CHAPTER

More about locks and ways to low tech hack them

3

INFORMATION IN THIS CHAPTER

- A Little More about Locks and Lock Picking
- Forced Entry—And Other Ways to Cheat!
- Let's Break into a Semi–High Security Room
- Keys and Key Control
- Bait and Switch War Story That Could Happen to You
- Some Places to Go to Learn and Have Some Fun
- More about Keys and How to Make One If You Don't Have One
- Ways to Make a Key If You Didn't Bring a Key Machine
- One Final Lock to Talk about and Then We're Done

As I was preparing to write this chapter, I found myself thinking back over the past 45 years of my life. I consider myself one of the most blessed people on the planet when I think about all the things that I've been able to do and learn. I became somewhat of a techno geek while attending vocational-technical high school back in the mid-sixties. I've found electronics to be absolutely fascinating. In my senior year I was able to design a variable-speed (computerized) control for a synchronous motor using a handful of transistors. It was considered by the school to be their first computerized control of an AC synchronous motor. When I visited the school about 10 years later, I was pleasantly surprised to see that they were still using the training manual that I had written describing how to construct this computerized control. It had taken me weeks to figure out how to do this. Using the manual, a new student could learn how to do it in less than an hour. In a sense, all of my time spent on experimenting, designing, and working with these transistors was pretty high tech, but it became a low tech process for the people who had the manual in front of them describing how to do it. This is exactly what happens with just about everything that starts off high tech it becomes fairly low tech to implement or exploit once you know how.

© 2012 Elsevier Inc. All rights reserved.

A LITTLE MORE ABOUT LOCKS AND LOCK PICKING

"What in the world does this have to do with locks?" you might be asking yourself. As I reminisced a little more, I remembered my return from Vietnam in the late 1960's (not 1860s like some of my friends think - I know - I'm old!). I had always enjoyed the physical security world, but I'd still had a tremendous interest in the worlds of technology and technical security. Shortly after returning from Vietnam in the early 70s, I decided to become a locksmith. After completing about 6 months of training I had an opportunity to purchase half ownership of a locksmith shop in Baltimore. I learned a lot during the few years that I worked as a locksmith part-time. One of the things that I learned that greatly impacts some of what I'll be discussing in this chapter is that locks don't change very much. Most of the types of locks that I worked on 45 years ago are still in use today. Many of them had been used for decades before I became a locksmith. The difference between locks used in the physical security world and the current world of technology fascinated me. I've been saying this during presentations for years, "regarding technology, if you can buy it, it's obsolete". Over the years I have continuously said "The biggest potential problem with technical security is a lack of proper physical security." Throughout this chapter I'm going to be talking about a few things concerning a few types of locks that have existed for over 100 years, as well as some suggestions for ways to improve our knowledge of what makes a good lock versus a not-so-good lock. I hope you will learn a few things along the way.

WARNING

Please keep in mind that conducting any of the activities mentioned in this chapter on locks you do not personally own could very well be illegal. If you are a paid penetration tester, conducting an inside penetration test, you need to be sure that you have permission from the company that hired you to use this form of attack. My main reasoning for even discussing any of this is to make people aware of the possibilities of things that the bad guys can do, should you let them into your building. This is why for 20+ years, I've been preaching about the need for increased physical security to prevent access to these critical resources in the first place. I personally would not suspect that most inside penetration tests would go to this level of testing. You wouldn't be testing the ability to do this to a lock as much as you would be testing your social engineering ability to have someone open that door to let you into the room to be able to conduct this attack. As I've mentioned several times throughout this book, once we were inside the buildings it was assumed by everyone that we came in contact with that we belonged there.

As with many of the things I write, this chapter will have an interesting flavor of risk management. Just what are the risks, threats, vulnerabilities, and countermeasures that we should consider when looking at the locks in our homes as well as at work? Another statement that I have been making for years regarding security in general is that if there's a discussion of a certain situation on YouTube, you had better know about it. If it's on YouTube, you can bet that all of the people that want to exploit it have probably already seen it.

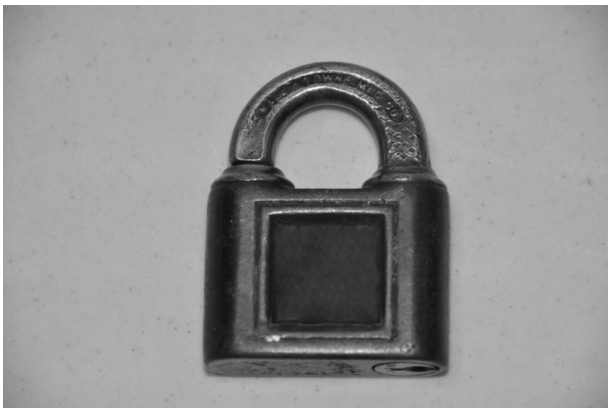

FIGURE 3.1

My 110-year-old lock: eBay, $3

Figure 3.1 is a picture of the oldest pin tumbler lock that I own. On the bottom of the lock, there is a patent date of 1901. This is a pin tumbler lock very much like the locks in most of our homes. I tried for quite some time (unsuccessfully) to open it. As you will see a little later in the chapter, it can be picked open. I have had some fairly sophisticated lock picks for decades. As with anything else in life, practice, practice, practice is the only way to stay good at just about anything. Unfortunately, I don't practice very much with my lock toys any more because of other time commitments. I still have several hundred locks in my collection and find each one to be a very interesting puzzle. I'll also be recommending a few places to go and a few books to learn a little more about these cool mechanical devices. It is very encouraging to me to see more and more (mostly young) people begin to take up lock picking and lock knowledge as a fun hobby. Even mentioning lock picking as a hobby is a fairly new thing for me. For years the inner workings of locks were considered the secret things of locksmiths and lock manufacturers. I've always been one to not necessarily agree with that need for secrecy. My feelings have always been if the bad guys of the world are aware of certain things including vulnerabilities, the good guys need to be aware of them as well. I want to say this once again, because I think it's critically important. If there is a vulnerability that's explained in detail on YouTube and other places on the Internet, you and whoever is in charge of security for your organization had better know about.

WARNING

Possessing lock-picking equipment is not legal in some states. If you intend to pursue lock picking as a hobby, or as a part of conducting your own "official" penetration test, you still need to be sure that you are not breaking the law in any way by making or using these tools. Laws and restrictions about owning and using lock-picking equipment vary greatly between states, counties, and cities. In some locations, it is a crime to use your lock picks to open your neighbors' home, even upon their request, if they lock their keys inside and ask you to help.

Continued

WARNING—cont'd

As with almost any subject today, there is a wealth of information regarding the legal issues associated with lock picking available on www.google.com by entering "are lock picking tools legal to own" or something similar. Another link showing information on this subject is http://www.lockwiki.com/index.php/Legal_issues, which shows the current requirements in all fifty states as well as a few other countries. Another website with a little more detail regarding the laws of each state is http://www.lockpickguide.com/legalityoflockpicks.html.

The bad guys' that I collectively refer to throughout this chapter most likely won't care if they are legal or not, but you need to care!

What kinds of locks are the most popular?

In many ways, locks are the hardware versions of the passwords and authentication devices that we use to gain access to our computers. They are also what I like to call the low-hanging fruit of your perimeter security. Unfortunately, many times, they are the devices on which we spend the least amount of money (including in our homes). I'm going to try to convince you to spend a little more money for a whole lot more protection when selecting locks for your office or home.

In preparation for this part of my chapter, I wanted to see what kinds of locks people typically purchased for their personal use. I do a lot of people watching while I'm out and about. It's fascinating. Last fall, as I was looking around at the locks available in different stores, I watched as several people came over to the area where the locks were displayed and quickly picked up a lock or two for school. Most of them chose an inexpensive brand of combination lock that has been a standard for decades. That didn't surprise me, and in most cases, it is the required lock for the lockers in many schools. I also watched as several people purchased padlocks with keys. What every one of them did wasn't a surprise either—most of them purchased the CHEAPEST lock that they could find. I watched this over and over again. Little do they realize that they got what they paid for.

For those people who didn't purchase a combination lock, most of them picked up either a cheap pin tumbler padlock as shown in Figure 3.2, or a warded padlock as shown in Figure 3.3, none of which costs more than $5. The keys for these two types of locks are shown in Figure 3.4. The key on the right is the warded padlock key, and the key on the left is the pin tumbler key. These locks looked as strong as the better locks on the outside. Anyone who knows even a little bit about locks knows that these less expensive locks are just going to keep the honest people honest. They are not high security locks. How about a quick lock awareness war story to give you an example of how easily the wrong type of lock can be bypassed:

NOTE

Our penetration team had been inside the building of a customer who had hired us for about 4 hours when we came across a row of file cabinets that must have contained some important documents. There were about ten tall file cabinets in a row, and each of them

had a vertical bar attached to the cabinet with a padlock securing the bar to the cabinet. This was more security than we frequently saw on these kinds of cabinets.

When we were working on the inside of a building (after social engineering our way in), we tried to look at everything that we thought could be a vulnerability. I took the time to quickly examine every lock on these file cabinets. It wasn't surprising to me to find one that looked the same as the others on the outside, but was drastically different on the inside. Someone had replaced one of the pin tumbler padlocks (Figure 3.2) with a warded padlock (Figure 3.3). In less than 10 seconds, I opened the warded lock, taped my business card on the INSIDE of the file cabinet to prove that we were there, and closed the lock again. The bad guys could have gotten to the entire content of that file cabinet just as quickly. Warded padlocks are among the oldest lock designs in existence. A skeleton key capable of opening many hundreds of locks can be created by filing down some of the bittings on any key for one of these locks.

Why was this one lock different from the rest of them? I suspect that someone either lost the key to the original (slightly more secure) lock or lost the lock itself. If that happened, they could have simply gone to the hardware section of their local store and purchased a lock that looked like the rest of the locks on those file cabinets. If they went with the mindset of most people that I watched purchase locks, they would have purchased the least expensive lock that they could get as long as it looked as strong as the original lock.

Let's take a look at a few types of locks to help you learn which ones are more secure than others: Figure 3.2 shows a pin tumbler padlock. It's the exact kind of lock that we saw on most of the file cabinet where padlocks were used in buildings that we were pen testing. Pin tumbler locks are also the most common type of lock that we see in homes and office buildings on doors. These locks can be picked with a little practice.

The warded padlock that we found on a file cabinet during one of our pen tests looked about the same as the more secure pin tumbler padlocks, but it had a different keyway, as seen in the lock shown in Figure 3.3.

FIGURE 3.2

Pin tumbler padlock

FIGURE 3.3

Warded padlock

I was able to open this one (Figure 3.3) in less than 10 seconds, and you could too. Opening locks like this one isn't even lock picking in my opinion. The pick sets for these are more like master keys. A simple pick for warded padlocks like this one can be made by simply filing down all of the bittings as shown by the arrows in Figure 3.4.

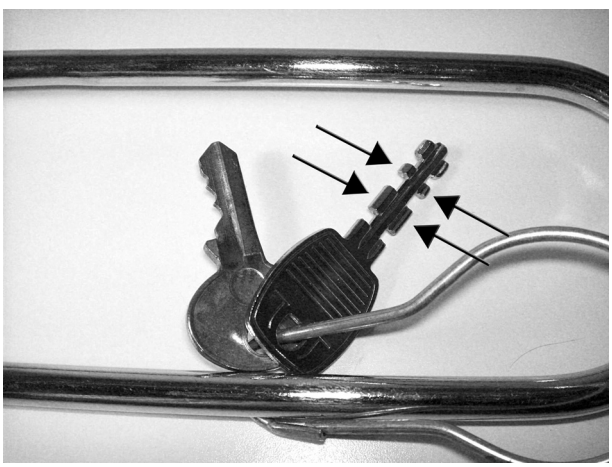

FIGURE 3.4

Pin tumbler and warded keys

Purchasing better quality locks will be cost effective

So, are there any padlocks that are reasonably secure and not terribly expensive? My favorite has always been a lock that looks a little different but has a lot of leave-me-alone features. One of my favorites is a lock made in Germany and it's quite secure for its price of about $25. It's the pin tumbler lock shown in Figure 3.5 with all five of its pins being mushroom-type driver pins. Mushroom pins are shaped somewhat like an hourglass. This shape can cause the pins to bind as someone attempts to pick them.

While I don't consider this lock to be maximum security, it is considerably better than most of the inexpensive locks that I see out there. This is the type of lock that you will see on about 90% of the storage facilities that allow you to use your own lock. It is a pin tumbler lock and does offer a few additional security features. First, it would be more difficult to attack with bolt cutters or even a hacksaw. You can't see it by looking at this lock, but this lock also offers something that I really like called *key retention*. What that means is that while the lock is unlocked, you cannot remove the key from the lock. The key is retained in the lock until it is secured again. When I remove the lock from my storage location, I immediately place the lock in my pocket with the keys still in the lock. That same keychain also contains the keys to just about every other lock that I need access to. With a huge lock in my pocket I am very unlikely to attempt to start the car as I leave the storage area without seeing this monster hanging on the key ring. With the key retained in the lock whenever it is unlocked, I always know that, if the key is in my pocket with no lock attached to it, the lock is locked somewhere, hopefully back on my locker at the storage facility. I can't tell you the number of times that I returned to a storage facility that didn't use this key retention process to double check that I had really locked the door. I've always liked key retention type locks for that very reason.

FIGURE 3.5

Disk-type pin tumbler lock: eBay, $15

Let's consider a couple of other features of this lock. In addition to being difficult to remove by pure force, it contains pins that are mushroom shaped. These are much more difficult to pick than standard pins. There is something else that I've watched develop as more and more locks are manufactured. I've begun to see a number of locks that look very much like this one but aren't designed with anywhere near its quality. This lock retails for around $25. There are versions of this out there that retail for as little as $5. As we've all heard many times throughout life, you will definitely get what you pay for.

Be aware of lock vulnerabilities

There is one vulnerability for this type of lock that is all too common. I have incorporated my own countermeasure in an attempt to prevent this from happening to me. As I look through the complex of this storage location I see every one of the locks like this placed on the HASP (the device on the door where the lock is placed) the same way that I had placed the one in the photograph. The keyway where you would insert your key is open for easy access. In my mind, a lock placed in this position would be most vulnerable to drilling. This is an old/new threat that is now much easier to use with the advent of battery-powered drills. In the 70s when I started as a locksmith we didn't have battery-powered drills. If we couldn't get to a location where power tools were needed, we would have to come up with a generator or some sort of auxiliary power from our locksmith van. Things have changed! Very powerful battery-operated drills are now available everywhere. If I can get to that keyway and begin to drill out those pins, thereby creating what's known as a *shear line*, I will be able to retract that bolt and remove the lock. The lock would certainly be destroyed, and there would be evidence of forced entry, but the contents of the storage shed (or whatever else was being secured by the lock) would most likely be gone. I'll be discussing drilling again later as we talk about a few other issues with locks. For now, let me show you what I did to slightly change this vulnerability for my lock on my storage facility. Let's take a look at Figure 3.6.

At first glance, this looks like the same picture as the photo in Figure 3.5. It is but with the exception that the keyway is no longer in the same vulnerable position. Doing this doesn't completely remove the threat of someone coming along with the battery-powered drill and drilling out the keyway. What it does do is make it much more difficult for someone to be able to do that. The space between the keyway and the side of the building frame is now only a couple of inches. For me, that makes it just a little bit more difficult to get my key into the lock. It also makes it much more difficult, even with a fairly small battery-powered drill and short bit, to be able to easily drill out that lock. The bottom line is that my lock is now a slightly tougher target than most of the rest of them in that complex. As a fun exercise, one afternoon I drove through the complex looking at locks that people used. I didn't find any of them that have made the changes that I did to make it more difficult to drill. What I did find really didn't surprise me either. I saw countless locks that I'm sure cost no

FIGURE 3.6

Lock turned 180 degrees

more than $3 to $4 that people would put on their storage containers obviously full of valuable material to them. It just continues to amaze me after 40+ years of dealing with this that so few people really understand the vulnerability of these very inexpensive locks. I have always tried to use the best available security for whatever I was trying to protect. In some cases that required a very expensive lock or vault or safe. In other cases, like the entrance to my home crawlspace where there is little of value, it might not be necessary to have an incredibly expensive lock. I see this time and time again in homes as well as in industry where we were conducting penetration tests, that these devices were just misunderstood. In many cases people could spend not even twice as much as they currently spend on locks and get something considerably better and more secure.

TIP

We're going to dive a little deeper into some of my thoughts on locks as we go through this chapter. I do want to encourage you to consider purchasing Deviant Ollam's excellent book titled *Practical Lock Picking*: *A Physical Penetration Tester's Training Guide* (ISBN: 978-1-59749-611-7, Syngress). It's an excellent book, and Deviant is well known in the industry as a person actively pursuing the hobby of lock picking. I own the book and I find it excellent for a number of reasons. Deviant has a unique knack for explaining with drawings exactly how certain types of locks work. Some of the things that I will be covering in this chapter and the rest of the book will be my thoughts, experiences, and opinions concerning locks and bypass methods. These fascinating mechanical devices will play an important part at our homes and at work well into the foreseeable future. The lack of knowledge, or even a basic understanding of locks and the way that they work, has surprised me throughout my career in security.

FORCED ENTRY—AND OTHER WAYS TO CHEAT!

Unfortunately, getting past whatever is keeping a certain door cabinet or window locked often causes damage. Even picking a lock with spring steel picks rubbing against brass pins can cause some damage. Sometimes the good guys, and most of the time the bad guys, could care less about this potential damage. I want to talk a little bit about the vulnerability of forced entry. As with most things concerning locks, these vulnerabilities are not new. If we look at any door as an example, and want to simply get it to open, there are a number of ways to do that. In emergency situations, the good guys will do whatever they have to do to get through that door. Let me show you a picture of a typical rim cylinder lock that would control the dead bolt lock on a typical door (Figure 3.7). This could be a door at an office or at your home.

For a rim cylinder lock, this one is very high quality. The weight of the lock is not always an indication of quality, but usually a very lightweight lock will not be as strong as a stainless steel or an all-brass high quality lock. The serrated copper-looking piece sticking out the back of the lock is the tailpiece. When the key is inserted, and all of the pins are at the proper shear line, the plug will turn, which will turn the tailpiece and retract the bolt. This sounds like a simple process, and it is. That tailpiece is inserted through a mechanism that turns the bolt and retracts it from the strike in the door frame. When I'm asked the simple question, "What allows the door to be opened?," I answer by saying, "The retraction of the bolt is what allows the door to open." We'll take a look at the bolt in a few minutes. The important point here is that the bolt itself is retracted by the movement of the tailpiece. If the lock cylinder and the tailpiece were not there, a simple screwdriver would easily act as a tailpiece to turn the mechanism to retract the bolt.

FIGURE 3.7

Rim cylinder lock with keys and mounting plate: eBay, $4

In Figure 3.7, there is also a silver piece of metal with two screws sticking through it. This is the mounting plate. It would be located on the inside of the door and the screws would be fastened to the back of a lock through the holes in the mounting plate and into the threaded holes in the lock body. This is the way that most rim cylinder locks are installed in our homes. The potential weak point in this construction is the two holes in the mounting plate. Most of the mounting plates for the locks in my collection are made of fairly soft sheet metal.

A time-tested low tech method of forced entry

At first glance, this is going to sound like cheating. I have on occasion had the need to get into a house very quickly without a key. This was when I was a practicing locksmith years ago. This low tech way of entry was often used in emergency situations where someone's life was in danger. If a bad guy was exploiting this form of entry, it would certainly be considered forced entry. (There are YouTube examples of this vulnerability as well.) I am sharing it to let you know that anyone with access to the Internet could now know how to do this. As I will continue to say, if it's out there on the Internet, you had better know about it. Just enter this into your favorite search engine: "How to use a dent puller to remove an auto ignition lock." The dent puller that you will see described in a number of places on the Internet is what we refer to as a *slide hammer*. The one that I have weighs about 3 pounds and has a drill chuck on the end of it (Figure 3.8). This has one of those case-hardened screws in the drill chuck. This method of forced entry could be used to remove a lock cylinder in an automobile or in a home or business. With the rim tumbler lock such as shown in Figure 3.7, it would be a simple matter of twisting the screw directly into the

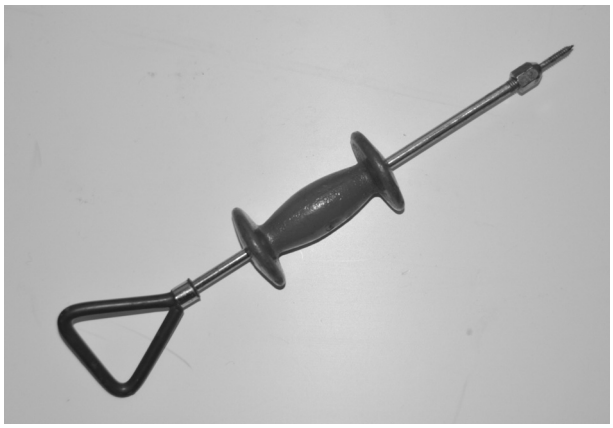

FIGURE 3.8

Slide hammer: flea market, $10

keyway of the lock and sliding the weight on the slide hammer back heavily several times. The entire cylinder and tailpiece came out every time that our locksmith team needed to use this forced method entry over 40 years ago. This is not a new vulnerability. With the tailpiece removed, it would be a simple matter to place a screwdriver into the lock and retract the bolt. As I said earlier, what allows the door to open is the retraction of the bolt. It really doesn't matter to the door how that happened. In this case it happened with forced entry.

There are a couple of countermeasures that can make this exploit a lot more difficult. In my locks at home, I installed a small steel washer between the head of the screw and the mounting plate. Doing this would require a lot more force to remove the cylinder. I'm not going to say that this would prevent the cylinder from being removed, but it would make it a lot more difficult.

Another countermeasure would be to construct or purchase a steel mounting plate. If the mounting plate were considerably stronger, the physical strength of the screws would then be the weak point.

If our concern is the wrong people getting into our homes or buildings, we really do need to understand the strengths and weaknesses of the devices that we used to prevent that. This is also why I like to see a number of books on the subject of locks, lock picking, high security locks, and bypass methods. We just can't defend ourselves against things that we don't understand. I always enjoy removing the mystery.

TIP

I'd like to mention a few of the books that I personally have in my library on the subject of locks and lock picking.

- *Practical Lock Picking: A Physical Penetration Tester's Training Guide*, Deviant Ollam, ISBN: 978-1-59749-611-7, Syngress

I really like Deviant's book. I wish I had his talent for creating those excellent drawings. He explains exactly what's going on inside the lock predominantly for picking. This is what most people are interested in as a hobby and I think that's excellent. I've been saying this for years: the more that people know about locks, the more likely they are to choose a good one for the things that they are trying to secure. If you are going to buy your first book on lock picking, get Deviant's book.

- *The Complete Book of Locks and Locksmithing*, Sixth Edition, Bill Phillips, ISBN-13: 978-0-07-144829-1, McGraw Hill

This 588-page book is a classic in the world of locksmithing. This book covers the history of locks, the tools of the trade, types of locks and keys, and a number of other interesting topics should you decide to get into the field of locksmithing. It's a fascinating field that I have been dabbling in for over 40 years.

- *High-Security Mechanical Locks: An Encyclopedic Reference*, Graham W. Pulford, ISBN: 978-0-7506-8437-8, Butterworth-Heinemann

This is one of the most detailed books by Elsevier that I have ever seen on locks. At just over 600 pages, it goes into great detail about the subject of high security locks. I enjoyed his discussion of warded locks all based on the type of lock that I show in Figure 3.3. Some of the warded locks that he describes are over 700 years old.

- *Open in Thirty Seconds: Cracking One of the Most Secure Locks in America*, Mark Weber Tobias, ISBN: 978-0975947920, Pine Hill Press

I've known Mark for several years, and he is one of the most respected high security lock specialists in the world. This is an excellent book on the history of conventional as well as high tech locks to include some of their vulnerabilities. There's not another book out there quite like it, and I highly recommend it.

- *How to Open Locks with Improvised Tools: Practical, Non-destructive Ways of Getting Back into Just about Everything When You Lose Your Keys*, Hans Conkel, ISBN: 978-0966608717, Level Four Publications

This is an interesting book that I picked up a couple of years ago. It addresses interesting low tech ways to get into just about everything you can think of. I've not tried all of these myself, but it does look like most of these bypass methods would work. The one that I find the most interesting is the discussion of a bypass method for a very common knob set like you would find in your home. I do know that the procedure described in the book works, because I used it myself as a working locksmith. The interesting part about this bypass method is that it is completely nondestructive and just about as fast as using your key.

LET'S BREAK INTO A SEMI–HIGH SECURITY ROOM

The scenario that I'm about to describe is one that I used many years ago to gain easy access to a room over a several-week timeframe. The target room of interest was secured by a high security lock. My goal was to find a way into the room the first time and then establish a means to get back into the room fairly quickly on additional visits during our penetration tests for clients. The process that we used involved a little bit of social engineering, a little bit of locksmithing, and a little bit of ingenuity knowing how this particular lock worked.

This combined process is why I like to see people learn more about locks. It can be challenging to come up with countermeasures for some of these exploits. You'll see what I mean as we go a little deeper into the process of gaining control of this lock.

The lock shown in Figure 3.9 was rather expensive considering many of my other purchases. It was originally a display model for a very high security lock. Buying a lock like that gave me an opportunity to see exactly how locks of this type work and how they were installed. Most of the new lock enthusiasts that I've met buy as many things on eBay as I do. As I've said several times throughout these chapters I highly encourage people to begin to learn more about locks and how they can be compromised. This lock is a dead bolt type of lock similar to what you probably have on your doors at home. Those doors at home have two locks. One of the locks is typically a key-in-knob lock where you place your key into the doorknob and rotate the plug to retract the bolt. This bolt will be spring-loaded, which will allow you to open and close the door by simply turning the doorknob. The bolt on the lock in Figure 3.9

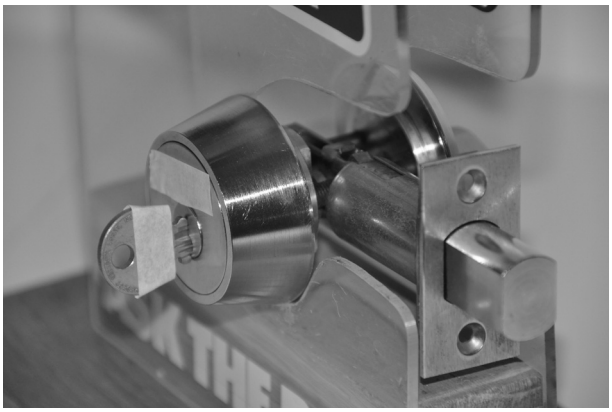

FIGURE 3.9

High quality high security lock: eBay, $45

is a dead bolt that needs to be manually retracted with the key from the outside or with a thumb latch from the inside to retract the bolt. If you had the opportunity to hold this lock in your hand, you would be amazed at the quality of the craftsmanship and the physical weight of the lock. It is an expensive lock, but you are definitely going to get what you pay for. Most of the locks in your home will not be of this quality. That doesn't mean that they're not good locks; it's just that most people do not put locks that cost hundreds of dollars each in their homes.

Retracting the bolt to open the door

Let's talk about how a bolt actually retracts. Remember what I had said earlier: the door is allowed to open when the bolt retracts. To open this very high security lock shown in Figure 3.9, you need the correct high security key if the lock is working properly. There may be other ways to open it by retracting the bolt. This is where a little bit of social engineering came into play during one of our pen tests as we needed to get into the room being secured by a lock similar to this. Who in the building would have the keys to that room? As our pen testing team found time and time again, the people whose job it was to keep the building neat and tidy frequently had the keys to everything. In almost every case it was simply a matter of looking like we were supposed to be there and needing a favor. In a few sentences, I'm trying to describe something that may have taken several days and multiple visits: which was to gain the trust of the right people who had these keys. This was always the case with social engineering and inside penetration tests. Once we were inside the buildings, almost everyone that we came in contact with eventually believed we should be there. Their guard was down. Over the years, the thought of how easy it was to get into most buildings has bothered me. There have been many studies about how intellectual property becomes compromised. Unless someone was caught inside

your building, you may not know they were ever there. To the best of my knowledge, very few people who saw us during the penetration test even remember that we were there.

I'm not going to describe the social engineering story that we used to convince them that we needed to get into that room. Once they opened the room and gave us a little bit of time, we were able to determine exactly which locks were used on those doors. The lock shown in Figure 3.9 is similar to the locks that we found on the doors in these buildings. It is an excellent lock for me to show you the mindset of penetration testing using a multi-entry attack. I found it very interesting over the years that for some reason multifaceted attacks seem to really throw people off guard as to your intent. I believe that most people would have fallen for the attack I described in the social engineering chapter where I made two phone calls to that medical group. Both calls seem so innocent, and yet when you combine them they lead to a devastating effect. This seemed to be the case with dealing with locks and entry through doors in most of the buildings that we were targeting during our pen tests. If we could determine the keyway of the lock being used, we could normally obtain key blanks for that exact keyway. The portable key machine that I purchased at a yard sale many years ago was very accurate. I used it on several penetration tests to reproduce the building master keys after we were able to use our social engineering skills to borrow the keys from someone in the building who had access to them.

After figuring out how the lock in Figure 3.9 works by spending a few minutes studying it, I was able to devise a low tech hacking means of defeating the bolt mechanism. Since this was a dead bolt, I didn't have any springs or deadlocking plungers to worry about. Notice that I said defeating the *bolt* mechanism, not the *lock* mechanism. Figure 3.10 shows what I came up with as one way to low tech hack the bolt.

I had to borrow our dining room table to take a picture of this because it was almost invisible on my standard white background. I needed to make something fairly

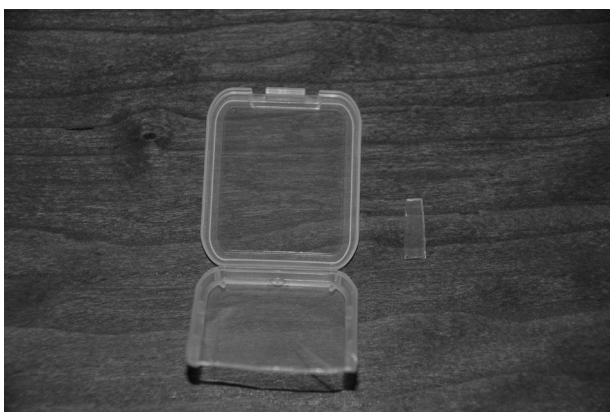

FIGURE 3.10

Jack's low tech bolt hacking tool: free

stiff and about a 1/32 of an inch thick. I began cutting up a plastic flash drive case that looked to be about the right thickness. The only piece that I wound up using was that small clear piece to the right of the picture. In seeing how the bolt operated in the lock in Figure 3.9, I noticed that if I stop the bolt from traveling that final 1/8 of an inch, the bolt would appear to be deadlock, but it wasn't. If I allow the bolt to go into full deadlock by completing that final 1/8 of an inch travel, the lock could only easily be opened with the key on one side or the thumb latch on the other. Obviously with the door closed, I wouldn't have access to the key on the outside of the door or the thumb latch on the inside of the door. With the dead bolt not properly engaged because of my improvised small piece of plastic, and depending on the tolerance of the door in the doorjamb, I might be able to get a very thin fingernail file or something smaller into the opening to begin retracting the bolt. This would be much easier to show you than it is to explain. If you look at your locks at home from the inside of your home you will see what I mean. Most homes are constructed with a fair amount of an opening between the door and the door frame. I have found deadbolts on doors that had no protection against using a thin knife or a fingernail file slipped between the door and the door frame to retract the bolt. I know I've said it before, but I'll say it again. What allows the door to open is the retraction of the bolt.

Gaining access to the lock itself

Please keep in mind that this is just an example of one quick way to defeat the lock. In order to be able to get this small piece of plastic into the lock mechanism, it would be necessary to temporarily remove the lock from the door. This can be done from the inside, especially considering the inside faceplate of the lock is only secured to the door with several screws that are accessible from the inside of the door. This brings up another good point about the things that we experienced during our inside penetration tests. Every time we started the test, especially when we were in the process of getting into the building, we always felt like we would immediately be caught. Once we were in the building, that feeling of possibly getting caught continued for a while. It didn't take very long for our penetration team to realize that we could pretty much do anything once we were inside the building because people just felt like we belonged there. I'm still amazed at that. I'm convinced that in most places, if someone walked by while we were doing just about anything inside the building, we would go unchallenged. On one occasion we saw two people trying to move some equipment, and we stopped what we were doing and offered to help. They were most thankful and didn't even ask us our names, much less what we were doing there. Scheduled security awareness training would go a long way in helping to keep employees more aware of who should be challenged or at least reported if they are not recognized. Keep in mind that this company had already been a victim of theft, which is why we were hired to see where the vulnerability might exist in their operational security.

Figure 3.11 shows the lock with my little piece of plastic added to the top of the bolt. I didn't take the time to securely fasten it to the top of the bolt, but I did hold it

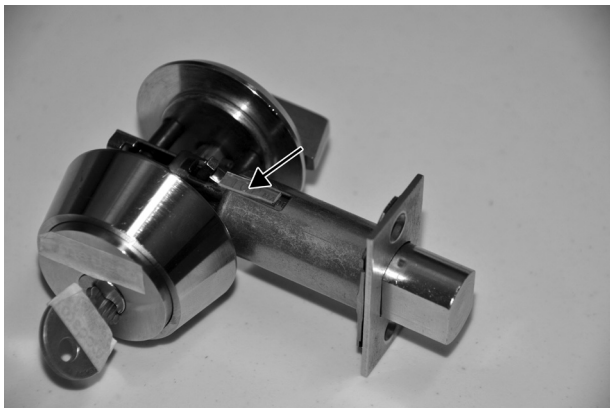

FIGURE 3.11

Jack's low tech bolt hacking tool placed in the bolt: free

there while I was experimenting with the bolt and saw that the piece of plastic did prevent the bolt from completely locking in place. If a device like this were installed in the lock permanently, the bolt could possibly be retracted with the small fingernail file or knife blade at a later time.

In Figure 3.11, you will recognize that little piece of plastic (indicated by the arrow pointing to it) sitting on top of the bolt on the left-hand side near the cut-out. That small piece of plastic prevented the final 1/16 of an inch of travel in the bolt that prevented the bolt from opening fully. I held the little piece of plastic in place and operated the lock with the key as well as with the thumb turn. In both cases it felt like the lock was locked. It even looked like the bolt was fully extended. Figure 3.11 shows it in the compromised position. That bolt is not securely locked open. With enough room between the end of the bolt plate and the strike in the door frame to get a small thin knife or fingernail file into the opening, the bolt can easily be retracted.

TIP

I'll say it again: the real vulnerability here isn't the keyway, and it isn't the quality of the lock or the solid stainless steel bolt. The real vulnerability in my opinion would be the ability to get to that lock and borrow the key to get into that room and then compromise it. Security is a very difficult ongoing task that every employee of every company needs to be a part of. Frequently when I'm out presenting at a conference, I'll ask the question, "How many of you are a part of your company's security team?" Considering that I'm usually speaking at a security conference, quite a few of the hands go up. I then say, "If you see me present again, and I asked that question, I would really like to see every hand go up." It takes all of us to create true security in our homes and in our workplace.

This quick scenario is really designed just to show that locks are in some ways like puzzles. That's pretty much how most of the lock enthusiasts that now pick locks as a hobby look at it. I think that's wonderful! The more that employees, and especially the security teams, know about locks, the more they can insure that the proper locks are used for given situation. They will also know quite a bit about ways to defeat these locks and possible ways to prevent that.

Here's one more quick example of things that we don't typically think of but that the bad guys just might. This example is going to use our same high tech lock shown in Figure 3.9. I've used this in several training classes just to describe a little bit about pin tumbler locks and ways to defeat them. After letting people in the class who wanted to examine and operate the lock, I asked if they noticed anything unique about it. So far, of all the people that have looked at that lock, no one has. This is another low tech hack that we would normally not think about when dealing with pin tumbler locks. This lock is designed in a very interesting way that allows it to pretty much feel the same if there are pins in the lock or if there aren't. In this case there are no pins in the lock. If you think about it, removing even a few of the pins from any pin tumbler lock makes it really easy to pick. If even one pin were left in a pin tumbler lock, that lock may well appear normal to anyone using their key to open the lock. I suspect the lock could exist like that for years until it was worked on by a locksmith or a building mechanic for some reason. What that would do is allow virtually anyone with even a little bit of lock-picking experience to pick that single- or even two-pin lock. Maybe I just think a little differently from some people, but I just don't think too many people ever think of these kinds of low tech vulnerabilities.

Over the years I've trained a lot of internal auditors on auditing physical and technical issues associated with security. I think it would be a good idea to occasionally audit the status of the locks within the building. This was something else that we found every time we conducted an inside penetration test. There always seemed to be at least one door that was no longer functioning properly. It was normally a key-in-knob-type lock or a pushbutton combination lock where the bolt would stick partially open. This would frequently be a problem with doors that were exposed to outdoor elements. Let me show you what I mean. Take a look at Figure 3.12.

I've been keeping an eye on this door for about 3 months now. I guess I've been looking at locks and doors for so many decades that I just can't help but do it pretty much everywhere. This is one of about 20 doors that secure entrances to a multi-tenant office complex. This is a perfect example of what our inside penetration team typically found at least once on every job that we did. These locks are mechanical devices, and in this case all of them are exposed to the outside elements. I found this lock in this condition on about a half-dozen occasions throughout the past 3 months. If the weather was extremely cold, or if we were experiencing a lot of rain, the lock (bolt) seem to fail and not close all the way. This is one of those maintenance issues that needs to be audited. Aside from this glaring problem, this is a pretty substantial door. It contains security glass and a pretty expensive pushbutton lock. Seeing that exposed bolt

FIGURE 3.12

Door to a secured office complex

that was supposed to retract into the lock and then spring back open once the door was closed is a very open sign that security has failed. You can't see it in this picture, but stenciled onto that door in fairly large letters is a sign that reads "Please be sure that door is closed behind you." I'm not saying anyone was at fault here for going out the door without making sure that it was locked. That's just not something that the typical person would do. They expect it to close and automatically lock like it does every other time. It's also possible that the person who went through the door is still on the inside, not knowing that the lock did not lock behind them.

This office complex is fairly large and is used by hundreds of people. On several occasions I have seen the doors to inside secured areas such as this one propped open. This was the case when someone obviously had a number of things to take into or out of the facility and just decided that it was too much trouble to continue to unlock the door. On at least one occasion, I saw one of the doors that was propped open on successive visits spanning several hours. In this case I suspect that whoever propped the door open just left and went about their business, and when they were finished, they didn't bother removing the board that they used to prop the door open.

None of these security issues is rocket science. It's just that we seem to have become a nation that isn't as careful as we should be about simple matters of security. Many of the inside penetration tests that our teams conducted were contracted because the organizations were suffering serious loss of intellectual property. The situation with locks in large buildings is one of the areas where I like to see all employees become involved. They don't have to know a lot about locks, but they can be trained to immediately report any locks that they feel are not working properly.

KEYS AND KEY CONTROL

The types of keys used in most buildings have remained virtually unchanged since Linus Yale invented them in 1861. Just about all of our homes and most businesses still use his pin tumbler locks for their primary perimeter defense. I have no way of knowing how often the master, grand master, and possibly great-grand-master key systems in buildings are changed. I do suspect that it's not very often because it can be an expensive process.

Social engineering and key access

While using our social engineering skills during each penetration test, our team always tried to make friends with the janitorial team. Sooner or later, we would need to ask a favor, and borrow their keys for a few minutes. Typically, their keys would open all of the doors on that floor and sometimes the entire building. A few minutes was all that it took for us to make a copy with the portable key machine that we brought with us in a small bag. Very few people have any idea of how the internal details of locks and keys work. Common knowledge of how locks work is another area of physical security that has changed greatly during the past few decades. When I became a bonded locksmith in the 1970s I found learning about the "secret things" about locks to be fascinating. Back then, I couldn't even purchase lock picks or key blanks until I graduated from a credited locksmithing school and had proper identification. Now, about 40 years later, we have much more at risk, and anyone can purchase lock picks at several local hardware stores or from the Internet without any questions asked about why they wants them.

Regarding the use of lock picks to get into buildings and rooms, I don't suspect that many pen testers use them. Lock picking does require a lot of practice, practice, and more practice, which is required for any pen testing skill. The easy availability of these devices is something that corporate security specialists need to consider as they plan their countermeasures.

Who has the keys to your kingdom

I'll be mentioning a few things about key control throughout this chapter. It is absolutely critical that you know who has the keys to your kingdom. This is another situation where the risks are very similar at home and at work. When I train senior executives and even law enforcement agents, I always encourage them to change the locks on their homes if they suspect anyone has compromised one of the keys. When you first move into your home, even a newly constructed home, you have no idea who has copies of those keys. Keys are the hardware equivalent of passwords, except that they are normally much more difficult to change. If you aren't absolutely certain that no one has been able to duplicate your keys, you should consider purchasing new locks, or having the combinations (pins) changed on your current locks.

TIP

Attempt to set up some form of key control if you don't already have a system in place. It is very important to know who has the keys to your kingdom as well as how many doors can be opened by each key. It is very seldom a good idea to have one key that opens everything in the building. That may be more convenient for certain things, but it does open the security concern of controlling who has those keys and how easily they can be duplicated.

Master keys are an additional concern if you rent space in a large building or office park. You might have a very strict policy of your own for your company, but if the management company that handles the building rentals isn't as careful with their master keys, the entire building could be at risk. Unless the keys are of a high security design like the Medeco line, they can be duplicated anywhere. Even if the disgruntled building maintenance person turns in his or her keys upon being fired, there is no way to be sure that copies weren't made. You should ask the building manager about the corporate policy regarding issue and security of the master keys.

For certain high value (to you or your organization) areas, it might be wise to install special locks on critical doors. Highly pick-resistant Medeco locks are some of the most effective. In addition to providing additional security, they add another level of due diligence should you need to document your attempts to prevent intrusions.

Special key control awareness training

Conduct special employee awareness training for everyone who works on the evening and night shift. That's when I took our team into the pen testing clients' buildings most of the time. We used our social engineering skills to befriend these people, and to the best of my knowledge, our being there was never reported by any of them.

Another prime target during our evening and night visits was the janitorial team. The main reason we always tried to befriend the people on the janitorial team is that they usually had those important keys that we were trying to get our hands on. These are some of the most important people in your company when it comes to protecting your buildings when most people are gone. They spend some time in just about every room in the building each week. If you don't train anyone else in your company, these people need to be well trained in how they can help. They should be made aware of your security policies and what they should do if they see anything suspicious. This would include strangers asking to have any doors opened, suspicious packages, doors that are opened that should be locked, etc. The members of the out-of-hours janitorial team are some of your most valuable resources. Tell them that, and teach them how they can help.

BAIT AND SWITCH WAR STORY THAT COULD HAPPEN TO YOU

I'd like to share a war story with you that happened to a friend of mine and it involves one of his locks. This friend was exercising at his local gym when this happened. He completed his exercise routine went to the locker room to take a shower. When he returned from taking a shower, he seemed to have a problem.

The combination lock that he had been using for years no longer opened. He tried it many times and it just wouldn't open. Consider the situation: he's standing there in front of his locker wearing a towel. Everything else that's important to him is inside the locker. If this happened to you, what would you do? Obviously, you can only try the combination so many times before you finally give in to the fact that it's not going to open. This has never happened to him before. Perhaps the lock was broken.

He and his towel obviously had to get some help in getting the lock opened. The manager of the gym wanted to be sure that this was really his locker before cutting the lock off. Without identification, the manager wasn't sure of what to believe. This was truly a Catch-22. If you think about it, the manager was confronted with an interesting situation. He has someone standing there asking to have a lock cut from a locker that the manager doesn't even know whether or not he has the right to open. In this case, the manager did finally go and get some bolt cutters and cut the lock off. To my friend's dismay, when they opened his locker, it was empty. Everything that he had in that locker had been stolen: his wallet, car keys, and some other very important items. As far as I know, law enforcement was immediately involved and the incident is still ongoing. Let's consider how the bad guy could have possibly used some low tech hacking to get into that locker. The bad guy also wound up using a little bit of low tech social engineering to place another lock on the locker that looked like the original lock. All of this bought the bad guy time to get away.

Figure 3.13 shows a lock that is virtually identical to the lock that belonged to my friend. There are several brands available of these combination locks, and they have remained unchanged for decades. This is perhaps the most common lock in the world. That doesn't make it a bad lock, but it does mean that more and more people are now beginning to realize ways to bypass the locking mechanism and cause it to open. I don't know how the lock was opened in the incident involving my friend, but I

FIGURE 3.13

Combination lock and a commercial shim

do know of several low tech hacking ways that these locks can be easily removed. Probably the most common way with a pair of bolt cutters. It's possible that this happened to my friend, but usually people walking around with bolt cutters might look a little more suspicious than others.

The little V-shaped item to the left of the lock in Figure 3.13 is a commercial padlock lock shim. This is one area where I differ slightly with the descriptions that you see on YouTube or even in Deviant's book as well as the *No Tech Hacking* (ISBN: 978-1-59749-215-7, Syngress) book that Johnny Long wrote (I wrote the Social Engineering chapter in *No Tech Hacking*). There are many excellent hacking descriptions of building these shims with empty soda cans, or better still, beer cans. My concern with spending a lot of time doing that would be cut fingers. I also know the amount of pressure that is needed to shim open padlocks similar to this one even with a spring steel commercial shim like the one shown in Figure 3.13. My other reason for not wanting to spend the time to make a shim out of a soda can is that the commercial versions, which work very well, cost only about $1.50 each including shipping. For me, it's just not worth the time and aggravation and possibly bloody fingers to build my own.

Padlock shims are not a new threat

Something else that I found interesting about using these padlock shims is the information among the lock enthusiasts about a vulnerability that's been known in the locksmithing world for over 40 years. While this is another vulnerability well documented on YouTube that you certainly need to know about, I don't think most non lock enthusiasts know about it. For the past several years I have taken padlocks with me as I present at various security conferences. I always let people experience the use of the shims on several of my personal padlocks to show them how they work and how easy it is. Among the hundreds of people who were in the various audiences, I don't think that many of them knew about that vulnerability before I mentioned it during the presentation. Most seemed very surprised as well as very interested in the fact that a lock that they had been familiar with since childhood could be opened so easily with a small piece of metal. All of this helps enforce my feeling that more and more people need to know and understand how locks work as well as ways that they can become compromised.

The vulnerability described here, and the impact that it had on my friend, standing there with nothing left but a towel, made me think of possible countermeasures. The scenario would have been slightly different if the bad guy had simply removed my friend's lock and left the locker completely open. The reaction of getting management involved could have been much quicker if that had happened. By adding the little social engineering twist of placing another lock in its place, the bad guy immediately created a diversion. If you've ever owned a combination lock with the serial number on the back of it, can you tell me that serial number? Probably not! So unless you can remember the serial number (and I don't plan to try), I usually suggest that people take one of those etching tools and make some mark known to them

somewhere on the back of the lock. It can even appear to be an accidental scratch. This won't stop the bad guy from taking your lock. But if you suspect that something like this has happened to you, you could probably quickly find out that the lock now securing your locker is not your lock.

In this scenario, where we're at a gym, there are a number of other things you could do to become a little tougher target. For years, when I was going to a local gym, I would use a key lock that was also a key retention lock similar to the one shown in Figure 3.5 but not as big. I did that for the same reason that I described what I like about the key retention lock earlier in the chapter. If that key was on the little wrist strap on my arm, I knew that the lock was locked somewhere. It could not be taken out of the lock if the lock was still (opened) unlocked. Many times when going to that same gym I would see locks of the type shown in Figure 3.13 on several lockers left unlocked. If you think about it, unless the locker was empty and the person went home and forgot the lock, it should never be on the locker unlocked unless you are standing there. Those people simply walked away and forgot to lock the lock. With the key retention lock, that can't happen. In most cases the key retention lock will also look considerably different from the majority of the locks in the gym. Most will look like the lock in Figure 3.13. If your lock looks different from everybody else's, and functions somewhat differently from everybody else's, you will automatically become a tougher target. It will be very difficult for the bad guy to have the right lock to be able to exchange yours with his.

I don't want to belabor this simple war story, but I do want you to understand that being a tougher target, and being a little bit more difficult to compromise than the next guy, is really the name of the game with security. If you are targeted personally, it will be very difficult for you to prevent certain things. Most situations similar to what happened to my friend are probably random thefts of opportunity. He didn't suspect that he was targeted. He may have been watched by a bad guy to see when he went to the shower, knowing that he would most likely be gone for about 5 minutes or more, and the bad guy could spend that time taking everything that my friend owned out of his locker.

SOME PLACES TO GO TO LEARN AND HAVE SOME FUN

I find it encouraging to learn about more and more local lock pick enthusiasts groups starting up. As I've said many times throughout this book, I believe that the more you know about locks and the ways that they operate, the more likely you are to choose a good one for your security needs. Let me tell you a little bit about the team from FALE (FALE Association of Locksport Enthusiasts) located in Winston-Salem, North Carolina. I had occasion to spend the day at a conference with them in May 2011. The FALE team that day consisted of Matt Block, Adam Sheesley, Jon Welborn, and Evan Booth. Check out their website at http://www.lockfale.com to learn more about them.

The lock collection that they had with them looked very similar to mine as they spread the locks out across three tables. In the exhibit area of the conference, I watched as people gathered around their tables and began the journey of learning what makes locks tick. It seemed like no matter how quiet or busy the exhibit hall was, there were always people gathered around those tables being fascinated with locks, and ways to open them. People can't seem to get enough of these truly interesting puzzles that we also use for some pretty critical security applications. It's a good idea to learn as much as you can about how and why they work.

My 110-year-old puzzle

I brought some of my locks with me, including my antique favorite with the patent date of 1901 stamped on the bottom. Many of the conference attendees who were standing at the FALE tables learning about locks were impressed with it and found it as fascinating as I did. Toward mid-afternoon I handed it to one of the FALE association leaders to see if he could open it. I wanted to be sure that the picking efforts didn't destroy it because lock picks are made of spring steel, and the pins inside the lock were 100+-year-old brass pins. The FALE team members were familiar with how the mechanism worked, and that was impressive to me in itself. This turned out not to be an easy task even for these young experts. I was again impressed with their ingenuity as they showed me a new device that I didn't know existed that allowed them to open the lock. Figure 3.14 is a picture of the newly opened lock.

From what we could see of the lock, this was truly one of the first pin tumbler padlocks. They quickly determined that there were four pins securing the plug. The lock was quite ingenious the way it was constructed. I had never seen anything quite like it. The FALE team knew that this lock required hitting the shear line with all four pins while pushing up on the lock shackle. I left for a while to view some of the rest

FIGURE 3.14

My 1901 padlock picked open by the FALE team

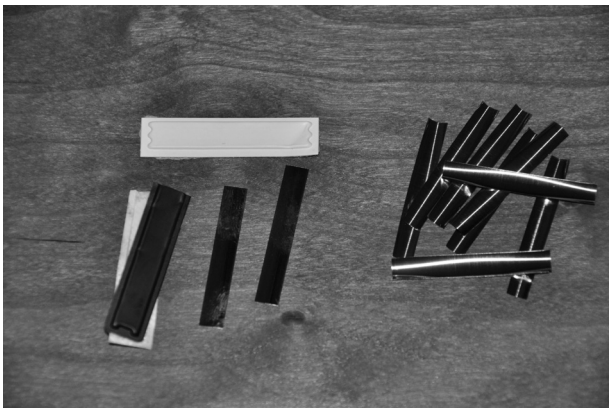

FIGURE 3.15

Low tech hacking shims and commercial shims

of the conference, and when I returned the lock was opened as shown in figure 3.14. They had opened it by using a plug shim in a way that I had never used. They used an improvised plug shim between the lock body and the plug on the side of the plug where the key enters. In addition, they used a shim that I did not recognize (see Figure 3.15). This is such a perfect example of using what I would consider low tech hacking for locks. I had never seen shims that thin. Figure 3.15 shows my standard shims on the right-hand side of the picture. The shims that they used, as shown on the left-hand side of the picture, come from the security devices that are found on most DVD cases. Someone discovered that if you cut the case open, there were two tiny pieces of metal inside that worked perfectly as shims. I don't do nearly as much with locks and keys as I used to, but on the day that I met the FALE team I learned a few new tricks from them. That improvised plug shim shown sticking out of the lock in Figure 3.14 is one of these shims from a DVD security device.

There are several devices that locksmiths use that are referred to as *shims*. The commercial shims, and the low tech hacking shims from the DVD security tags, are used as a shim to turn the plug in a pin tumbler lock. The lock shown in Figure 3.14 is one example of how they can be used. The shims commonly used to open the shackle of padlock are shown in Figure 3.13.

MORE ABOUT KEYS AND HOW TO MAKE ONE IF YOU DON'T HAVE ONE

My fascination with locks, and especially keys, has gotten out of hand a couple of times over the years. It seems like every time I see some neat little gadget or lock-related item, I need to have it. In the class that I was conducting a couple of years ago about penetration methods, I brought close to 100 locks with me for the demonstration. The students had a lot of fun, and obviously this was a very hands-on

demonstration. I'm going to spend the next little while talking about keys. For the sake of time, I'll narrow that down to discuss keys for pin tumbler locks. Since these are the most common locks that we see in our homes and offices, they are also the most likely to be attacked or tampered with by the bad guys of the world. For this next discussion, I'm going to assume that you know a little bit about the keys in your pocket. The notches in the key of varying depths are called *bittings* (some of us old guys still call them *cuts*). These need to be very accurate down to a couple thousandths of an inch in order for the pins in the lock to reach the shear line when the key is inserted, thus allowing the plug to turn. Those bittings each appear to be at a random depth. They aren't. Each lock manufacturer has a series of specific depths for the bittings on the keys for their locks, and there are normally between six and nine different depths of bittings for each keyway from that manufacturer.

Five pounds of my favorite keys

Here's an eBay find that has been one of my favorites over the years. Figure 3.16 is a picture of 5 pounds of pin tumbler keys that I spotted one afternoon for sale on eBay. To the untrained eye, it would appear to be a box of random keys from many manufacturers. I saw it as something completely different. You might not be able to see it in the picture of this box of keys, but each of the sets of keys from a respective manufacturer were held together by keychain. If I remember correctly, I was the only one who bid on this apparent 5-pound box of junk keys. I paid $10 for the box of keys, and another $10 to have them shipped to me. When I received them,

FIGURE 3.16

Five pounds of keys: eBay, $20.00

and opened the box to take a look, I was pleasantly surprised to see that they were exactly what I thought they were. These were 32 sets of depth keys from virtually every lock manufacturer that I was aware of and a few I had never even heard of before. These must have belonged to some retired locksmith. If I were to go out and buy these today as individuals sets, the retail price for what I had in that box would be over $1,000. Not a bad buy for 20 bucks. I love eBay!

Depth keys are quite interesting. Those that have 10 keys in their sequence will have a key with bitting depths starting with zero and ending with the key with all of the bittings cut to a depth of nine. The zero depth is the shallowest, and the nine depth is the deepest. If you begin to dive deeper into the world of locksmithing, you will eventually need to know a little more about key coding. This is another area where there is a lot of information on the Internet about this subject. There is another interesting find in this box of depth keys. Using bump keys is not something that was just discovered. It has been well known for a number of years, but again, with the Internet and new groups coming online to learn about locks, there are few people who have not heard about bump keys and bumping a lock opened. These bump keys are sometimes called *999 keys*. As I look at my sets of depth keys, many of them have a total of 10 keys, starting with key 0 and ending with key 9. Knowing this and seeing all of those sets of keys let me know that I also now had the beginnings of a complete set of bump keys. This was another bonus from my $20 purchase.

So now some of you are wondering, "Why should I care about all these keys?" Here's where a bit of knowledge, and little bit of social engineering, can be used to create a key for a lock that you have no key for. As mentioned earlier, our pen testing teams never failed to be able to use their social engineering skills to encourage someone to open certain doors for them. Keep in mind that locks on doors at work and locks on doors at home are quite easy to remove if you do it from the secured side of the door. If you are standing in front of the door that is locked, and you need a key to open the door, you are standing on the unsecure side of the door. Locks are designed to be difficult to remove from the unsecure side of the door. Take a look at this in your house the next time you examine your locks. You never want it to be any easier than it has to be to open the door from the outside without using a key. From the inside it's a different story. That's how the locks were designed to be removed should they ever need to be replaced or rekeyed. If it is a dead bolt lock, the screws to remove the thumb latch or the inside cylinder lock are on the secured side (inside) of the door. All that you frequently need is the correct screwdriver. Most key-in-knob locks have a small spring-loaded latch somewhere in the vicinity of the doorknob on the secured side of the door. If I can remove that lock, I will be able to shim the lock open (with one of the plug shims shown in Figure 3.15) and remove the plug. Using the proper set of depth keys, it will be easy to determine the necessary bittings (cuts) needed to then go out and have a key made. From that point on you would never need to pick that lock again. You would have your own key.

TIP

I'm intentionally not covering every detail of exactly how to do this. This will be your homework as you look at other books, check out YouTube, and look around the Internet using some of the keywords that you've seen in this chapter to begin your studies. I do want to mention that should you be shimming a lock that has master key pins, you will be able to use your pin tumbler shims (Figure 3.15) to open the lock, but you won't know whether you've hit the shear line that involves a master pin that could either be in the plug or the cylinder if the actual master key were used. The key that you create will open the lock that you're standing in front of, but it most likely would not be a master key that would open any other lock.

WAYS TO MAKE A KEY IF YOU DIDN'T BRING A KEY MACHINE

On several occasions, our penetration team was able to become friendly enough with the right people to have them let us borrow their keys to open a certain door when we didn't have our portable key machine with us. Our team always returned the keys within a few minutes and thanked them. Please keep in mind that this wasn't a situation where we just walked up to a total stranger and said may I borrow your keys? Getting to the point of building that much trust frequently took us several days or longer using social engineering skills. Keep in mind that we were always in buildings where we should not have been allowed such unlimited access. Now that I had their keys for just a few minutes, I was able to use a few more of my tools to find a way to create a copy of their key. Figure 3.17 shows a couple of those

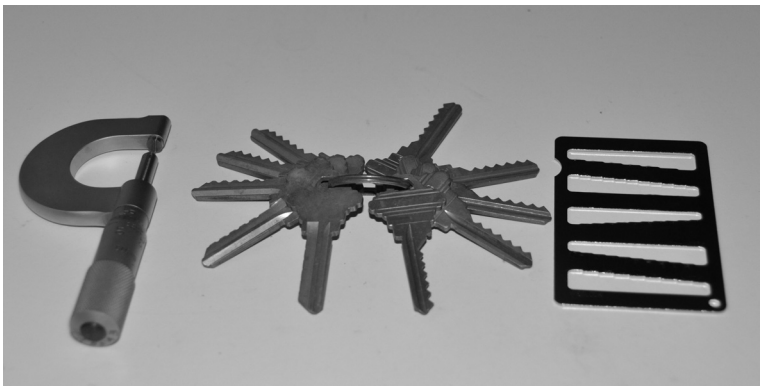

FIGURE 3.17

Micrometer, depth keys, and a key gauge

tools. The tool on the left is a micrometer that reads accurately to 1/1000 of an inch. There are micrometers specifically called *key micrometers*, but that's not what this is. It does function as well as an official key micrometer for my purposes. I bought this one at a yard sale many years ago for a few dollars. In the center of Figure 3.17 is one of the sets of depth keys from the box shown in Figure 3.16. I tried to photograph these keys in such a way that you could see the different depths of cuts on them. The key on the left of the pile pointing straight down is the zero cut key. Clockwise all the way around to the other key pointing straight down we go from 0 to 9. If you look closely you will see that each key seems to have bittings (cuts) that are a little deeper than the one just before it. Typically, the difference between bittings (cuts) is roughly between .015 to .020 of an inch. The device on the right of Figure 3.17 is a key gauge. It is designed for specific brands of keys, and the brand of key for each slot is marked on the gauge.

There are several things that I can do with these devices if I can hold your key for just a few minutes. In order to find the depth of the bittings on your key I could measure it with the key micrometer on the left, or I could use the key gauge on the right. To use the key gauge, I would slide your key into the gauge and read the number from 0 to 9 for each of the bittings on your key. Let's assume that this is the lock in your house, and I borrowed your key for a few minutes. If I determine that the depths of the bittings on your key are say, 35218, I can then take the depth keys using a simple inexpensive key machine or even a pippin file (a special file for use on key blanks, retail about $25) and duplicate your key. These depth keys are very accurate. Even if I don't have the key machine or a pippin file, I know that I can take this to the stand where they cut keys at the local flea market and have them make me a key from this code. Technically, this is not the code to your key but the numbers that equate to the depths of bittings for those respective numbers for that manufacturer. It is amazingly accurate and somewhat easy to do, and there are descriptions of very similar things on YouTube and other places on the Internet. I don't want you to be afraid to use your keys, but I do want you to be aware of a few of the ways that people can duplicate your keys, or even create one of their own from scratch with a few simple tools. ALWAYS BE CAREFUL WHO HAS ACCESS TO YOUR KEYS!

After reading this chapter I would like for you to think about your keys every time that they are out of your sight. This is especially true when you are places other than home. I've watched countless times over the years as people hand their complete set of keys to a parking attendant for valet parking. Think about what you have in your car. Not only would your keys be there, which as we've seen can be fairly easily duplicated, but much of your personal information resides on the registration for that vehicle. It's a little more difficult to duplicate most of the newer car keys. Obviously you need to give the parking attendant your vehicle key in order to have him or her drive your vehicle to the lot where the cars are to be parked, but you don't need to give anyone that much unlimited access to the rest of your keys.

WARNING

This warning will begin with one of my war stories. As I go about my normal day-to-day activities, I can't help but look at things through the eyes of security. Sometimes I see things that I almost can't believe. I was in the downtown area of a major city in a public parking garage that was a part of a major multi-tenant office building, and I had to use the restroom. (Don't panic, I'm not going to get too personal). As I walked over to wash my hands I noticed that there were a set of keys hanging out of the paper towel rack. Remember, this was in a public restroom in the garage of a very large multi-tenant building in the big city. Having spent a number of years in the locksmithing business and having a pretty good idea of what a master, grand master, and great-grand master key might look like, there were at least two of them on that key ring along with the key that opened the paper towel rack. This is pretty bad news. The little key that opens the towel rack to allow people to put in new paper towels is pretty much the tip of the screwdriver. It really isn't there for security at all. The rest of the keys on that key ring very well could have been the keys that open many of the doors in the entire building. Not a good situation. If those keys fell into the wrong hands, I have no idea how much it would cost to rekey a building of that size. Most likely, it would never be done. I turned the keys in to the building security office, and briefly mentioned that I didn't think that it was a good idea for such critical keys to be on the same key ring as the device that opens the towel rack. It was obviously left there by mistake by whoever just cleaned the restroom. I'm sure that wasn't intentional.

Key control is absolutely critical. It just seems to be so easy to become complacent about the things that we have been using all of our lives. Who has the keys to your kingdom?

ONE FINAL LOCK TO TALK ABOUT AND THEN WE'RE DONE

The final lock that I would like to talk about in this chapter is also the most common: locks found in office buildings and places other than homes. This is another pin tumbler lock typically containing either five or six pins. Most of these locks used in industry will also be set to some level of the master key. The additional pins in each stack actually allow for more potential shear lines to be hit when picking or shimming the lock open. Figure 3.18 is one of my photographs of a mortise cylinder lock.

At first glance this lock doesn't look much different from the rim cylinder lock that I showed in Figure 3.7. The main difference isn't the lock itself or even the keys. What makes this lock a little bit more commercial is the way that it installs into the main lock body. If you look closely at the lock you will see threads completely around the main body of the cylinder. This lock literally threads into the main body of the mortise lock in a similar way to threading a bolt into a nut. There are two screws that secure the lock in place by passing through the horizontal notch that you see cut through the threads. Figure 3.19 is a good example of an older but complete mortise lock set.

I have loosened one of the set screws for the outside cylinder and left it hanging so that I can explain it to you. Normally this screw would go horizontally into a threaded unit that lets it enter its respective channel in the mortise cylinder lock.

FIGURE 3.18

Mortise cylinder: eBay, $2

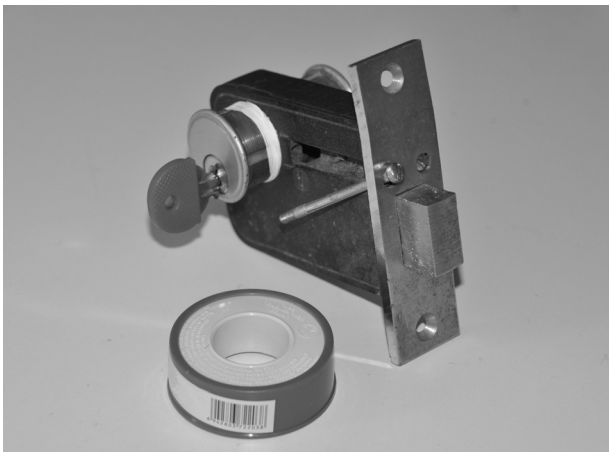

FIGURE 3.19

Mortise cylinder lock: eBay, $2

With that screw in place, the door closed, and the bolt extended as you see it, the lock itself cannot easily be removed with brute force. There are a couple of things that I've added to this picture that I need to explain. One of them is the Teflon plumbers tape that you see in the foreground. There's more of that tape around the cylinder that was screwed back into the mortise lock body. The reason for the tape is the social engineering version of the way that a lock like this could possibly be compromised by a bad guy or by a good guy conducting the penetration test. The tape allows the lock to remain in place securely while anyone using a key to

open that lock would think that it's completely normal. Without that set screw being in place, the lock is completely vulnerable. It would be a simple matter to insert a blank key (one with none of the bittings cut) to use as a lever to simply unscrew the lock cylinder from the mortise lock body. A screwdriver could also be used, but that could leave marks. Using a key blank would not leave any indication that the mortise cylinder lock was tampered with. Uncut key blanks are also very strong. Without the bittings being cut into the blade of the key it hasn't lost any of its strength. The final thing in that picture is the little key hood that I've placed over the key. This has become a low tech hacking way of covering the bow of the key so that you can not see that the key had "do not duplicate" stamped into the brass. When having a key duplicated at my local flea market, I have never seen the key machine operator remove the key from a keychain to cut the new key. I suspect that most people never look under those little key hoods to see if this is a key that should not be duplicated.

Rim cylinder locks vs. mortise cylinder locks

Mortise cylinder locks are different from rim cylinder locks in that they cannot be easily removed with a slide hammer (see Figure 3.8) as I described earlier in this chapter. They have other vulnerabilities, but the ease of removing the lock cylinder itself is not one of those vulnerabilities. The keyway is, however, still susceptible to being drilled if forced entry is used. The vulnerability of removing the lock greatly increases if I'm given the opportunity to open the door. Once the door is opened, the door edge as well as the normally secured side of the door are now exposed. The door edge is where the set screw resides that prevents this cylinder from being removed. If someone allows me to go into that room, in a fairly short time frame, I can remove the lock without damaging it, shim it opened so that I can remove the plug without any keys, use my depth keys to determine a shear line that will open that lock, reassemble the lock, and put everything back to normal. This would not take long for a person with some lock knowledge, and thanks to the Internet, many people now have that knowledge. I'll say again, the key that I could produce by doing something like this most likely would not be the master key that opens every door. It would simply be the key that would let me back in that door. (Once again, complete details of how to do something like this will be left to your additional study and practice.)

Let's go through one final social engineering attack scenario where I do have access to that key for a few minutes. To make this more interesting, let's assume that the key that I am able to borrow for a few minutes is one of the building master keys as is frequently the case. Again, our normal mode of attack was to befriend certain individuals over a period of time, gain their trust, and eventually ask for the small favor of being given access to our target room. This sounds like it could never work. Trust me, it worked pretty much every time. Figure 3.20 shows the target key, the key gauge that I showed you in Figure 3.17, and three small key covers (one of them is shown in Figure 3.19). These kinds of key covers can be used for more than just making certain keys on your key ring easy to spot.

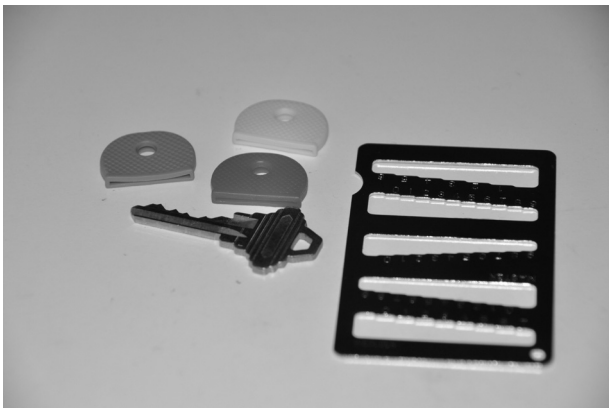

FIGURE 3.20

Key covers, target key, and a key gauge

Let me first address the key covers . These are available for less than a dollar each at pretty much any place that cuts keys. Keep in mind, probably 99% of the places that you go to have a key cut are not locksmith shops. I've seen a number of small key cutting shops working out of the back of a truck at a flea market. One of these is a small dealer that I have make all of my keys. Recently I asked him if he has ever been asked to cut a key using depth keys. He said no but that he would be happy to if I showed him how to do it. As you can probably tell by now, I really enjoy watching people while I'm out there practicing some of my favorite hobbies. I've seen a number of keys cut at this particular place where the key had one of those little hoods over it to make it easily identifiable for the owner. When a key like that is on a key ring, there is no need to remove the key from the key ring in order to copy it. There would be no way for the person cutting that key to know whether or not the key under the hood was marked "do not duplicate." Using one of those little hoods is certainly a low tech hack way of hiding the fact that the key should not be duplicated. I've never seen anyone look under the hood to see what the key said.

Now onto the key and the key gauge in Figure 3.20. Let's pretend that that key is the building master key and you were kind enough to loan it to me for just a minute or two to open the door. All that I would need to do is use my micrometer shown in Figure 3.17 to tell me the depth of each of the bittings on that key. This key could then be cut on a key machine that is capable of cutting keys by code. The key machine that I found at a yard sale several years ago for $10 could cut keys by code. If this were a key from a home or from a lock that was not on a master-keyed system, I could take the depth keys shown in Figure 3.17 to my local key-cutting buddy along with the code that I could easily read from the key gauge in Figure 3.17 and have him create an exact copy of that key.

Let's take this same scenario to your home. In most cases when we were doing inside penetration tests we would learn a little bit about some of the senior

management in that company. This is totally hypothetical, but if someone were to be able to get hired on to the cleaning service that cleans the executive's home, how hard would it be for them to pick up the executive's keys off of the kitchen counter and measure the cuts with the key gauge? Who doesn't leave their house keys on the counter of their home when they are in the home? If the bad guys can get access to the executive's home, they can quickly get enough information from any key to be able to duplicate it later. The bad guys wouldn't need to take the executive's key out of his home or even have access to it for more than a minute or so.

SUMMARY

—Low Tech Jack

The contents of this chapter could easily become an entire book. I do need to bring it in for a landing somewhere, and this is as good a place as any. My main purpose for including a chapter like this is to give people an idea of some of the ways that low tech hacking can be employed to compromise mechanical locks and gain physical access. As I mentioned several places throughout this book, I have seen enormous changes in the availability of information regarding locks, keys, and bypass methods over the past 40+ years. The existence of sites like YouTube, and the Internet in general, has provided everyone (including the bad guys of the world), with a lot more information about what I like to call lock threats and vulnerabilities than was available just a decade ago. What I don't see much of out there on the Internet are discussions about possible countermeasures for these vulnerabilities. I've said it hundreds of times over the past 40+ years that the number-one countermeasure for most security related issues is employee awareness training. Hopefully, this chapter will help open everyone's eyes regarding the ever-present clear and real threat to the physical security of our most valuable intellectual property and technical assets.