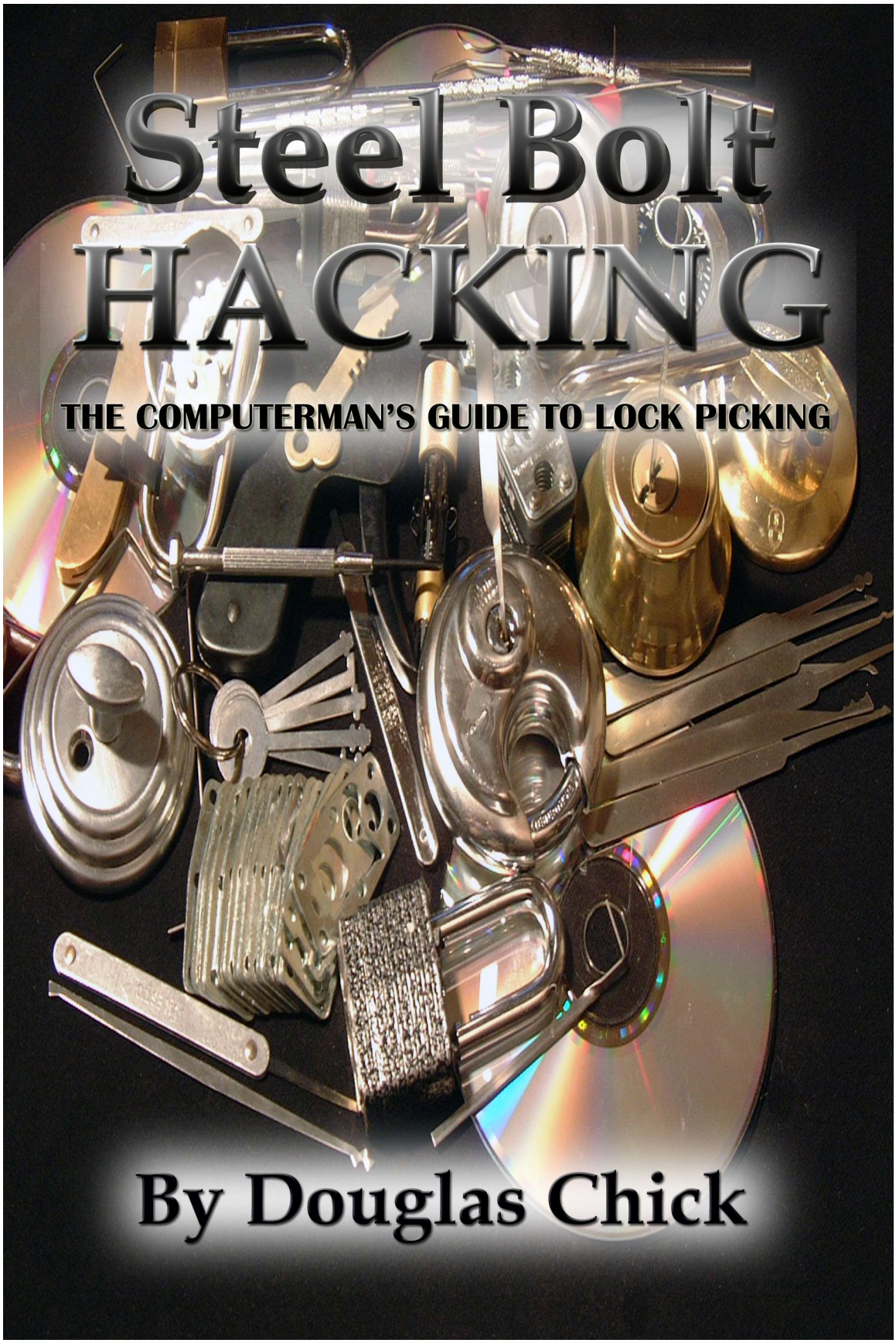

Steel Bolt
HACKING
THE COMPUTERMAN'S GUIDE TO LOCK PICKING
By Douglas Chick

Steel Bolt Hacking
By Douglas Chick
ISBN: 0974463019

Below you will find a few sample chapters from Steel Bolt Hacking

Introduction

Steel Bolt Hacking, or Lock Picking as it's most commonly known, is fast becoming a competitive sport among computer people. And it's far more than just picking locks. The 'sport' includes cracking combinations, push button door locks, electric key cards, and just about anything that has a lock to it. Lock picking sports groups are beginning to spring up in the U.S., the fastest growing groups are within the computer industry. Most computer people are fascinated with unlocking codes, bypassing security protocols and finding program vulnerabilities that can be exploited. Picking locks and cracking combinations are no different.

When I say that computer people have taken up the hobby of lock picking, I don't mean to suggest that they are breaking into people's homes or cars. Steel bolt hacking is nothing more than the challenge of picking locks in a legal and competitive manner. The only locks that are picked or combinations that are cracked are from locks that have been purchased for nothing more than the challenge of opening them with alternative methods. Some computer people have taken up lock picking as an alternative career that has led to becoming a part-time locksmith.

As far as I know, every computer person that has taken up lock picking or combination cracking has done so in a completely legal manner. The methods and styles of lock picking are passed on with an understanding that they are not to be used in committing illegal acts of breaking and entering. All the locks picked have been purchased and passed between other lock-picking enthusiasts to help sharpen their skills. Never have the skills and/or locks been used in a crime.

This book's objective isn't to turn anyone in to a master criminal, or a minor one for that matter, but instead to help educate enough people to turn lock picking into a larger and more competitive sport. The techniques discussed in this book will require time, patience and practice. It can take up to 30 minutes to pick a lock, that is too much time for a criminal who can easily jimmy the door or drill out a pin in under 2 minutes. Time is always against a criminal, this is why they typically use brute force entry when committing a crime. Lock picking is an art that requires time to learn.

Lock Picking Sporting Groups

The creation of lock picking as a sporting group is said to have begun in Germany. What started out as a curious interest quickly grew overnight to a 500- member club, and today is around 1000 members strong. For legal reasons, and how the laws in Germany are phrased, this group of lock picking enthusiasts did not want to be classified as an organized crime group and turned their club into a lock-picking sports group. There is a very strong anti-organized crime law in Germany that essentially says if you teach

someone a skill that is used to commit a crime, than you are involved in an organized group and will be prosecuted with the person who actually committed the crime. One could understand how 500 lock pickers assembling together and teaching each other how to pick locks could be difficult to explain if one of the members used this knowledge to commit an illegal offense.

A sports group was invented, with rules, contracts and membership cards. A signed contractual agreement stated that each member would never use his or her knowledge to commit a crime.

So there we have it, the birth of the first organized lock picking sport group in Germany that today has more than one thousand registered members. If you go to their Web site, http://www.lockpicking.org/ you will see that this sport has extended into the Netherlands, United Kingdon, and France.

Although the credit could go to a man named, Hans (The Unicorn) van de Looy from the Netherlands who is said to have inspired the Germans. You will find him and Barry (The Key) Wels at http://connect.waag.org/toool/.

The name 'sports group' has carried over and is used in the United States. Every year at DefCon, an annual hackers convention in Las Vegas, there is a lock picking competition.

For DefCon / LPCon FAQ:
http://www.worldwidewardrive.org/dclp/LPCONFAQ.html

For DefCon / LPCon Rules and Registration:
http://www.worldwidewardrive.org/dclp/DCLP.html

I first heard about this event from my friend in San Diego, Will Nett. He sent me my first lock picking set and told me that everyone he has introduced to lock picking became addicted. I just laughed at that statement. All of Will's friends are computer geeks. He was right. After the first lock sprung open, I was addicted. It must be a computer thing.

Holding the padlock

Hold your padlocks with the pins at the top of the key way. Some people will hold the lock with the pins down because it feels easier on their fingers. When in fact the lock is harder to pick because gravity pushes the pins back towards the shear line, you want gravity to push the key pins away from the shear line. With the pins on top it is easier to differentiate the feel of the pins that are pressed down upon by the top springs, or fall freely with gravity. It is still possible to pick a lock upside down, (I am told that most of the locks in Europe are installed upside down) it is just a little more difficult to do.

If you notice from *Figure* 1.9, I hold the padlock in one hand, and also push down on the torque wrench with the fingers from the same hand. This frees up my other hand to pick with. If this is uncomfortable for you, then simply play around with it until you find a position that works best for you. Left-handed people would simply use their right hand to hold the lock and their left to pick with.

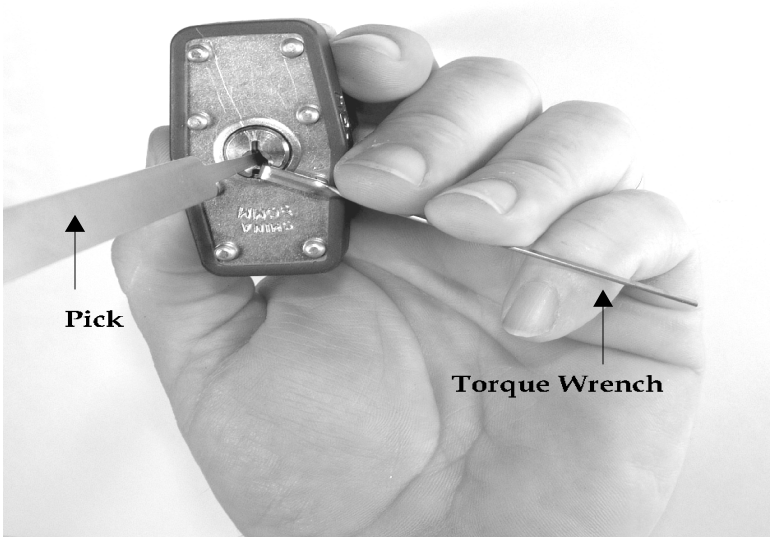


Figure 1.9 Holding a padlock

Counting the Pins

The first thing that I liked to do is count how many pins I'm going to be working with. Typically in a padlock there are only 4 pins, sometimes more on expensive locks. I always begin with my half-diamond pick and will drag it on the roof of the plug and count the pins. Because there is little or nothing you can actually see without the aid of a scope, you must rely on feel to count your pins. As I drag my pick along the top of the pins, I can feel that some pins are a little bouncier than others. Once a pin is set in its corresponding hull, you will feel that it has lost its bounce from the spring above the top, or set, pin.

Which Direction Does the Plug Turn

The Torque wrench is the tool you will use to turn the plug. Most padlocks will turn in either direction. Sometimes if you are unsure you can insert your torque wrench and turn it in both directions. The direction that turns the furthest is usually the correct direction for the key turn. It takes two tools to pick a lock; the pick to set the pins and the torque wrench to apply the turn.

Now that we are ready to pick our lock I want to make a final comment: You must exercise patience. Not everyone will get it on the first few attempts; it takes some people days before they successfully open a lock. It's easy to become frustrated and give up, when this happens, simply walk away and try again later. Only practice combined with diligence will make you a good lock picker. This is why lock picking isn't for criminals. Someone wanting to use the information in this book to help commit a crime would never read this many pages before committing a crime. That's why most burglaries are committed with a hammer and crowbar.

Lock Picking Facts:
In spy movies when you see the hero walk up to a door and insert a single pick and he or she immediately opens the door, that tool is called a key.

Padlock Shims

Another method of opening a padlock is by using padlock shims. Padlock shims are thinly formed stiff metal designed to slide between the shafts of a shackle on the toe or heel or even both. When the padlock shim is turned, they can block the latch from entering the shackle lock groove. Using padlock shims is often a faster and easier way to open a padlock. Padlock shims work on 90 percent of the most common padlocks and are typically faster at opening the lock than picking. Shims do require practice with different styles of locks, as the shackle lever is located in different positions. But even with a foreign padlock you can usually feel your way around and open it.

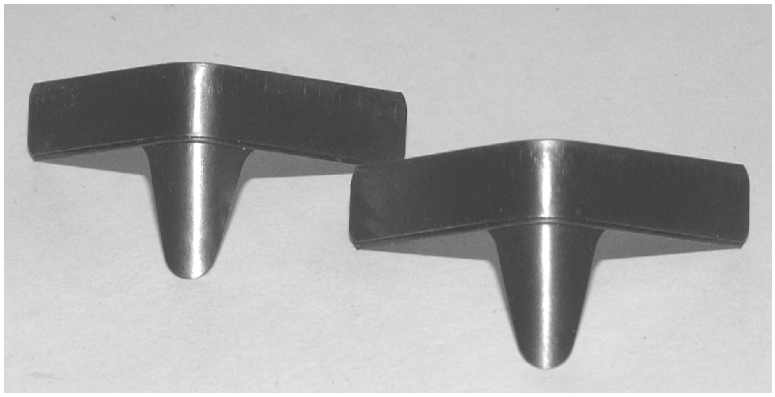


Figure 1.14 shows 2 Padlock Shims

Figure 1.15-A Shows two padlock shims slid down along the shackle and blocking the lock latch from inserting into groves on the shackle. 115-B shows the same lock opened with shims and an arrow pointing to the latch lever inside.

Padlock shims work on most padlocks, and generally come in four sizes. You can find them on the Internet for around $20 a set. When using a padlock shim you have to be careful with certain locks on how you place them because one wing handle should be placed on the inside of the shackle so when you turn them, one side of the shim doesn't get caught up on the shackle. You'll know what this means when you open your first lock.

The latch in *Figure* 1.15B is to the side. On other padlocks on which I've used this technique, the latch is usually on the inside of the hole. When you slide the shim along side the shackle and follow it into the hole, you can turn the shim and usually feel where the latch is because your shim will fit lower in some areas than others. Like with a pick, you must feel your way around to find the lowest point and then turn into the latch. *Figure* 1.15A shows two padlock shims, but some padlocks may only need one. Just listen for the clicks and any movement you feel it when it turns. Just a word of warning though, padlock shims are a little tough on the fingers. You have to gently slide the shims into place without bending them and bring the two wings together and twist hard.

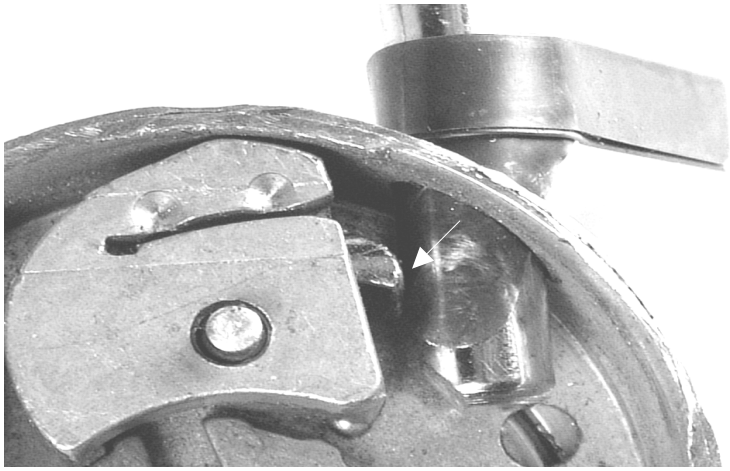
Cracking a Combination Padlock

In this next section I will show you two different ways to open a combination padlock without first knowing the combination code. This method can be used to uncover a lost combination code and is 90 percent accurate on all Master Lock combination padlocks. I only say 90 percent because I've heard that some people say it won't work on some locks.

However, I've had a 100 percent success rate so far. Master Lock Company is said to have redesigned its 1500 series combination lock, (this is the standard combination lock that you used in school as a child) and it showed up on the shelves somewhere in the middle of 1999 and 2000. These methods that are listed in the book may not work on those redesigned models. However, I have recently purchased three newer "1500 Series" padlocks and cracked all three. Some feel that Master Lock returned to their old design. The newer locks (ones that this method is reported not to work on) have serial numbers beginning with the number 800 on the back of the lock. Locks that do work are the locks with serial numbers beginning with 90, 01, 120 and five digit serial numbers, including those preceded by X's. However, I have heard it said that people are still opening these newer redesigned padlocks nonetheless. Also note: the same locks with keyholes in the back are also susceptible to this method. Those locks are made for schools so that school officials can inspect lockers. Either way, we are only picking locks for fun and or hobby, so if it doesn't work for you, it isn't like you are losing out on the market in reclaiming old padlocks with lost combinations. All those locks are collected at night by the lock gnomes and are never seen again.

Opening a Combination Lock with a Padlock Shim

Now, opening a combination lock with a padlock shim. You will need the largest shim you have to open a combination lock padlock, because of how deep the latch that holds down the shackle. You will need to slide the shim on the outside on the right hand side of the shackle. Slowly turn the shim until it is on the inside. You must wedge the shim between the shackle and the latch, as shown in *Figure* 1.26. The white arrow indicates that the shim has been successfully seated and the shackle can be pulled and unlocked. If the shim rises up during the turn, as in many cases it does, you will have to begin again. It is a delicate procedure sliding the padlock shim in and exerting enough force without bending it. You have to simply twist, wiggle and push the shim down and to the side until you can pull the shake out. The fastest that I've ever opened a combination lock with a shim has been 10 seconds. On the same lock a few days later it took me 4 minutes to open. Some days you surprise yourself with just how fast you are, while others you don't know what you're doing wrong.



You may purchase this book, Steel Bolt Hacking, on www.Barnesandnoble.com, www.Amazon.com or www.thenetworkadministrator.com

Steel Bolt Hacking
By Douglas Chick
ISBN: 0974463019