Locksmithing

Contents

This is not a freebie so much as it lets you get free...

Alarm

Beware that in many instances where you encounter good locks, there is likely to be an alarm system in place.

Car Door Locks

Older cars can be unlocked with a metal yard stick that has a 1/2 inch notch cut into it, start hooking near where the door key box appears to be. This risks setting off side airbags and injuring the user in cars equipped with them...

Car doors (and even ignitions) usually use wafer locks, and the priority is light weight and safety over security. These locks generally have poor tolerances and can accept half height cuts. This makes tryout keys, jiggler picks, and special "slimline wafer picks" highly effective. These all essentially go through every possible key combination very rapidly until the lock turns.

The wafer locks are also vulnerable to the same type of impressioning as the pin tumblers generally found on doors.

Tubular Locks

Tubular locks (aka cylinder key locks or rim locks) have to be picked pin by pin. Rotate them about 20 degrees after the pins are in place and press a piece of clay firmly in the lock to create a key. Be careful not to deform it when removing it and allow it to harden thoroughly before use. Don't forget to turn the lock back so nobody notices while you're waiting for your key. This will get you into vending machines and sometimes let you operate security system keyswitches. The Van-Lock, a flat face tubular lock has the same vulnerabilities.

Also a special picking tool exists but it can cost anywhere from $30-200, and such a purchase raises suspicion.

Picking Lever Locks

These are old looking locks with a typical keyhole shape. They can be which can be opened with two pieces of stiff wire, one to apply rotation and the other to raise levers in to place. You only need to torque one pin, generally behind the rest, and most keys only have about 2-3 levers (high security varieties with as many as 20 exist). Practice makes perfect, so buy a deadbolt like from your local hardware store for about $10 and see what works best for you.

Warded Locks

Truly old locks, those that came about before lever locks, and cheapo padlocks use this locking mechanism. They'll be either old with the traditional "keyhole" shape, if they're warded door locks, or on a padlock you'll generally see a rotating disk as the keyway, which will often be zig-zag shaped (MasterLock will). Theses really are a joke of security, to open them you need to rotate one lever inside of the lock. The only thing preventing this is a series of obstructions so you can't just jam a flat piece of metal in the keyway. These can be opened with a firm piece of bent wire, or for convenience one can use special warded picks. Masterlocks contain two levers that must be operated at once.

Masterlock skeleton key: Acquire a Masterlock warded key, it has a different shape to it's head, is double sided. It will only have two "heights", either having protrusions or not. File off all but the two at the tip, and then carefully play with how deep it's inserted into the lock. You should now be able to consistently open all padlocks with this mechanism with a simple counterclockwise rotation of your skeleton key.

Pin Tumblers

By far the most common type of lock, there are a multitude of ways to defeat these:

Freeze the Lock

A number of locks are vulnerable to properly executed freon attacks. Freeze the cylinder so that it becomes (relatively) brittle. Use liquid nitrogen if it's available, or try emptying an air duster into the lock. Immediately after freezing the lock, put a chisel in and strike as firmly as possible with a hammer. Hopefully after this the lock will be willing to turn. This should also work against wafer locks.

Lock Bumping

A very effective and easy way to open almost any lock. Have a key fitting the lock cut to maximum depth on all cylinders leaving shallow elevations between, the tip and shoulder are filed back 1mm, your bump key is ready. If tapped with a screwdriver handle, while applying a gentle turning pressure in the direction of opening, will bounce the pins separating them and allowing the lock to turn after a few tries. If you want to make your own bump key, all you need is a file and a key; go here (http://www.youtube.com/watch?v=pwTVBWCijEQ) to learn how to make one. Or click here (http://www.capricorn.org/~akira/home/lockpick/bumping.pdf) if you want to learn more about the theory and application of bump keys.

See also http://en.wikipedia.org/wiki/Lock_bumping

This will require either getting appropriate keys or keyblanks to cut down.

Blanks for Schlage and Kwikset, common residential locks can be had at your local hardware store or shopping mall key cutters. Try asking an unproffesional employee at the mall to cut you a 999 key. Some blanks, like BEST and other institutional locks, may require a bit of effort to track down, but can be found online.

Using a pick gun or vibration pick with a tension wrench is a variation on bumping, and works similarly. Be sure to keep your impact length low, put the blade directly under all of the pins, and hold it flat to deliver a vertical impact. Gradually increase the impact length if the lock doesn't spring open in a few tries, and beware that you may overset pins and need to release tension (if you've bumped it around ten times and it's not opening).

Bumping will NOT open wafer locks

Traditional Tension and Pick

The traditional method of lock picking is slow and requires quite a bit of skill. There is no magic Magnum PI ten second unlocks without the practise of a competitive unlocker. The technique involves applying tension in the opening direction of the lock with a flat torque wrench made from a hairpin or bought in a picking kit, a pick or rake is introduced and an attempt is made to align all of the

pins in their sticking spots in the mechanism where they are held by the tension from your wrench. If you want to learn this useful technique, you should read the MIT Guide to Lock Picking, available here (http://www.capricorn.org/~akira/home/lockpick/) and here (http://www.lysator.liu.se/mit-guide/Main.html) .

This should also work against wafer locks.

Door Jack

If you can use a jack of some sort to bow out the door frame even deadbolts might be defeated in seconds, put plywood squares at the contact points to prevent scarring the door frame. Any lock can be compromised by bypass.

This technique is often employed against steel doors by locksmiths. The door features a "deadlatch" to prevent people from jamming a card into the door to open it. Using a wedge or jack, one can spread the door frame and latch far enough apart that the deadlatch mechanism disables. Then, one simply slips a credit card or butter knife between the two and pushes the door open.

Push Knife

Some doors are not equipped with a deadlatching mechanism or have one incorrectly installed, and you can push the bolt back into the doorframe with a credit card or butter knife, springing the door open.

Drilling

This technique works best for pin tumbler locks. Identify where the pin stacks are, then drill through them at the top of the plug (cylindrical part the key enters, which you rotate) where the plug meets the lock body. The drill bit only needs to be slightly wider than the pins. Once all pin stacks have been drilled through, insert a flathead screwdriver in the lock and turn. A carbide end mill in a die grinder will go even through anti drill pins with relative ease.

And to think that some locksmiths have said "criminals don't drill locks"...

Wafer locks are harder to drill, but it is possible to use a hole saw and cut around them. Another possible method is to insert a blank key and with the top of the handle filed off, then to drill like a pin tumbler. This should cause all wafers to bind at the top of the plug, and proceed to destroy that point. Afterwords, the blank key should be able to turn the lock easily

Combination Locks

Used on safes and padlocks they can be opened by listening to the clicks of the mechanism, beating the combo out of its owner, or dynamiting the safe. The safecracker listening to the clicks is often offended by the sound of detonating dynamite next to his head.

Mutli-dial combo locks, including those used for bicycles, can often be quickly picked by applying opening pressure, then rotating the dials one by one until they stick on a number (with a little click of a peg going into a http://wiki.stealthiswiki.org/wiki/LockSmithing 4/8 hole). Normally this process can be done in a few seconds and will open the lock. Some locks have additional security features where the wheels will bind in a few wrong positions, the simplest way to overcome this is to feel all the wheels that resist turning. If they feel like they're scraping, they're probably a wrong number and should be rotated farther; if they feel like they're stuck on a number but not scraping against a piece of metal, they're most likely correct.

Cheap padlocks can be shimmed with a properly cut piece of thin aluminum, from a beverage can material for example. It is also often easy to break cheap locks by holding on tightly and jerking it hard a few times until it opens, assuming you have no bolt cutters.

Buy a cheap bendy saw (.99cents at some stores) and simply saw through the narrowest metal part of the lock. This works on padlocks and some bike locks too, and only takes about a minute.

Kaba Simplex Vulnerability

The Simplex is a type of mechanical push-button combination lock often deployed as high security on government and corporate buildings. It resembles a lever handle with a rectangular area above it, containing about five vertically stacked buttons. In a recent ”restricted to security professionals” release, the lock was bypassed in a matter of seconds.

A powerful magnet (450+ lb pull force) is placed on the left side of the lock at approximately the level of the bottom of the buttons. The handle should then engage the latch and allow you to operate the door successfully.

Videx CyberLock

A new line of electronic retrofit locks has found itself onto store fronts and vending machines around the nation. These locks are advertised as very high security, but can be bypassed with very little skill, given the right knowledge. Since they're shaped to match older mechanical locks, they're placed anywhere regular locks could be.

A paperclip can be shaped to fit the keyway quite accurately, and is used to rotate the lock. First, the paperclip is put in place. Next, a powerful magnet is applied to the face of the lock. Afterwords, the lock is struck with a plastic or rubber hammer to cause it to vibrate. This should move an internal component forward, where the magnet will hold it.

At this point, the paperclip should become able to turn the lock and unlock whatever it was "securing".

Copy a Key

Plaster Mold

OSS officers in WW-II sometimes carried a key kit containing plaster of paris and talcum powder to take a double sided impression of a key. The talcum powder would keep the two plaster sides from sticking as the impression was taken. A special low melting point alloy would be melted with a candle and poured into the mold making hopefully a perfect if flimsy copy key. One possible alloy is Cerrotru or other Cerro alloy, Bismuth-Lead, Tin, Cadmium & Indium Alloys which melt at between 160° F and 281° F, low enough that a candle or even boiling water would work. Tin and bismuth can also be melted to make a similar melting alloy.

Align and File

Matching a proper blank to a functional key in a vice and carefully filing by hand will produce a working copy. It can help to blacken the working key with a candle, so that you can know when to stop filing as soon as the soot scrapes off. Remember that the only thing you need to get right is the height of the flat parts between peaks. Also, alignment is crucial!

This is only necessary with keys marked "do not duplicate" and/or cut on obscure blanks (BEST, Arrow, Yale) because in the time spent in this method you could easily have it replicated at a key cutter. It's still worth a shot at various unprofesional key cutters if it says "do not duplicate" as there really isn't much legal weight behind the stamp.

Impressioning

This technique is wonderful because it creates a working key to the lock, or even master keyed system, without access to the original key. This requires getting a fitting key blank. Ideally one would then make a mold of that and produce either a soft metal (copper or lead) blank.

Using pliers or vice grips, insert the key into the lock, apply as much rotational force as possible without bending the key, and then jiggle it up and down forcibly, repeat this turning in the other direction.

Now look at the top of the key, where either the pins or wafers should have scratched it. Pins will generally leave a circular mark near the center of the top of the key, wafers often mark the edges, or create a line across the key. Make a couple passes with a fine file in these areas, and try again.

Be sure to angle the metal between two flat areas, otherwise the key will get stuck in the lock, or not enter.

Performing this technique should get you a working key in anywhere from 5-60 minutes depending on the lock and your expertise.

Tin Can Copy

Get some scissors A square of thin metal Gluestick A ruler And a printer

First scan your key- you could take a photo with a ruler present if you're in a pinch (you can also use a quarter for a reference size, and edit it with photoshop) print the scan or images as copies to a 1:1 scale *same size as the key* cut them out with paper around the edges.

Stick key number one onto a piece of the metal Cut it out, but leave metal around the teeth

Now use the ruler to force a v shaped groove into the key along the grove on the picture Now that you have the correct grooves, you can line up the key with the second printed copy, at this point you will need to cut the second printout exactly around the profile of the key (teeth included). Now it will become apparent why we left some extra on the teeth; the groove will have shortened the height of the key and so the teeth now need to be cut higher up on the metal.

Cut the teeth with continual reference to the printout. This is the crucial part, it must be very accurate. Make sure the teeth are not slanting to one side, if this is the case then the thin metal may slide down the edge of the pins and not push them up. Use scissors with a good pointed cutting end and try to cut only using this end- this allows you to get quite accurate cuts without maneuvering the scissors around risking bending the teeth.

You will have to turn the lock with a mini Flathead or a torque wrench as the metal is usually to weak. Wiggle it in the lock very gently- if it does not work the teeth may be bent or slightly off- print out more images just in case.

Hand Cuffs

These are simple warded locks with a locking pin on the other side of the cuff. That is what the little nub on the back of a cuff key is for. Almost all hand cuffs use identical keys, sew on into the back of a belt or your pants. Although it is almost impossible with the double sided nature of cuffs to unlock yourself, two friends could save each other. A loop on the key makes it harder to drop when your hands are behind your back. Shimming the ratchet with a piece of steel or aluminum can might be an option if you are running from the prison work crew, but if they have been double locked a shim may not work. Buy a hand cuff set for fooling around with your partner and try to escape while distracted by.....

Prox cards

Most prox cards have an encrypted chip that is fed a signal and then responds with an answer via radio frequency. A reader/writer for your card would be needed to hack it. These Readers have become for more accessible in recent days, even store like RadioShit carry them now. It's quite possible, with some antenna and power hacking, to read these chips from about a dozen feet away. This means you can walk by an employee or sit by them in starbucks with your laptop, and produce a copy of their working key for your own use. See Infiltrating for related content.

Magnetic Stripe Cards

These are easy to copy and have mostly gone out of use except with ATM and credit cards in the US and Canada. You can see the four tracks found on most magnetic cards by dusting with fine iron oxide it looks like a narrow bar code in dust, you need to align four heads designed to write to these data tracks.

Practice and Advice

All of these techniques, even bumping, require practice. Buy several different kinds of locks and start playing with them, figure out what a combination lock sounds like when you enter the right combination and what clicks happen at wrong numbers. Learn the feel of a lock pin that is caught at the halfway point so you can go to the next pin.

A good motto for entry is try before you pry. Look for unlocked windows and back doors, maybe kicking the drywall will get you through, is the wall of that bank vault made from easily sledgehammered cinder block? Why spend twenty minutes working on the front door when the fire escape leads to an open window in back?

Stick a Lock

Superglue will seize a lock. Blast the lock with a shot of carburetor cleaner to remove any oils then shoot a whole tube into the keyhole. The lock should be out of operation and difficult to remove since the pins will be seized, don't do this as a gag, it is an expensive fix as the door may also need to be replaced from the violent removal of the lock mechanism.

Another, although slightly easier to fix approach, is to get a key that fits the system, and file the top part of it to a barbed edge. This will let the pins raise over the key and drop past the barb, but not in reverse. Now they have a non-removable key that will cost hundreds of dollars and several hours of locksmith work to remove.

Locks this guide can't cover

There are many varieties of high security mechanical locks that it's not reasonable to expect anybody reading only this text to get open. If you see any of the following brand names, it's probably time to move on, or whip out the drill: Medeco, BiLock, Schlage Primus, Abloy Protec, Keymark, Mul-t-Lock, etc.

While most electronic locks are considered high security, they will fail (open, or become inoperable) either from powerful magnetic fields, applying high power across the pins, or microwaving.

Outside Links

http://en.wikipedia.org/wiki/Lock_picking
http://www.instructables.com/id/E3RGSYZ641EQHOASFH/ Making a Padlock Shim
http://en.wikipedia.org/wiki/Hand_cuff#Escaping
http://mia.ece.uic.edu/~papers/etc/pdf00002.pdf MIT Guide to Picking Locks
http://en.wikibooks.org/wiki/How_To_Pick_Locks
http://www.lockpicking101.com/
http://crypto.com/photos/misc/sfic/

Locksmithing

Last updated: 16 August 2011

stealthiswiki.com