

Introduction To Basic Lock Picking

Gurney Halleck

DefCon VI

Jul 29-Aug 2, 1998

Contents

- Why Lock Picking?
- How a Lock Works
- Exploiting Vulnerabilities
- Picking Tools
- Methods: Scrubbing
- Hints and Tips
- Thoughts on Lock Picking
- References

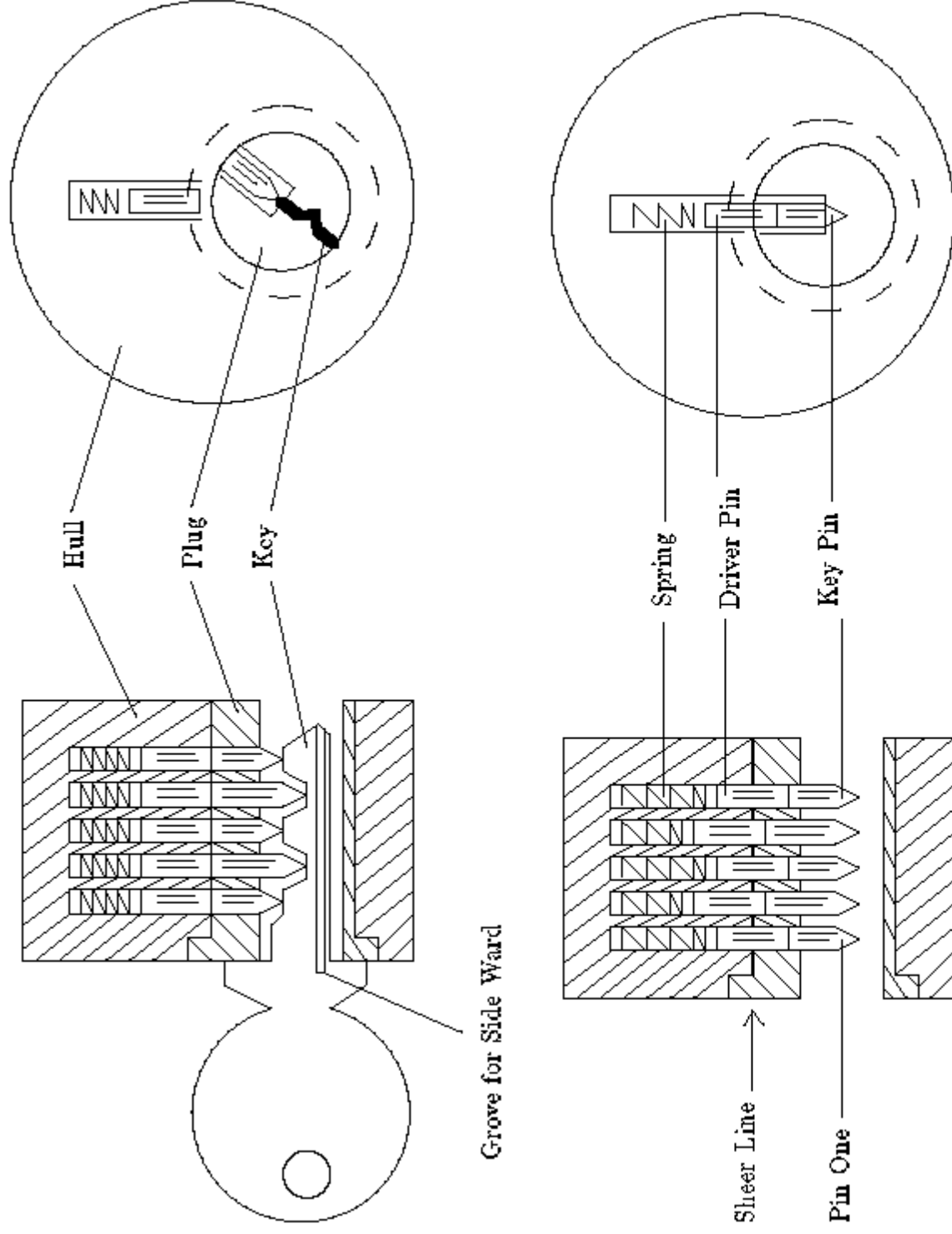
Why Lock Picking?

- Easy and Effective Hack
 - With a little practice, you'll be able to open most of the locks you encounter.
- A Practical Skill
 - Several times a year, friends and co-workers come to me because they've locked their desk, office, car or computer case and forgotten the key. A quick pick can save a lot of time, frustration and money.
- Promotes Analytical Thinking
 - Since you can not 'see' the actual picking of the lock, you need to feel and imagine the process. A very good skill for any hacker.

How a Lock Works

- Figure 1 shows the major components of a pin tumbler lock. While not all locks work exactly this way the principals are similar.
- As the Key is inserted into the keyway it lifts the pins.
- Once the proper key is fully inserted all the driver pins and key pins are lifted to the shear line. When the pins are at the shear line the plug can rotate in the hull opening the lock.
- If an improper key is inserted, some or all of the pins will not be lifted to the shear line preventing the plug from rotating and the lock from opening.

Figure 1: A Pin Tumbler Lock



Exploiting Vulnerabilities

- If locks were perfect and all the pins were aligned perfectly, the key would have to lift all the pins at the same time to the sheer line to allow the plug to rotate.
- In fact no locks are perfect, there is always some sort of skew in the the pin alignment. (Figure 2)
- When torque is applied to the plug some pins will bind before other pins. This defect allows us to set each pin individually allowing the plug to rotate slightly. This small rotation holds the set pin up while binding another unset pin. (Figure 3)
- If the proper torque is maintained on the plug each pin can be set one by one to open the lock.

Figure 2: Pin Alignment

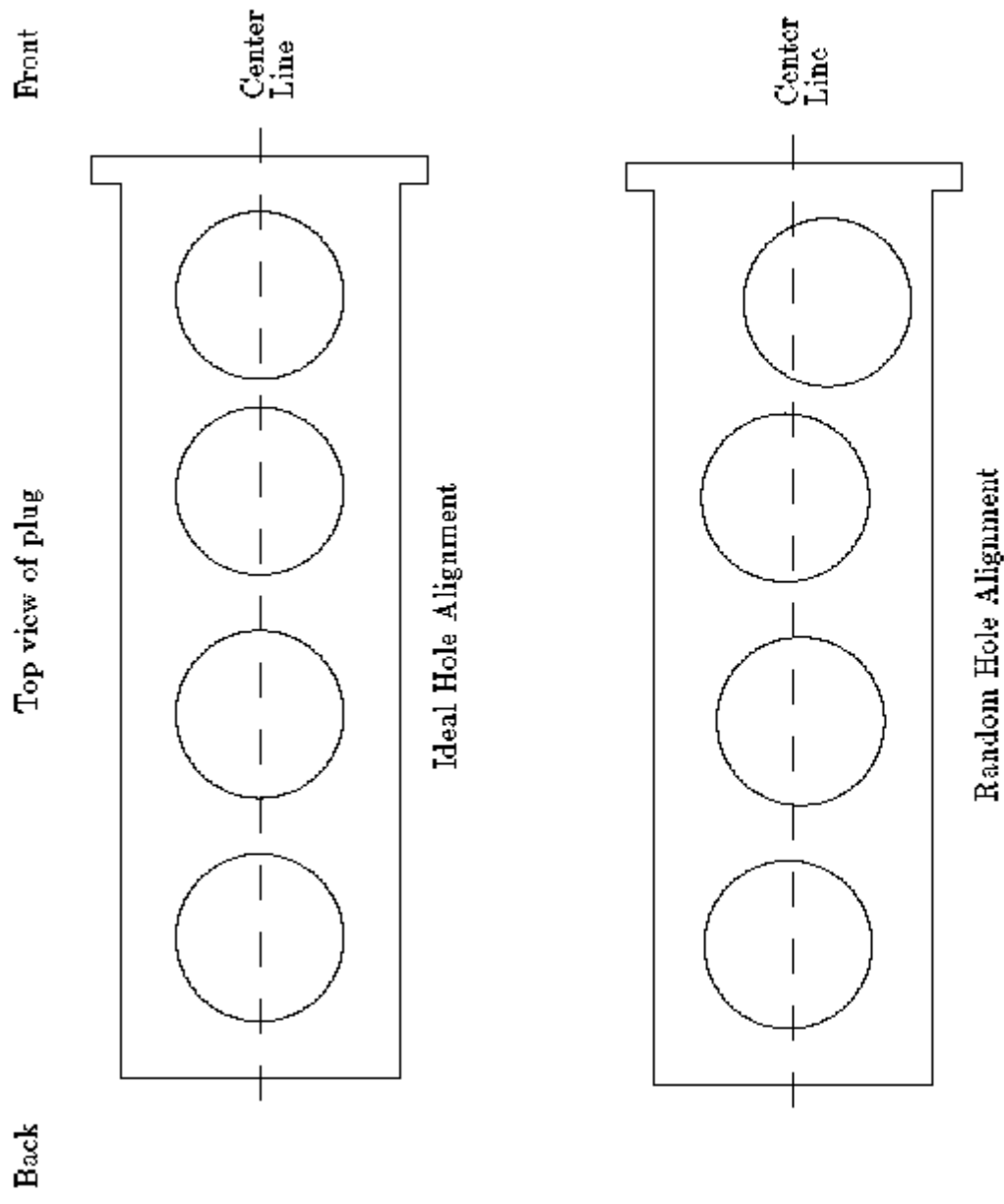
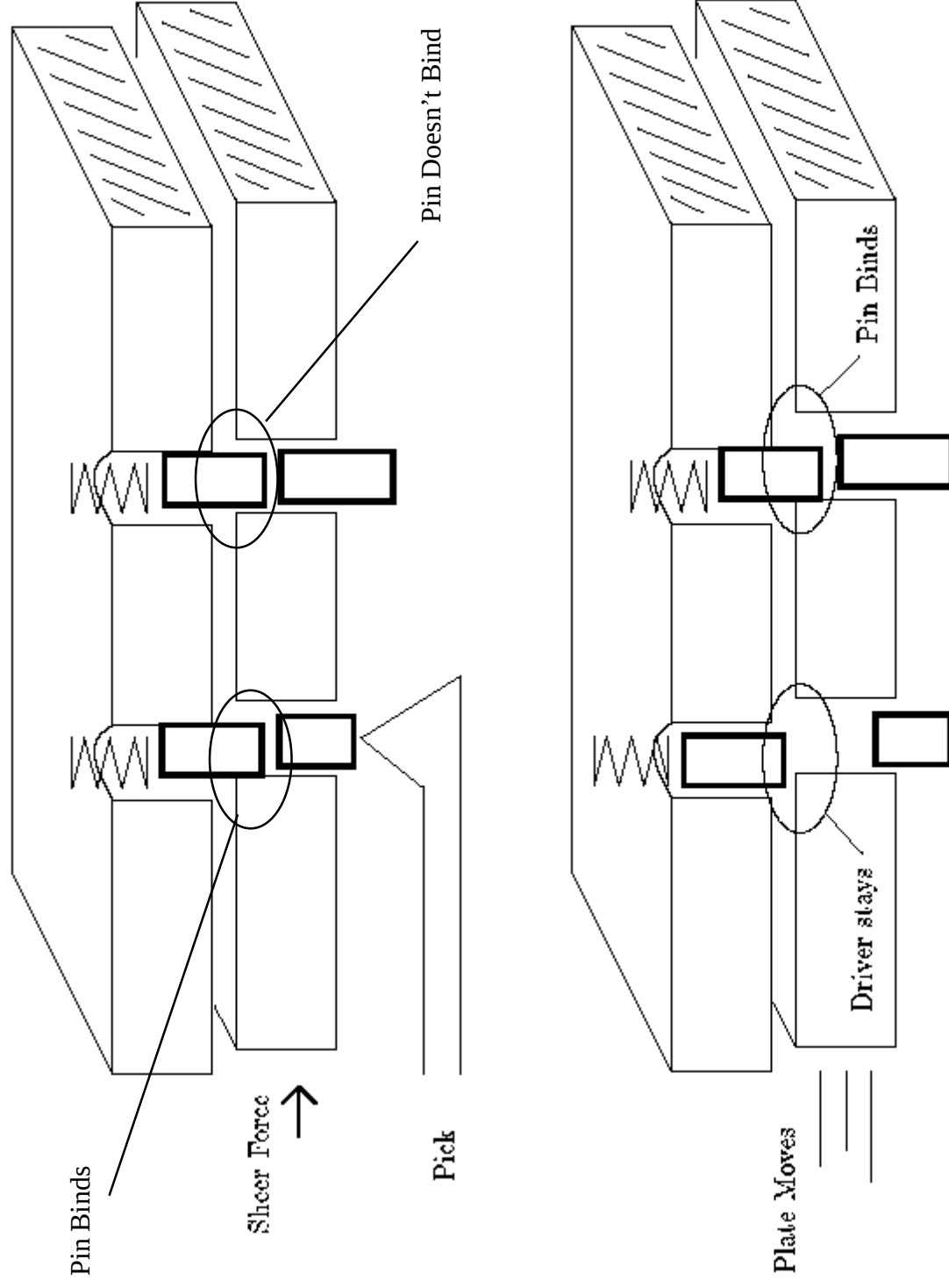


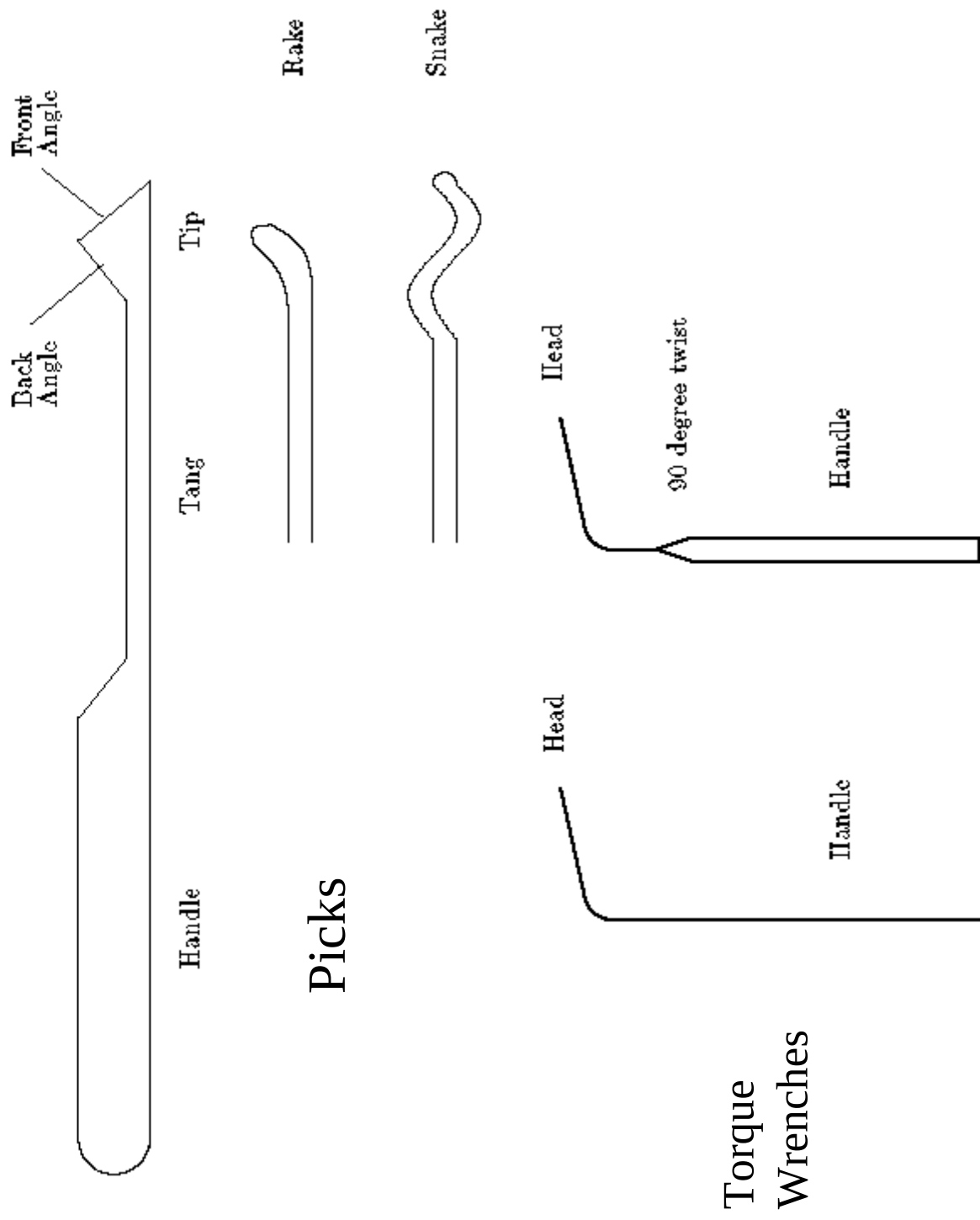
Figure 3: Setting Pins



Picking Tools

- The Average pick set will come with several picks and one or more torque wrenches. (Figure 4) Cheaper sets will have bare handles while nicer ones will have finished handles. The ones with finished handles are much easier to work with due to the extra weight and the larger surface area. (the bare handles tend to 'bite' your hands)
- I find that my most commonly used pick is the snake shaped rake and a torque wrench with a 90° twist. If you buy (or make) the tools individually these are the two that I would recommend. They will open the majority of locks using the scrubbing method.
- The basic rake is used when actually 'picking' the lock one pin at a time. (usually not necessary)
- Having a couple of torque wrenches, one for light torque and one for heavier torque, is very convenient.
- Unless you absolutely can not buy pick tools, I wouldn't suggest making your own.

Figure 4: Picking Tools



Methods: Scrubbing

- In most cases you won't actually be 'picking' the lock you will be scrubbing. Scrubbing will work on most locks you come across, is very easy to learn and usually faster than setting pins individually.
- First, a light torque is applied to the plug to bind a pin. The rake (I recommend the snake) is inserted in the keyway and 'raked' across the keypins until the bound pin sets. As more pins set, the torque will need to be increased to hold the set pins and bind the final pins.
- Torque needs to be regulated such that it is enough to bind a pin and hold the set pins but not so much that the bound pin can not be pushed up to be set.
- Raking should be done so that the rake can 'bounce' across the keypins. Pressure on the pins from the rake should be from the wrist not the fingers or arm.
- Pressure needs to be regulated such that it is enough to push the drive pin to the shear line but not so much that it pushes the keypin into the hull.
- It may sound complicated but, after a few tries you'll get the feel of the torque Vs. pressure technique required to set the pins and open the lock.

Hints and Tips

- **Getting Frustrated**
 - Each lock is different. Even the same make and model. Even the same lock from day to day. Each lock will require a different combination of torque and pressure to successfully pick. Practice and experience is the only solution. If you get some pins set but can't get the last few, release the torque and start again. Try to 'feel' the process of setting the pins and 'picture' the mechanics in you mind - Zen is your friend.
- **Which way to turn**
 - It's 50/50. Usually the wrong way has a hard stop and feels that way. The right way pushes against the pins and feels 'squishy'. Cheap padlocks will open when turned either way.

Hints and Tips (cont.)

- **Loose Plugs**
 - Cheap locks may have loose plugs. Often, desk and file drawers. (I've actually had plugs fall out into my hand) Some times you can use this to your advantage. Pushing and pulling on the plug may help in setting the pins.
- **Over Rotating**
 - Most locks open with a turn of less than 180° some require more. Be careful when rotating 180° or more, the drive pins may fall into the keyway and ruin the lock.

Hints and Tips (cont.)

- **Spring held Drawers**
 - Some Desk Drawers and File Drawers require that you push the drawer in against a spring to lock them. Some are locked by pushing the hull in against a spring until it locks. Often, the force from this spring requires extra torque to turn the plug making it more difficult to pick the lock. If possible, relieve the extra force by pushing the drawer or hull in against the spring while picking the lock.
- **Car Doors**
 - While car keys look like they are for double sided locks often they are not. The keys are just made that way so you don't have to think about which way to put them in. Most car locks can be picked just as easily as any other lock.

Hints and Tips (cont.)

- Master Key Locks
 - Master Key locks are a type of lock where several different keys can open the same lock. For example, your key only opens your hotel room door but, the cleaning crew has a single key that can open all the rooms on your floor. While many hotels are going away from mechanical key locks they can still be found at some hotels and in the office. Effectively, the pin has two (or more) positions at which it can be at the sheer line. Since you only care about getting the pins to any sheer line these types of locks can increase your chances (or speed) of picking them.
- Buying Pick Sets
 - Most ‘Spy’ Stores will carry pick sets or they can be ordered through ‘Military’ or ‘Adventure’ magazines. Go for the smallest set. (Even though I have a fifteen piece pick set, I only use about three tools from it.)

Thoughts on Lock Picking

- “Only Criminals Pick Locks”

- I can’t imagine why any average criminal would want to learn how to pick locks. Lock picking is a skill that takes practice. A sledge hammer or crow bar is a much faster and more effective way to open any door, window or desk and requires very little skill. If you care so little about others to steal something then why should doing damage bother you?

- “Locks Keep Honest People Honest”

- By now you should realize that picking locks is fairly simple. So, why do we use them at all? It’s a deterrent, even if it is more a mental one than a physical one. While an honest person probably won’t take your CDs if they are inside a locked car they might be tempted to take them if the car was obviously not locked. Someone with true criminal intent wouldn’t think twice about the lock.

References

- MIT Guide to Lock Picking by Ted the Tool
 - Excellent. On the Web in various formats
- The Alt.Locksmithing FAQ
 - Alt.Locksmithing or your favorite FAQ archive.