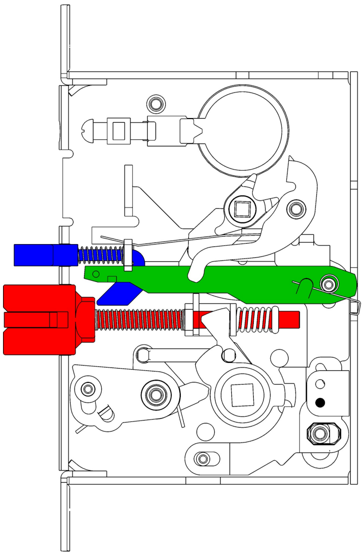


Figure 3.1: Diagram of a Spring Latch Mechanism.
Red: latch bolt. Green: auxiliary stop. Blue: auxiliary latch bolt. [3]

When the door is closed, a plastic card or a slide (a stiff L-shaped device) can be used to apply lateral pressure (and therefore end pressure) to the latch. Flexible cards are used if the door opens away from you, as they must maneuver around the door jamb. Slides are used when the door opens towards you. Because you must push the latch from behind, they must be stiff. Thin sheet metal is recommended. As noted, both cards and slides are operate along the sloped edge, depressing the latch.

For doors that open towards you, a knife may be used to "walk" the latch over. Pulling on the door causes friction between the latch and the strike plate, which can be used to capture progress between short sideways motions.

Deadbolts are impervious to this attack, since they do not retract under end pressure. This is what it means to be "dead".

A dead latch combines both of these ideas. When the door is open, it behaves as a spring latch. When the door is closed, the latch bolt becomes dead. An auxiliary bolt is used to tell whether the door is open or closed. When the door is open, the auxiliary bolt is extended. When the door is closed, the auxiliary bolt is depressed, deadlocking the latch in place.

There are two types of deadlatch designs that are used commonly. One has a large auxiliary bolt significantly above or below the latch bolt. This interfaces with a different part of the strike plate than the latch bolt. The other type has the auxiliary bolt right next to the latch bolt. In this configuration it is frequently called the deadlocking "plunger". It is frequently very small–either a sheath or a small semicircle.

It's worth noting that most industrial latch bolts have an "anti-friction tongue" in the center of the latch bolt. The purpose of this floating piece is to act like a lever and reduce friction on the latch as the door closes. It is unrelated to the auxiliary bolt.

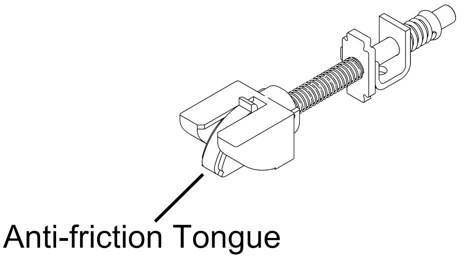


Figure 3.2: Spring Latch with anti-friction tongue [3]

Auxiliary bolts of the first kind are fairly robust to door misinstallation. As long as the crack between the door and the jamb is less than about 1/2", the latch will function properly. Additionally, they are extremely insensitive to how far the door swings shut (how "tightly" it closes) .

3.2 Common Deadlatch Failure Modes

Deadlocking plungers or sheaths are slightly more sensitive to crack width (5/16"), but are much more sensitive to how far the door swings shut. A misalignment of just 3/16" can allow the plunger to extend into the mortise, rendering it useless. This amount of slop can easily be seen in doors with weatherproofing strips.

There are three ways that the deadlocking mechanism on a door can malfunction. When this happens, it becomes a spring latch and the door is vulnerable to a card / slide, which makes the door trivial to open in a few seconds without looking suspicious.

First, the auxiliary bolt may extend into the mortise due to misalignment or improper installation of the strike plate. Occasionally, holes are cut into the strike plate to allow the auxiliary bolt to extend into it by people who don't understand its function. Sometimes applying force to the door (towards you if you are carding, away from you if you are sliding) can cause the auxiliary bolt to fall into the mortise.

Second, the internal deadlocking mechanism may be broken, despite the auxiliary bolt being retracted. This mechanism is quite fragile; we will examine it more closely soon.

Third, the latch bolt may not be fully extended. The deadlocking mechanism will not function if the latch bolt never extends fully. The anti-friction tongue allows some doors to appear latched, whilst only a fraction of the latch bolt extends into the mortise. Since the latch bolt has never fully extended, the deadlocking mechanism cannot engage.

4 Sabotaging a door

At some point during the attack, it may become necessary to covertly sabotage a door to ensure future access. This can be done by disabling the deadlocking mechanism in a latch, allowing the door to be opened via a card or slide. The door will still appear to function normally.

Many latches have a similar internal mechanism. This mechanism contains a lever held up by the auxiliary latch (the "auxiliary stop"). When the auxiliary latch is depressed, the lever lowers and prevents the latch bolt from retracting, making the latch "dead." However, we show that it is possible to disable this mechanism in both open and closed doors, enabling carding and sliding attacks.

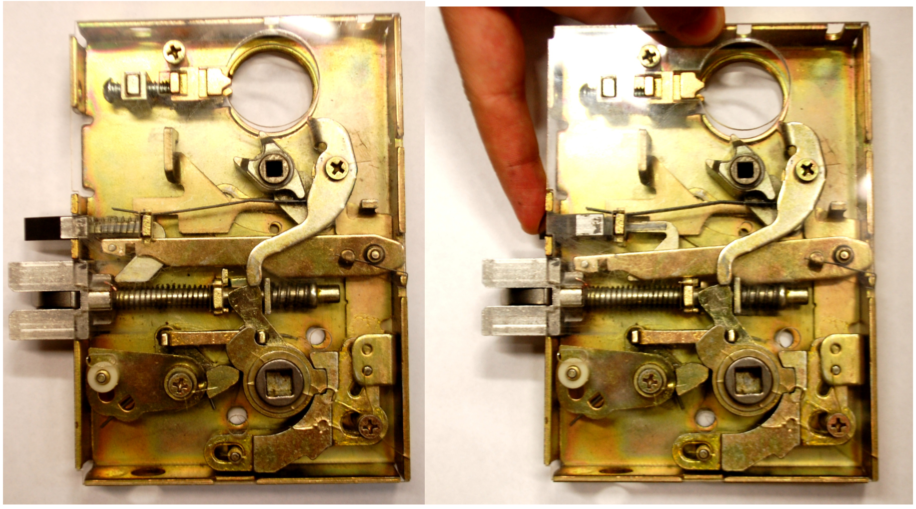


Figure 4.1: A working deadlatch: Pressing on the auxiliary bolt causes the auxiliary stop to fall, preventing the latch bolt from retracting. [4]

4.1 Covertly Disabling the Deadlocking mechanism

Across several brands of latch, the deadlocking mechanism is incredibly fragile. On an open door with this lock, you can insert a small magnet (e.g. a neodymium cube) into the lock casing through the opening for either of the bolts. The magnet will fix the auxiliary stop in place, which prevents the deadlocking mechanism from functioning. This makes the door trivial to open at a future time by using a card or slide.

A simple inspection of the deadlatch mechanism would reveal that it is not working properly, but such a security check is unlikely to be performed regularly.

This attack is useful if a door is open sometimes, such as during business hours. It allows security to be subverted beforehand, allowing you to come back to discreetly open the door later.

This attack does leave evidence: the magnet remaining in the latch will be obvious upon disassembly. However, removing the magnet when done will leave no trace of this attack. This is possible without disassembly, by means of picks and pliers.

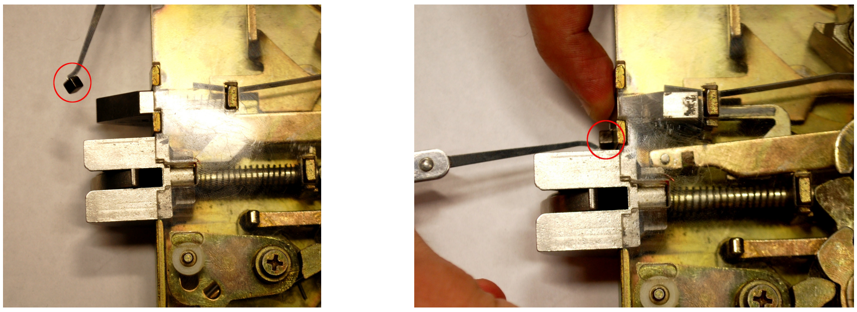


Figure 4.2: Here a magnet is prepared for insertion. In the right image, the auxiliary latch is depressed to create space for the magnet, and the auxiliary stop has fallen to block the latch bolt.[4]

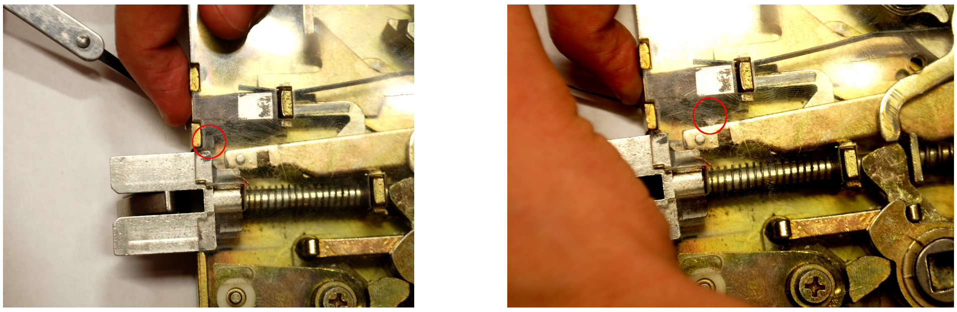


Figure 4.3: The magnet is worked into the latch until it is behind the auxiliary stop. This attack is not very sensitive to the magnet's position; it can be anywhere in the vicinity of the stop.[4]

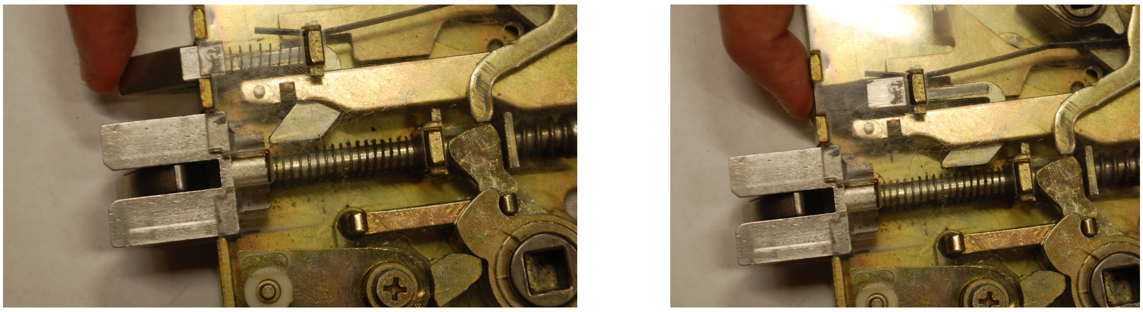


Figure 4.4: The auxiliary latch is released, and the auxiliary stop becomes fixed in the "up" position. [4]

4.2 Defeating the Deadlocking Mechanism in a Closed Door

If the attacker encounters a closed door with a working deadlatch, there are some cases in which it is possible to defeat it.

Another attack, primarily for double doors and doors that open outward, relies on their visible latch bolt and large gap. This surreptitious attack allows an otherwise working door to be opened with simple tools.

By inserting a small, stiff shim through the opening for the auxiliary latch bolt, it is possible to raise the auxiliary stop and disengage it from the latch bolt. Once it is out of the way, the latch bolt can move freely, and can be retracted with a knife to open the door. This attack takes a few seconds longer and is more elaborate than simply carding or sliding a door, but is still possible to do discreetly.

After performing this attack, the deadlocking mechanism on the door can then be semi-permanently disabled using the previous attack if needed.

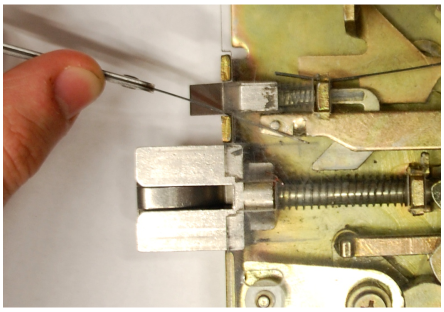


Figure 4.5: The auxiliary stop is lifted with a hook pick inserted through the deadlatch. This is demonstrated on an isolated latch with a clear front plate, but it has been realized on a closed, locked, and otherwise working door. [4]

5 Information gathering

5.1 Lock Removal

Once a door is open, the next step is to remove the lock for decoding. On most open doors it is extremely easy to remove the lock cylinder, even while the door is still locked.

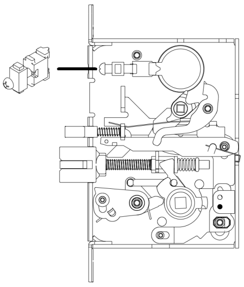


Figure 5.1: The L-series latch cylinder retention mechanism[3]

Examine the faceplate on the side of the door. If it has a screw which aligns radially with the mortise cylinder of the lock, there is a good chance that screw holds in the cylinder.

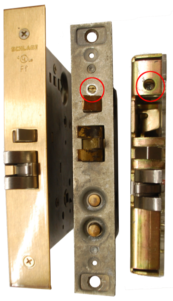


Figure 5.2: Left to right: Latch with faceplate covering the retaining screw, latch with exposed retaining screw, and latch with exposed retaining screw after the faceplate is removed. [4]

If such a screw isn't visible, it is probably necessary to remove the faceplate to access it. The faceplate is generally held on with two screws that are only 1/4" long. Once the faceplate is removed, the screw holding in the cylinder should be exposed. It may be slightly recessed.

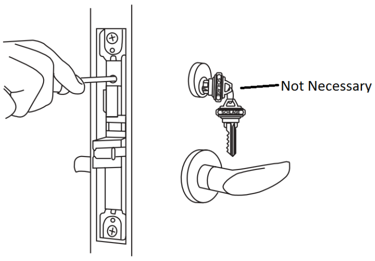


Figure 5.3: [3]

This retaining screw only needs to be moved about 1/8”, as it engages a slight detent in the mortise cylinder. Once the cylinder is free, it can be unscrewed from the lock. Inserting a screwdriver into the keyway facilitates this process, but a blank key will leave less damage to the lock face.

Once removed, the lock can be taken off-site where it can be decoded.

If necessary, a placeholder mortise cylinder can be installed to avoid raising suspicion while the lock is being decoded. It does not necessarily need to open with the right key, or even fit the right key, as long as the door is left open or unlocked. In these circumstances, it is unlikely that anybody will try the key. This makes it advantageous to choose a door which is usually unlocked. If the door is infrequently used and out of sight, a placeholder may not be necessary at all.

This entire process can be executed in just 1-2 minutes. It looks incredibly sketchy, but appropriate deliberation in choosing a door can minimize risk.

The best case scenario is when a mortise cylinder is not fully tightened in the first place. No disassembly will have to be done, the cylinder will simply have to be unscrewed or pulled out. It is very easy to spot these cylinders – look for ones that are not perfectly straight. Try to twist them. If they spin, they can be removed, even from a closed and locked door. They represent the greatest security risk.

Figure 5.4: A sideways lock is a removable lock. [4]

5.2 Decoding

Once a lock has been removed and relocated, it must be decoded. Through prior research, the model, warding, pin spacing, and possible cut depths should already be known. Optimally, you would be ready with a blank key at this point. We are at the point where only the bitting is unknown.

First we will consider mortise cylinders with the plug directly integrated. Interchangeable core mortise cylinders operate slightly differently, and will be discussed later.

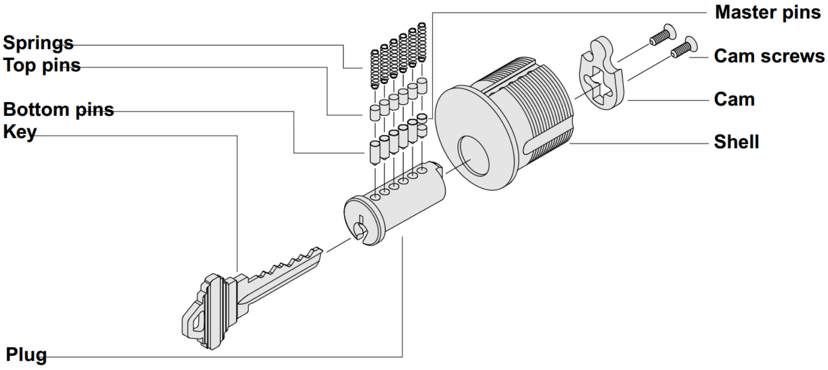


Figure 5.5: Exploded view of a standard mortise cylinder[3]

The utmost care must be taken with the decoding procedure. If any pins are lost or scrambled, you will be unable to reassemble the lock into its previous working state. This means that the correct keys will no longer operate it, which will raise a lot of suspicion.

The first step of decoding is to remove all hardware around the plug that can be removed, to expose the shear line in the back of the plug. The lock now must be picked. This process can be made trivial through the use of very thin shim stock which is placed at the shear line and is used to capture pins when they are set. Once the lock is picked, the cylinder can be carefully removed out the front of the lock, making sure to not lose track of any pins along the way. A plug follower is recommended but not strictly necessary.

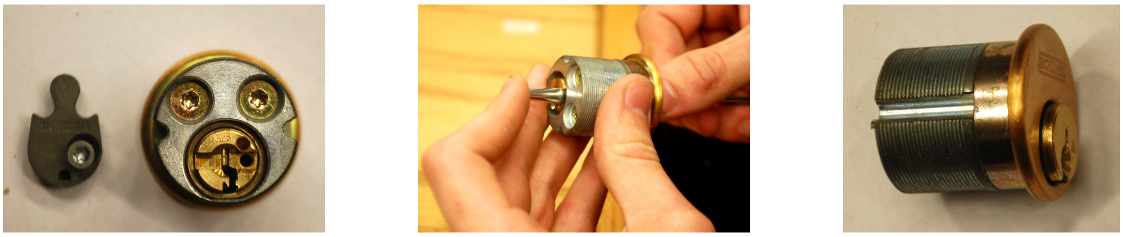


Figure 5.6: Lock is disassembled and picked using a shim.[4]

It is vital to not allow the driver pins to fall back into place as the cylinder is extracted. This is accomplished by using a shim or by extracting the plug at an angle so that the holes never align. If the driver pins are allowed to reset, they may carry master wafers from one chamber to another. It will be impossible to tell with certainty which chamber those master wafers originated from.

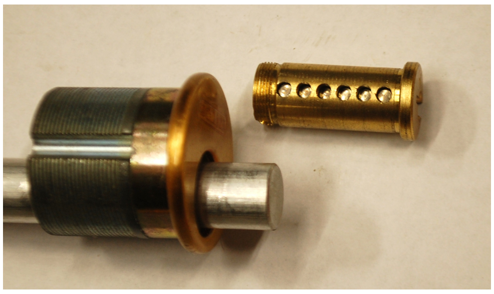


Figure 5.7: The plug is extracted using a piece of aluminum as a plug follower.[4]

Once the plug has been removed and all pins exposed, they should be carefully removed and measured. Calipers or a micrometer are recommended. All pins in each pin stack should be measured except the driver pin. It is rare for a lock to have multiple master wafers, but it may happen. Cuts that are impossibly low should be discarded, as occasionally multiple master wafers are used as a driver pin when a properly sized balanced driver is not available.

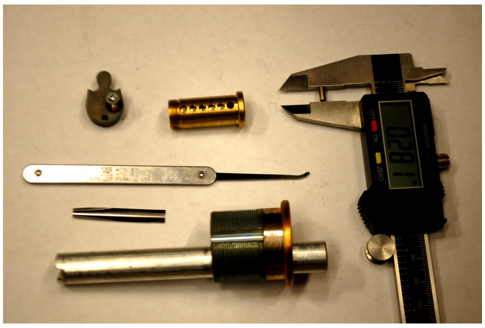


Figure 5.8: The pins are measured using calipers. Shown here is the complete set of tools necessary for decoding a lock. [4]

If the lock is not mastered, you will get one possible height for each chamber. If the lock is mastered, you will get one or two possible heights for each chamber. All of this information should be recorded, and the lock re-assembled exactly how it was before. You now have enough information to manufacture a key for this lock. The cylinder should be re-installed into the door in the same manner it was removed.

5.3 Small Format Interchangeable Core Locks

SFIC locks pose an interesting problem, which is that the cores usually cannot be removed for decoding without them first being picked to the control line. However, once the core is free, it can be decoded while locked.

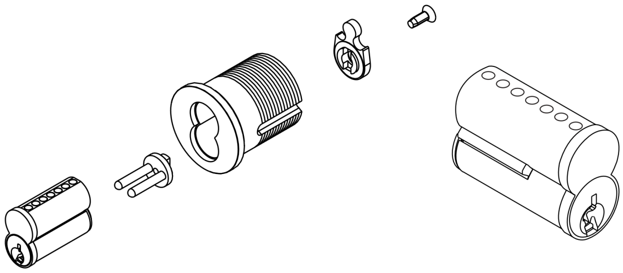


Figure 5.9: Exploded view: SFIC lock[3]

When picking SFIC locks traditionally, it is nearly impossible to choose which shear line the pins set to. For a given lock, it will always tend to pick to the same shear line, whether that be control or regular. This can be altered by applying tension to just one of the shear lines. A simple example of this is picking a bare SFIC without a tension wrench, using your thumb to press on the control sheath. This will allow you to pick the control line. Extrapolating from this, if tension can be applied to the control sheath in whatever housing the lock is in, it will pick to the control line and can then be removed. There also exist special tension tools which engage the control sheath. [5]

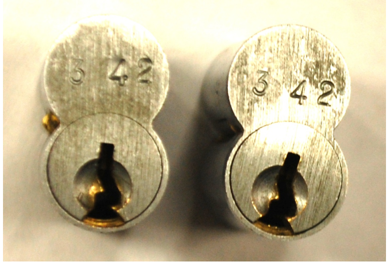


Figure 5.10: The core on the right has been picked to control.[4]

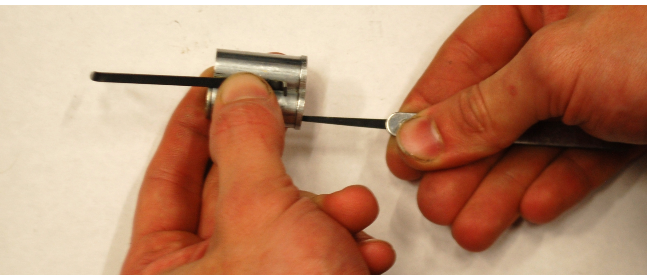


Figure 5.11: Picking a SFIC to control by using pressure applied to the control sheath. This attack is shown here on a bare core for demonstration purposes only, as a core in this state can be decoded without first needing to be picked.[4]

If the control sheath is not exposed, and the lock does not tend to pick to the control line, a semi-destructive method may be employed. This method is semi-destructive in that it does not damage any irreplaceable parts. Using a rotary tool, grinder, drill, or milling machine, parts of the mortise cylinder are slowly removed until the control sheath is exposed. Then, pressure can be applied to it in order to pick the control line. Care should be taken to not damage any part of the core during this process. The mortise cylinder will need to be replaced, but these are readily available stock parts.

If none of the above methods are acceptable, it may be necessary to find a different lock to decode. When looking for another door, look for cores that are missing their face plate (the thin piece of metal above the keyway). This is rare, but these cores can be picked trivially using a shim at the exposed control line.

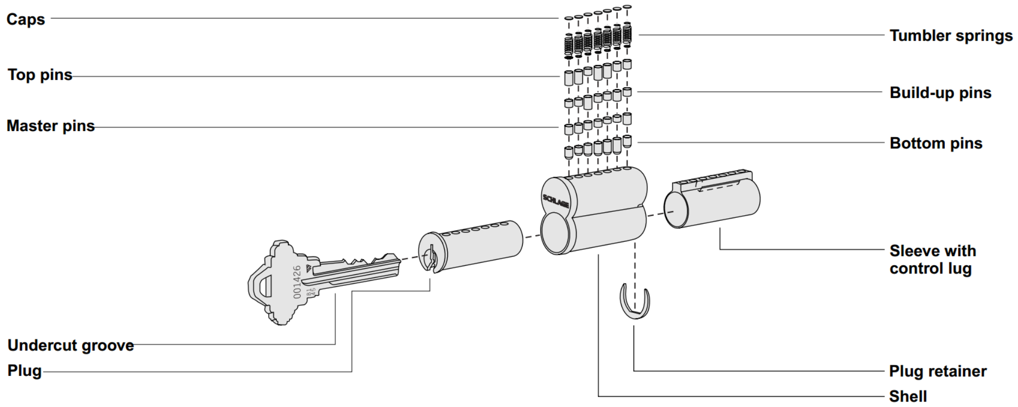


Figure 5.12: Exploded view: SFIC [3]

Once the SFIC is free, a very small punch can be used to remove the chamber plugs, springs and pin stacks. It is now important to keep track of the order in which the pins come out of the stack, as there can be as many as four shear lines. Typically, however, there are only three, and some leeway is gained by the fact that each pin stack must sum to the same height. Pins and springs can be lifted out through the top of the lock by inserting a punch or paper clip through the holes in the bottom of it.

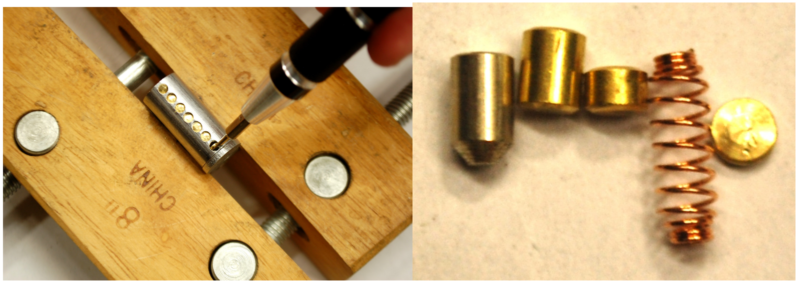


Figure 5.13: Using a punch to remove the caps on an SFIC, and the resultant pin stack (key pin, control pin, driver pin, spring, cap) [4]

5.4 Large Format Interchangeable Core Locks

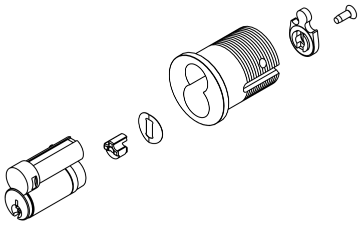


Figure 5.14: Exploded view: LFIC core and housing [3]

LFIC cores also must generally be removed from their housing to be decoded. However, they do not have a separate bitting for the control key. Instead, the control key is longer and actuates a pin near the back of the lock. Under normal operation, this pin shears just like the others, without needing to be lifted at all. If lifted, it binds and engages the control ring, which retracts a retaining pin.

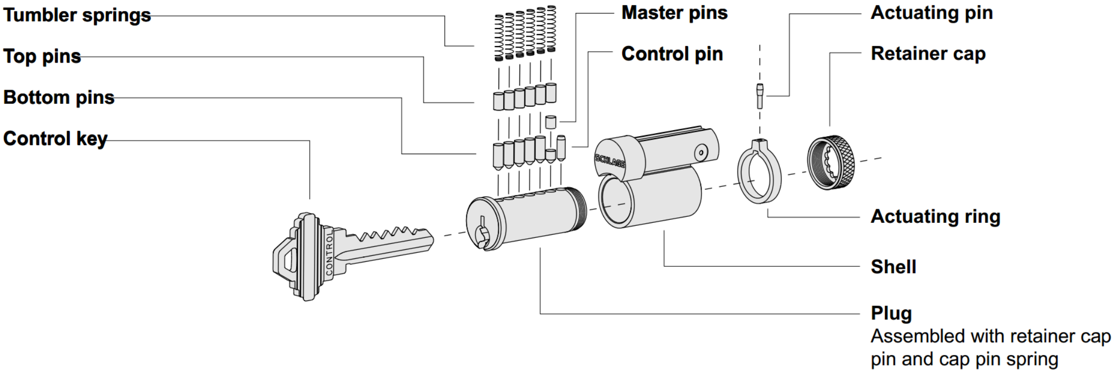


Figure 5.15: Exploded view: LFIC core [3]

There are three ways of removing LFIC cores from their housings. First, a picking attack is possible. The lock is picked traditionally, and rotated 180 degrees. The bottom of the keyway is open, and in this position it exposes the bottom side of the sheared pins. On certain locks, this may cause small master wafers to be ejected from the lock, so special care should be taken to hold them in. A pick is then inserted far back into the lock, and the control pin is pressed upwards. This engages the control ring, and the lock must then be rotated another few degrees to retract the retaining pin. The pick must be very small at the end, and a stiff paperclip may serve as a better tool. [8]

The second way uses a “coring shim” to depress the control pin semi-permanently. A shim is cut from metal stock such that when it is inserted far back into the keyway, it raises the control pin and becomes wedged in place. The lock can then be picked normally, and when it turns, the retaining pin will retract. Care must be taken to produce a working control shim, as it may render the lock inoperable if improperly sized. It is recommended to try this on a bare core to ensure that the shim works properly. This method is recommended if the lock cannot be turned 180 degrees (e.g. a padlock) or if there exists a working key for the lock. However, if there exists a working key, a more reliable method would be to duplicate this key onto a control blank which actuates the back pin without the need for a coring shim.

The third method is semi-destructive, just as with SFIC locks. On most LFIC mortise cylinders, the retaining pin engages a cavity on the inside of the cylinder. This machining operation is typically accomplished by drilling a blind hole starting all the way on the other side of the lock. By using this hole as a guide, one can drill out the core’s retaining mechanism. The core can then be shaken out of the housing. This does not damage the mortise cylinder, the plug, or the pins. It only damages the sheath and retaining hardware, which are inexpensive stock parts and can be replaced easily. This method is recommended if there are replacement parts on hand and there is time pressure.

Once the LFIC core is removed, it can be disassembled in the same way as a standard mortise cylinder.

5.5 Padlocks

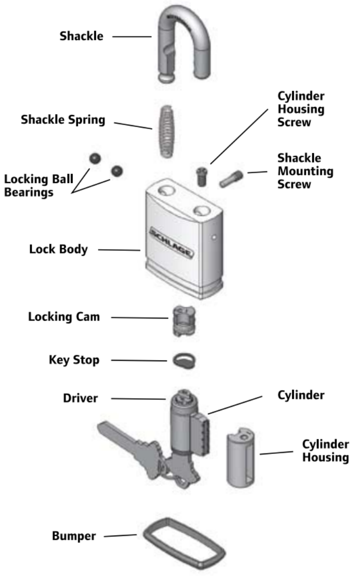


Figure 5.16: Exploded view: Padlock [5]

Often, padlocks are on a different system, as unmastered Master locks are incredibly cheap and are not opened frequently. However, if you have reason to believe that a padlock is part of the system under attack, then it will serve just as well in terms of information gathering.

The best way to obtain a padlock is to find one that has been left open and borrow it. This takes no time and is unlikely to be noticed, even in crowded areas. Padlocks left unlocked are an enormous security risk for this reason. If no suitable open padlock can be found, we can remove one by picking it open. This takes a potentially indeterminate amount of time and is therefore not recommended. One final method of obtaining a padlock is by removing it by force, using bolt cutters or an angle grinder. This should only be done if replacement shackles are available for the lock so that it can be returned in its original condition. It is not recommended.

Figure 5.17: Replacement shackles are often readily available. [5]

Sometimes padlocks contain interchangeable core locks. The core can be removed through methods described above. If they do not have an interchangeable core, they may be impossible to decode except destructively. If this is unacceptable, the lock should be returned and a different lock obtained.

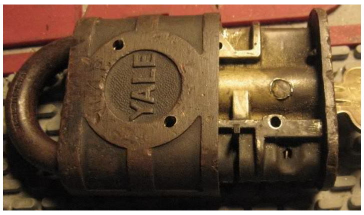


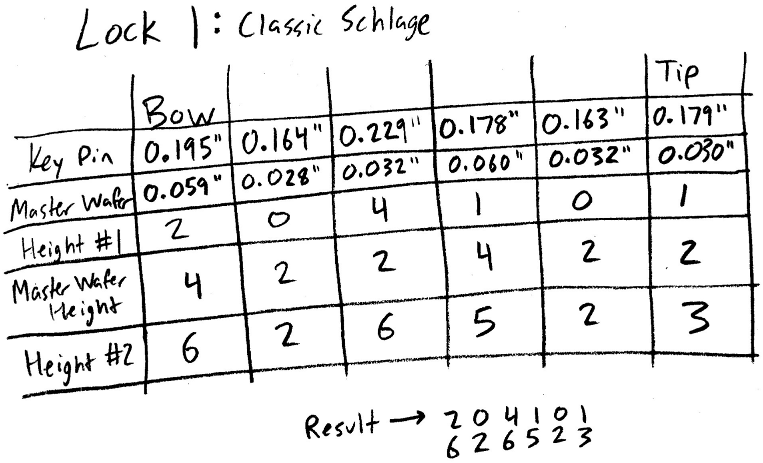
Figure 5.18: A Yale padlocked, partially disassembled by drilling out retaining pins [6]

6 Information reduction

Once one lock is decoded, a lot can be learned about the system. However, most of the time, two locks will need to be decoded before the master bitting becomes apparent.

If a lock is unmastered, a key should be manufactured with that bitting and tried liberally. It is possible that the entire system is unmastered and that a single key opens every lock. It is also possible that the lock chosen was singly-keyed for added security. If this is the case, a different lock must be examined.

If the lock is mastered, more information gathering must be done. If a lock with six chambers has all six of them mastered, then there are $2^6 = 64$ possible keys that open that lock. One of them is the change key, one is the master key, and some may be sub-master keys. One cannot tell simply from the pin sizes which is which.



Lock 1: Classic Schlage

	Bow					Tip
Key Pin	0.195"	0.164"	0.229"	0.178"	0.163"	0.179"
Master Wafer	0.059"	0.028"	0.032"	0.060"	0.032"	0.030"
Height #1	2	0	4	1	0	1
Master Wafer Height	4	2	2	4	2	2
Height #2	6	2	6	5	2	3

Result → 2 0 4 1 0 1
6 2 6 5 2 3

Figure 6.1: Process for recording measurements and decoding a lock[4]

It is possible but somewhat difficult to try 64 different keys on various locks until you can figure out which one is the master. On the other hand, decoding a second lock will be enlightening. It is best to make this second lock as different as possible from the first (as long as it is on the same system). This will yield another 64 possible keys that open it. However, with any luck, only one or two of these keys will open both locks. If only one key opens both, then that key is the master key. If two keys open both, then both should be cut and they should be tried in various locks to determine which is the true master. Sometimes this is quite ambiguous, as one may be a high-level sub-master. Choosing disparate locks decreases the probability of there being shared sub-master. It is rarely necessary to decode a third lock.

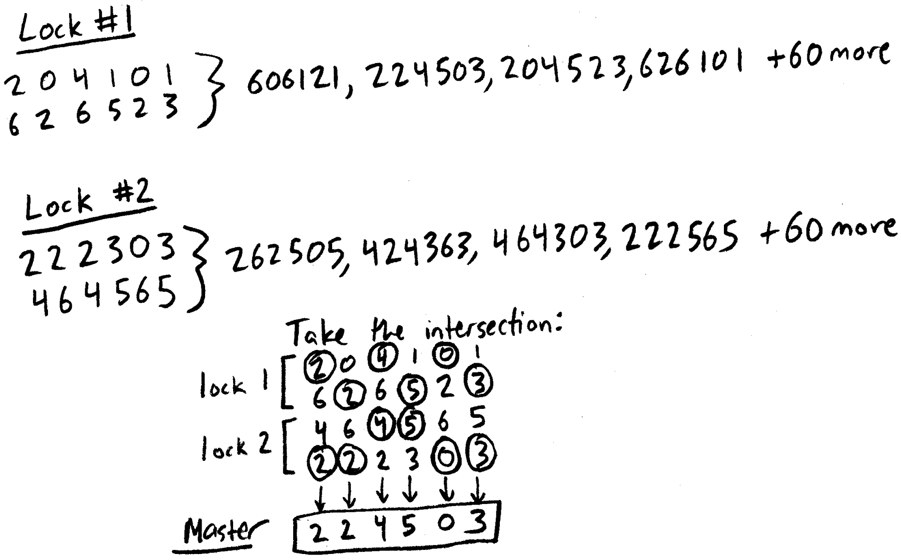


Figure 6.2: The intersection of the bittings of two locks yields a set of keys that will open both. If there is only one such key, then it is the master. [6]

6.1 Shortcuts

There exist a few shortcuts in this process that may only require one lock to be decoded. For example, if a change key is known, and the lock for that change key is decoded, a lot of the entropy is removed from the master bitting. In some systems, the change key and the master key share no cuts (sub-masters share cuts). In this case, the master key is fully determined, as it is the set of cuts that are not the change key. Some systems share one or two pins between the change key and the master key. If these chambers are not mastered, then the master key is still fully determined. If they are mastered, this technique may narrow down the keyspace slightly (e.g. to 6 possible master keys).

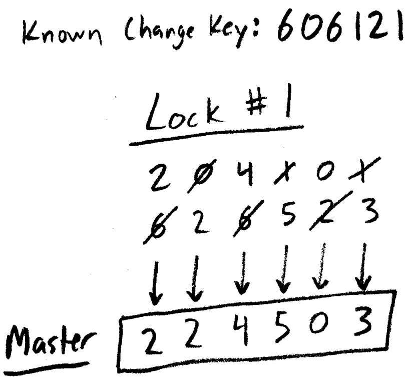


Figure 6.3: Decoding a lock by eliminating cuts based on a known change key.[6]

Another shortcut involves using impressioning to deduce the master key without disassembling another lock. One key is cut with the highest possible cuts for each stack in the decoded lock. One round of impressioning is performed in a different lock. Those stacks that leave marks are filed down to the lower of the two cuts in that stack. This process is repeated until the key works, just as in regular impressioning. The difference is that this attack requires significantly fewer impressioning cycles, since the bitting is predetermined down to two heights for each space. If marks are left on the higher cut, then it must be the lower cut. It requires at most one cycle for each pin, and likely will succeed in fewer. This process requires the attacker be proficient at impressioning, and so for less skilled attackers, decoding a second lock is probably faster and more reliable.

SFIC locks present a unique vulnerability. While it is slightly harder to decode the first lock, decoding subsequent locks becomes trivial. This is because the control line is rarely mastered. Therefore, decoding one core determines the control key. A control key can then be cut, which not only allows any door to be opened (through removal of the core and use of a screwdriver to actuate the lock) but greatly facilitates decoding. In a few seconds, a core can be removed and swapped out for a placeholder. This is much more discreet than removing a mortise cylinder. Once a second core is decoded, the master key can be cut, which will allow for doors to be opened without needing to remove the core.

7 Key Manufacturing

There are a few methods available for the manufacture of keys. Almost all of them assume access to fitting key blanks, but it is possible to make your own blank.

7.1 Cutting Keys

The simplest way to create a key yourself is by hand-filing. A high-quality file is recommended. If a square file is used, care must be taken to make smooth ramps between valleys. Any sharp edges will cause the key to get stuck, hopefully on the way in, but potentially on the way out. This may damage the lock, and the intent would be apparent to the locksmith who has to come and extract it. For that reason, a round file is recommended, though you must be careful to file straight down at each pin location and not at an angle, else the pin will not fall at the lowest point of the circle. You may also have trouble getting keys that have been cut with a circular file duplicated at hardware stores.

A rotary tool may appear to be an attractive way to cut keys, and it does work, but not nearly as well as a hand file. It takes off too much material too irregularly, exacerbating the square-edge problem.

A more expensive way to cut keys is using a blue-punch type device. These will cut keys very nicely. Depending on what kind of system you are attacking, the given depth gradations may be incorrect, forcing you to use your own reference.

Another expensive way to cut keys is by using a duplicator machine. These machines use a stylus and a cutting wheel to read and cut a new key based on an old one. If you are using the techniques described above, you will need to cut keys by code, which is traditionally not possible on a duplication machine. However, if you can obtain a set of references for your key system, you can use the machine to cut by code by duplicating specific regions of your reference keys onto your new key.

Sometimes hardware stores who own these machines will cut keys to code for you, without you having to buy the machines yourself. Look for places that use a blue-punch type machine, as places that have duplication machines will not be able to cut by code. There also exist some online services like this. You may also get hardware stores or online services to produce you a set of references for your duplication machine.

7.2 Fabricating Keys

A milling machine will also cut keys, assuming they are fixtured well enough. Care must be taken on the ramps if plunge cuts are used. Making circular cuts using the side of an end-mill is recommended, assuming the key can be clamped properly. Milling machines can also produce restricted key blanks out of brass stock. However, this is a fairly difficult operation and modifying existing key blanks is highly recommended. Milling machines are also able to produce a variety of high-security features on keys.

Laser cutters can also be used to produce keys. Most laser cutters will not cut metal, but will cut very precisely into plastic. It is possible to create acrylic keys on the laser cutter out of a piece of acrylic stock. Unfortunately, acrylic keys are incredibly weak and will probably eventually break off in a lock, leaving behind evidence of unauthorized key manufacture. Instead of using acrylic keys, one can laser-cut just the bitting onto a piece of acrylic and then use a key duplication machine to copy it onto metal.

On a similar note, 3D printers can be used to produce working keys. There are several 3D printing technologies. Fused deposition modelling (FDM) is the most common, and uses extruded plastic. It has poor tolerances and is unlikely to produce working keys. However, it is incredibly cheap and may be used to prototype keys until the proper warding is determined. Then, a technology such as stereolithography (SLA) can produce plastic keys with a tighter tolerance. However, they still may be too weak to be used reliably. Selective laser sintering (SLS) can produce metal keys with incredibly fine tolerance, but is quite expensive per key and the price does not scale well.

8 Case Study

This is a fictional scenario made up to illustrate just how powerful the above technique can be at compromising the security of a building. Any similarities to a real building are by design because all buildings are secured in pretty much the same way, which is unfortunate.

The venue under attack is a large building. Large portions of it are open to the public during the day, but some areas are restricted.

On the first day, the attacker enters the building and checks out the locks. The building uses a Best SFIC system for most doors, and Schlage locks for mechanical rooms and outward facing doors. The attacker photographs a few locks in public places using a camera phone and leaves. There do not appear to be any poorly installed locks that can simply be unscrewed, but there are plenty of open doors with Best locks in them. There are no open doors with Schlage locks in them. A secluded open door is found and noted.

On the evening of day one, The attacker analyzes the photographs and finds that each make of lock uses only one keyway, and that they appear to be custom keyways. However, the Ilco FM and Schlage SC20 all-section keys look like they might fit. Since these are common blanks, the attacker has some on hand.

On the second day, the attacker enters the building armed with a multi-tool and a spare Best SFIC lock in a mortise cylinder that he had lying around. He heads to the aforementioned secluded door and finds it open. This gives him confidence that the door is never closed. As soon as there are no people around, he removes the latch face plate and loosens the retaining screw on the lock. He unscrews the lock and screws in the spare. The keyway does not match, but the door is never closed or locked, so it is unlikely anybody will try to use a key on it. Swapping out the locks takes two minutes and the attacker is not noticed.

On the evening of the second day, the lock is picked leisurely. He picks it to the control line, and removes it from the mortise cylinder. The pins are removed, measured, and replaced. Now, the FM blank is tried in the lock. It fits after slight modifications on a grinder. The decoded lock was found to have the control line unmastered, but all seven chambers mastered for the operating key. The bitting for the control key is filed into the modified FM blank and it is used to put the core back into the mortise cylinder.

On the third day, the attacker visits the site again in the morning. He puts the correct lock back into the secluded door, which takes another 2 minutes. He travels to a different part of the building which is less secluded but still not too populated. When nobody is looking, he uses his newly cut control key to core a door. This gives him confidence that he has the correct control key for the building. He swaps out the core for his spare, and leaves temporarily.

It is worth noting at this point that it took just two days for the attacker to arrive at the one control key for the entire SFIC system. This means that he can open any door in the system, though it would require removing the core and manually actuating the mechanism. But, being greedy, the attacker wants the master operating key as well. It is also more discreet to open doors with an operating key than with a control key.

Having a control key greatly speeds up the process, since the core does not have to be picked or extracted from the cylinder. Therefore, rather than going home, the attacker goes to his sketchy unmarked white van, and decodes the lock. He compares the possible bittings from the two locks and finds that they intersect at just one configuration: the master key for the system. He hand-files this bitting onto a key and tests it in the lock.

Two hours later, the attacker re-enters the building and replaces the spare core with the correct core. He finds a new lock and tests the master key, and finds that it works. On the third night, he rests.

After three days, the attacker has obtained the master key and control key to the Best SFIC system being used by this facility. Next, we look at how he attacks the Schlage system.

On the fourth day, the attacker uses his Best master key to enter a locked, vacant maintenance corridor. He finds a mechanical room secured with a Schlage lock. He finds that the latch bolt is not fully extended and thus the deadlocking mechanism is not engaged. Using his knife, he retracts the latch bolt and opens the door. He removes the mortise cylinder from the door, and does not bother to replace it since he feels it will not be noticed.

On the fourth night, he realizes that the lock he took was an LFIC lock. He picks the lock at his leisure, flips it 180 degrees, actuates the control pin, and removes the core. He then disassembles the core and decodes the lock. All of the chambers are found to be mastered. He replaces the core. He inserts an SC20 blank and is pleased to discover that it fits. However, he cannot cut any keys yet, since no bittings are known.

On the fifth day, he re-enters the maintenance corridor and replaces the lock he took. He finds a similar mechanical room with double-doors. The deadlocking mechanism appears to be working. He uses a pick to disable the deadlocking mechanism and a knife to retract the latch bolt, opening the door. He removes the lock and again, does not bother to replace it.

On the fifth night, he decodes the second lock. Because he took the locks from such similar doors, the master key is not fully determined. Two chambers are identically pinned, yielding four possible master keys (three of which could be sub-masters). He painstakingly hand-files these four keys and tests them on his stolen lock.

On the sixth day, he replaces the stolen lock. He then enters a populated area containing a roof door. This door is sufficiently different from the mechanical room doors that it is unlikely they share a sub-master key. He tries all four of his keys in this lock. He is not noticed because this only takes a few seconds and doesn't look out-of-the-ordinary. He finds that only one opens it: the top-level master key. He discards the three sub-masters.

In less than one week (with ample rest time) the attacker has compromised two separate lock systems comprising the security of a building. He never had to pick a lock on-site, nor spend more than 2 minutes at a door at a time. The attack was entirely surreptitious.

9 Solutions

This is not an easy problem to solve. Some band-aid solutions include strengthening the security around the deadlocking lever, inspecting doors frequently, and installing door closers. Cameras, motion sensors, alarms, and sensors will also improve security but will not fix the underlying problem.

The real vulnerability lies in a desire for convenience. It is desirable for locksmiths to be able to swap locks in and out without needing to open them (e.g. if a key gets broken off in one). It is also desirable to have a small number of master keys. The decoding vulnerability would not exist if each lock was singly keyed, or if extraction of a lock from a door was impossible. Neither of these are practical solutions.

The real solution is to move away from a mechanical key system. Encryption is practically impossible when done purely mechanically. On the other hand, implementing public-key cryptography or a zero-knowledge proof of knowledge is quite trivial on a microcontroller. These systems can be made provably secure, such that an attacker cannot gain access even after completely dismantling and decoding the entire system.

Therefore, a recommended solution to this problem is implementing a cryptographically secure, potentially multi-factor authentication scheme electronically at each door. A central computer would have to store quite a bit of sensitive data securely, and so it would be necessary to physically secure a single room. This room should be singly-keyed with a high security lock, with as few trusted people as necessary given access to it. Each room may also contain singly-keyed bypass cylinders in the event that the electronic system fails.

This system eliminates the master key and therefore the majority of this attack's potential. It is unfortunately incredibly costly, and it is unlikely to be properly retrofit onto buildings.

10 Ramifications

This attack operates on a few key principles. First, every mastered lock contains the master key, slightly obfuscated. This means that in the right (or wrong) hands, such a lock is as powerful as the master key. Relatedly, loss of a lock is not something to be taken lightly. Loose locks or open padlocks represent huge vulnerabilities, and in most systems, it is not immediately obvious if a lock goes missing.

The ability to open doors translates directly into the ability to steal locks. Because of this, doors should be inspected incredibly frequently, as it only takes one insecure door to reveal the master bitting. It also only takes one dirty employee to decode the master bitting. Even change keys should only be issued to trusted people, which is not an assumption that key systems often operate under. Not only does having a change key enable effortless opening and disassembly of a lock, but it may greatly facilitate decoding.

Because of the power and ease of this attack, it is applicable to all types of criminals. It does require a bit of forethought and is therefore not applicable to crimes of opportunity. But anybody with one month or even one week worth of advance planning can execute this attack once and make subsequent break-ins trivial.

11 Summary

We hope this paper has been eye-opening as to the feasibility of a speedy, surreptitious attack on a key system integrated into a building. We publish it with the hopes that it will lead to improvement in the field of physical security, which appears to have fallen behind technologically. Mechanical key systems have been repeatedly shown to be lacking, and it is time they are vastly improved or phased out in favor of well-implemented electronic systems.

References

[1] "Schlage SFIC Service Manual." Ingersoll Rand Security Technologies. Ingersoll-Rand Company Limited, Dec. 2007. Web. <http://professional.schlage.com/pdfs/pc/Security_and_Keying_Solutions/SC_5292_SFIC_Service_Manual_for_web.pdf>.

[2] "Schlage Cylinders, Keys, and Key Control." Ingersoll Rand Security Technologies. Ingersoll-Rand Company Limited, 2002. Web. <http://professional.schlage.com/pdfs/literature/Cyls_Keys_and_Key_Control.pdf>.

[3] "Schlage L-Series Service Manual." Ingersoll Rand Security Technologies. Ingersoll-Rand Company Limited, Dec. 2007. Web. <http://www.mfsales.com/schlage/L-series-svm.pdf>.

[4] Photo by Authors

[5] "Schlage Portable Security and Cabinet Locks." Ingersoll Rand Security Technologies. Ingersoll-Rand Company Limited, Aug. 2008. Web. <http://professional.schlage.com/pdfs/literature/CL-Series.pdf>.

[6] ToolyMcGee. "Keying Your Old Yale & Towne Padlocks." Keypicking.com. N.p., 14 Dec. 2009. Web. <http://keypicking.com/viewtopic.php?f=58&t=2347>.

[7] Blaze, Matt. "Notes on SFIC (Best) Interchangeable Core Locks." N.p., 21 Apr. 2003. Web. <http://www.crypto.com/photos/misc/sfic/>.

[8] 45calcan. "Schlage I-Core Picked Then the Control Is "picked"" YouTube. N.p., 10 Mar. 2009. Web. <https://www.youtube.com/watch?v=g1VPVzJA_nA>.

[9] Christiaan008. "DEFCON 19: Introduction to Tamper Evident Devices." YouTube. N.p., 27 Oct. 2011. Web. <https://www.youtube.com/watch?v=W07ZpEv9Sog>.