Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Attacks Against The Mechanical Pin Tumbler Lock

This paper examines an overview of the common pin tumbler lock and the five methods to exploit them. Pin tumbler locks are found in a vast majority of residential, commercial, government and educational institutions. It is possible for an attacker without using any specialized tools or having an expert skill level to quickly open them. When evaluating the current or future key based pin tumbler lock the security practitioner should protect against the methods of picking, impact, impression, decode and bypass. The relev...

Copyright SANS Institute
Author Retains Full Rights

AD

Attacks Against The Mechanical Pin Tumbler Lock

© SANS Institute 2004, Author retains full rights.

Craig Kagawa
GIAC Security Essentials Certification (GSEC)
Practical Assignment Version 1.4b, Option 1
Date Submitted: January 1, 2004

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Table of Contents

1. Abstract …… 3

2. Introduction…….. 3

3. Brief History…… 3

4. Parts of the Pin Tumbler Lock……... 4

5. Five Methods… …… 5

Picking…… 5

Impact…… 8

Impression……10

Decode…… 11

Bypass……11

6. Practice Board…… 13

7. Conclusion…… 14

8. Notes……..15

9. References……18

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Abstract

This paper examines an overview of the common pin tumbler lock and the five methods to exploit them. Pin tumbler locks are found in a vast majority of residential, commercial, government and educational institutions. It is possible for an attacker without using any specialized tools or having an expert skill level to quickly open them. When evaluating the current or future key based pin tumbler lock the security practitioner should protect against the methods of picking, impact, impression, decode and bypass. The relevant information for this paper came from Internet websites, Internet message boards, literature, and video/audio files.

Introduction

The primary function of any mechanical lock is to deter intruders and prevent theft of property. They are an inexpensive and a simple security mechanism that can be found in residential, commercial, government and educational institutions.

In today's environment, the pin tumbler lock is the most common and widely used of the mechanical key based locks. You will find them in many different configurations and applications ranging from door locks to small suitcase padlocks.

It is possible to circumvent these locks by gaining access through an open window or an adjacent room. An attacker might use social engineering skills[1] to obtain his goal. The attacker could even apply enough physical force to break the lock or the surrounding environment to gain entry. The attacker also has another option. The attacker can exploit the lock to open with minimal effort. This could be a better solution since using force will leave noticeable physical evidence and the other methods may not be applicable. Imagine the problems that face the security practitioner if an attacker has free access to a restricted area and no one knows about it.

This paper will examine the common pin tumbler lock and the five methods that an attacker can use to unlock them without having the key. Understanding the attack methods will help the security practitioner evaluate their current and future key based pin tumbler locks.

Brief History

In 1844, Linus Yale Sr.[2] invented the Yale lock[3] also known as the pin tumbler lock. Alfred C. Hobbs,[4] a lock picker during this time, described the lock as "*Something like the Egyptian with something like the Bramah."*[5] The Egyptian lock[6] used a key with pegs while the Bramah[7] lock design had a key that didn't come in contact with the locking bolt. Between 1860 and 1865, his son Linus Yale Jr. improved on the initial design and is credited for the mass production of

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

the lock.[8] This design won worldwide support because it deter intruders, inexpensive to manufacture, easy to install and simple to change for a new set of keys. Since the improvements by Linus Yale Jr. in the mid 1800's little has changed.

Parts of the Pin Tumbler Lock

Today's basic pin tumbler lock has the following components.
The cylinder shell (also known as the hull) is the outer casing of the lock and does not move. The keyway is the opening where the key is inserted. The plug is the inner cylinder of the lock that rotates when you turn a key. Inside each pin chamber there is a spring that applies force to the top pin. The top pin (also called the driver pin or tumbler) pushes down on the bottom pin. The shear line is the gap between the plug and the cylinder shell. The combination of the top pin and the bottom pin is called a pin stack. The ward guides the key in the keyway and restricts the pins from escaping. The bottom pin (also called the key pin) makes physical contact with the key. The first pin that comes into contact with the key is called pin 1.

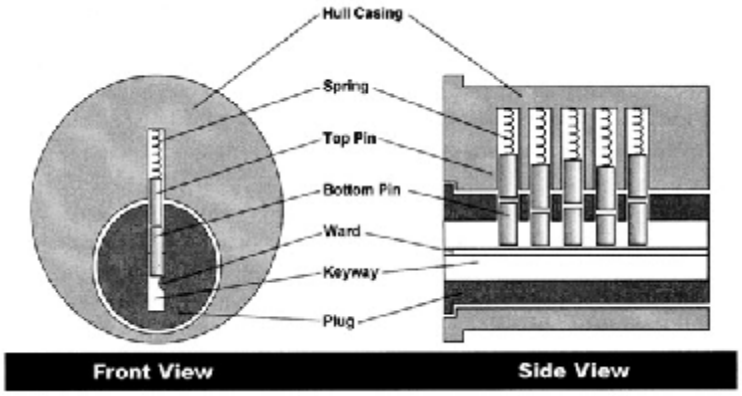


Figure 1. Parts of a Pin Tumbler lock[9]

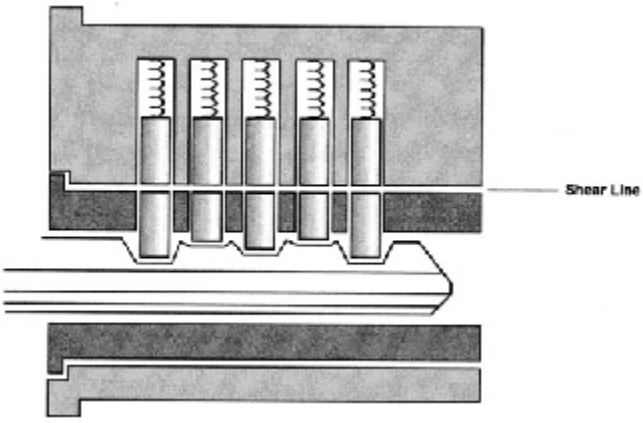


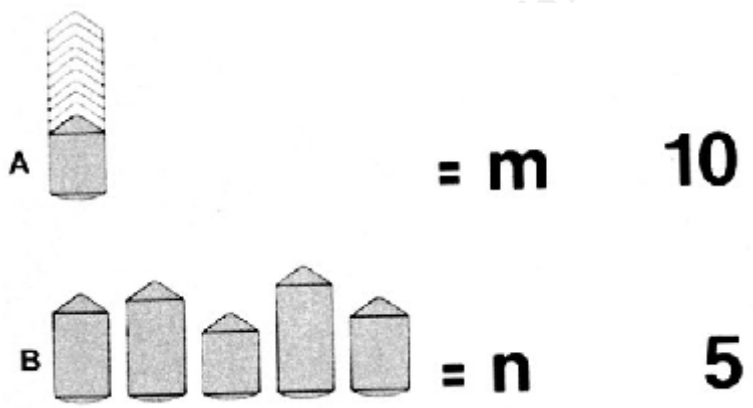
Figure 2. Side view cutaway – key inserted[10]

When the correct key is inserted, the key lifts each pin stack (bottom and top pin) until the separation between the bottom and the top pin reaches the shear line.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

When all of the pins attain this position, the plug is able to freely rotate, releasing the locking bolt and opening the lock. If an incorrect key is used or the key is removed some of the pins will cross the shear line preventing the plug from rotating.

The number of pin stacks determines how many different key combinations a pin tumbler lock can have. If you have six pin stacks in the chamber you have 10^6 or one million different key combinations. The number 10 equals the number of segments that the bottom pin can be divided into without interfering with the moving parts of the lock. The number of segments is determined by the lock manufacture. The height of this pin also determines the depth of the key cut on the shaft of the key. Instead of referencing to the number pin stacks it is common to refer to the number of bottom pins that the key touches. Tammy Niday of Custom & Security Hardware acknowledges that typically in today's conventional pin tumbler lock there are five pins.[11] This means there are only 100,000 possible key combinations.



Row A: m is the different height segments of the bottom pin
Row B: n is the total number of bottom pins
Figure 3. Key Combinations = 10^5 =100,000 [12]

Five Methods

Knowing that there are only 100,000 different key combinations the attacker has pretty good odds. If he had a tool that would allow him to try all the different combinations, then his only enemy would be time. There are 5 methods that he can use to quickly exploit a pin tumbler lock without damaging the lock or the surrounding environment. They are picking, impact, impression, decode and bypass. In many of these methods the attacker can create tools found in a residential home or purchase materials from a hardware store. The attacker isn't limited to a single technique. He can combine several techniques until the lock opens. More importantly he doesn't need to try 100,000 different key combinations.

Picking

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Picking can be described as *"… manipulating tumblers to operate a lock without the use of, or access to, its correct key"*[13] Picking is also commonly referred to as lockpicking. Locksmiths learn to pick locks as part of their trade; however the act of picking a lock can be found all around us. In films, it is common to see a character picking a lock on a door. Magicians learn to pick locks to escape from their death defying situations. Teenagers are even exposed to picking locks in video games. For example in the popular video game Tom Clancy's Splinter Cell[14], you control a covert spy who picks locks to gain access to restricted areas.

Picking works because there are small mechanical imperfections in every lock, even by the same manufacturer. *"Picking depends on weaknesses in the implementation of locks – small manufacturing imperfections – rather than fundamental, abstract design flaws that would be present no matter how carefully made the locks might be."* [15]

To pick a lock an attacker needs a lockpick set. A professional lockpick set can be purchased from a locksmith supply distributor or obtained on-line over the Internet. The United State's state and city laws vary from state to state regarding who can legally obtain and own lockpicks. Professional lockpicks are easy to purchase in spite of the laws. At DefCon 11, the Annual Hacker convention in Las Vegas, professional lockpicks were advertised and sold openly to anyone in the vendor area. [16]

A lockpick set contains the following items: a tension wrench and one or more picks. Both tools are available in all shapes and sizes. The tension wrench is known by several other names such as the turning tool, torque wrench, torsion wrench and tension tool. The purpose of the tension wrench is to apply the turning rotation on the plug. The pick is typically named after the shape of the pick's head such as diamond, snake, and circular (ball). Commonly the hook or the half diamond pick is best for picking a single pin at a time, while the snake pick is used for manipulating several pins at once.

Professional lockpicks are commonly constructed from steel or metal; however, there is a distributor that manufactures fiber picks. The head of the pick is made from small flexible nylon fibers. The company claims that the fiber pick gives better feedback to the user.[17]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

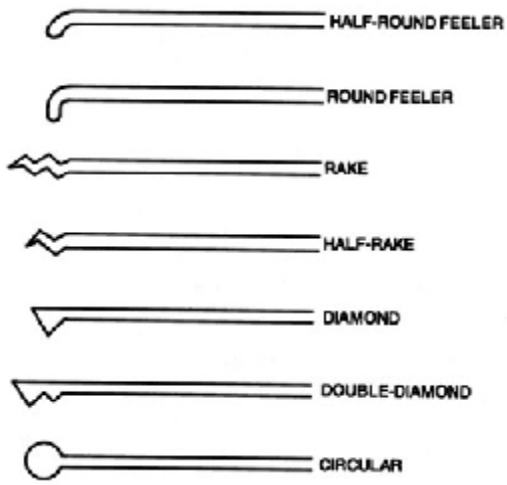


Figure 4. Some basic lockpick shapes[18]

Lockpick sets can also be created with common household objects and tools. Often there are advantages in crafting a homemade lock picks. *"Many experienced locksmiths and expert lock pickers prefer "home made" tools to the commercial selections, especially for picking unusual and high security locks"* [19]

The picks can be made from any thin strong material that can fit in the keyway of a lock. The attacker can shape the head of the pick with a metal file or an electrical grinder. Discarded street sweeper bristles are a popular choice as well as hacksaw blades, small screwdrivers and dental picks.

A tension wrench can be constructed by bending a piece of metal into an L shape form. The tension wrench requires that it be small enough to fit in the keyway of the lock and allow enough room for the pick to maneuver around. It should also be sufficiently strong so it will not lose its shape when rotating the plug.

The following technique demonstrates picking. The tension wrench is inserted in the keyway and the attacker slowly turns the plug. With pressure applied one or two of the pins will bind in the pin chamber. The lock will not bind on all of the pins because of the mechanical imperfections of the lock. Next the pick is inserted in the keyway. The attacker moves the pick to each of the individual pins and pushes them to feel for resistance. The pins that resist are binding. The attacker moves the binding pin up to the shear line. There will be a faint click or give when it reaches the shear line. This means that the pin is set. The attacker will be able to rotate the plug further and more pins will bind. The attacker moves to the next pin that is binding. The goal is to have all the pins reaching the shear line so the plug fully rotates which opens the lock.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

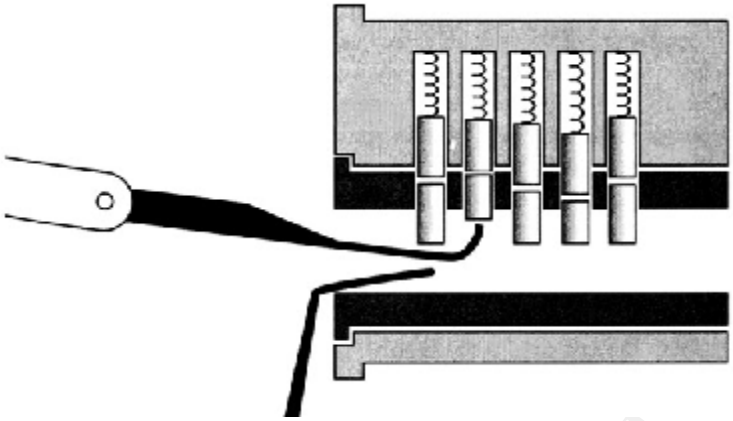


Figure 5. Placement of Pick and Tension Wrench in the lock keyway for picking [20]

While manipulating each pin, the attacker must rely on the pick's feedback since the attacker isn't able to see inside. It is very common during picking for the bottom pin to be pushed past the shear line. Another common mistake is to place too much pressure on the tension wrench, so the binding pins cannot be manipulated. If there is not enough pressure with the tension wrench the plug will not rotate. Sometimes the lock picker will rotate the tension wrench in the wrong direction. To solve this problem there is a tool called a plug spinner. [21] This tool rotates the plug in the opposite direction without sacrificing the attacker's work.

Raking is a common picking technique for beginners as well as professionals. Ted the Tool refers to this as *"scrubbing".*[22] This technique can be highly effective and quicker than manipulating each individual pin. There are several different techniques to rake as well as many different styles of raking picks.

The following technique demonstrates raking of a pin tumbler lock.
The attacker inserts the tension wrench and turns the plug. Next he inserts the pick and quickly rakes in a fast backwards and forwards motion across all of the pins. This moves a few bottom pins at any moment in time. The raking action will vibrate the top pins above the shear line.

Understanding the technique of picking is simple. However to be proficient at picking a variety of locks, it does require patience and practice. Barry the Key stated that if a person practiced 4-6 hours a day for 6 months, that person would be able to open 50% of the common locks. [23] The DefCon 11 2003 lockpicking contest winner took 2.97 minutes to open 3 locks.[24] He stated during the award ceremony that he begin picking locks 5 months before the contest and created his own lockpick set. [25]

Impact

The impact method is that a sudden shock or bump can enable a pin tumbler lock to open. Barry the Key described the theory of impact.[26] Two gray balls are next to each other. A third ball travels towards one of them. When the third ball

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

hits the gray ball it stops but the impact pushes the other gray ball. That gray ball travels along the plane. The same concept can be applied to the pins inside the chamber. If you bump the bottom pin of a common pin tumbler lock it can force the top pin to jump above the shear line.

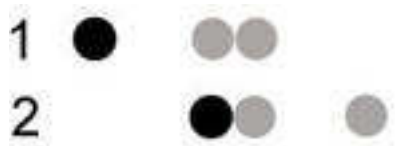


Figure 6. Demonstration of impact[27]

A popular technique to unlock pin tumbler locks is to use a bump key. A bump key goes by other popular names such as a 999 key, rapping key, or bounce key. A bump key is typically a blank key with tiny little bumps crafted on the key's shaft.

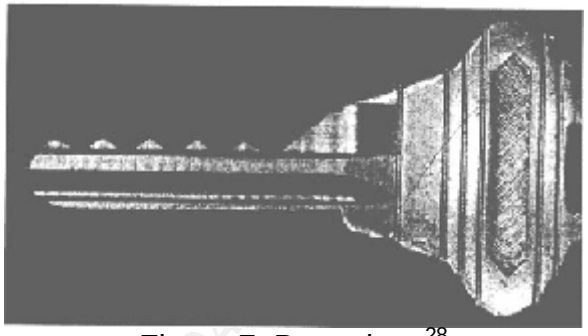


Figure 7. Bump key [28]

The following technique demonstrates using a bump key. The bump key is inserted in the keyway and is rotated as if it were opening the lock. The key is tilted up and the attacker bumps the underside of the key. The timing of turning and bumping is a critical factor when using this method because all of the top pins must go above the shear line and the plug must be rotated at the same time in order for the lock to release. It can take several hits.

A Pick gun (also known as snap gun) is a tool that uses a similar technique as the bump key. It is called a pick gun because it is shaped like a miniature gun. They are known to be fast and effective against pin tumbler locks.
The pick gun snaps all of the bottoms pins at once. To operate a pick gun the attacker inserts the tension wrench and the front-end of the gun into the keyway of the lock. The attacker rotates the plug with the tension wrench and pulls the trigger.

Pick guns can be easily obtained like lockpicks; however an attacker can also create them with a few simple household items. *"A Snap Pick" is basically a home made pick gun made from a wire coat hanger. It lacks the nifty trigger lever and adjustment wheel, but will do the job just as well and the only tools/materials required are a broom handle, a file, a whetstone, and a coat hanger."* [29]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Electronic picks can be described as the high tech pick guns. They are shaped like an oversized electrical screwdriver. Instead of manually pulling the trigger, the attacker pushes a button to oscillate the pick. An attacker who wishes to have an electronic pick could easily modify an electrical toothbrush.

Another impact technique is called rapping. It requires that the pins inside the pin chamber can freely move around. If there is a sudden shock or "rap" above or near the tumblers, it can cause the pins to jump and split at the shear line.

Max Alth gives a detail example.
"A tension wrench of a key that has been filed way down so that it doesn't touch the pins is inserted in the lock. The wrench or key is turned to produce a rotational tension on the lock. Then the face of the cylinder is struck a sharp blow with a plastic hammer or a mallet." [30]

Lawrence Fennelly informs that padlocks are acceptable to rapping technique.
"Since padlocks are not encased in a door, they respond more freely to rapping."[31]

Impression

In order for a correct key to operate a pin tumbler lock it must be of the correct length, fit in the keyway and raise the bottom pins to the shear line.
The impression method is to produce a working key that will unlock a lock.
An attacker could take a wax impression of a working key and create a duplicate key from the mold. If the attacker doesn't have access to the key, he can create a working key by using a blank key or any soft metal that can fit inside the keyway.

The following technique demonstrates using impression on a pin tumbler lock. Blank keys are probably the best material to use when using this technique because the blank keys are inexpensive and readily available from any local hardware store. A blank key is inserted in the keyway. The attacker applies a strong rotation tension to the blank key and jiggles it up and down. Scratches will be left on the top of the blank key. These scratches are from the bottom pins rubbing against the blank. If an attacker carefully files off the scratches and repeats the process until it produces no scratch marks, a rough duplicate key is created that will unlock the lock. This works because the bottom pins won't leave a scratch mark on the blank key if the pins are reaching the shear line. A common mistake is that the attacker files away too much. This can cause the driver pin to pass the shear line and prevent the plug from rotating.

Creating a key may sound time consuming; however, Mark Wanlass and Stan Hall wrote the following. ***"****With practice and by making use of shortcuts, it is not unusual to be able to make a key in about 10 minutes. Some locks will take longer. Sometimes as little as 5 minutes is possible if you are both lucky and*

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

skilled. If you try to pick a lock, you don't know in advance if it will take one minute or thirty. With impressioning, opening a lock is a more reliable and predictable process."[32]

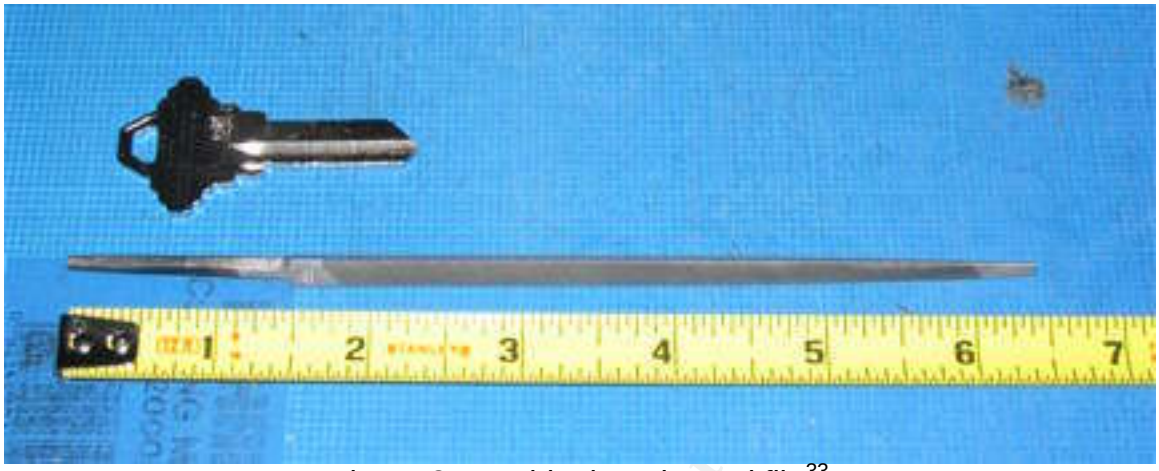


Figure 8. Key blank and metal file[33]

Decode

Another method that is similar to impression is called decode. The method is to produce a working key by examining a key or lock.

When you have a spare key duplicated by a locksmith, the inside of the key cutting machine uses a decode technique to create a key.
Another technique of decoding is accomplished with a tool that measures the bottom pins of the lock. Here is a detailed example of decoding.
"A more common method is to insert a decoding tool or a specially marked key blank for a short distance into the keyway of a pin or disc tumbler mechanism. Using the key, rotational tension is applied to the plug, which causes misalignment between the pin chambers in the plug and shell. The key is then slowly inserted into the keyway until it has forced the first tumbler to the shear line. The length of this first key pin is determined by the distance the blank (or special tool) enters the key way. The blank is then moved to the second tumbler, and so on until the length of all the tumblers is determined and the key can be cut." [34]

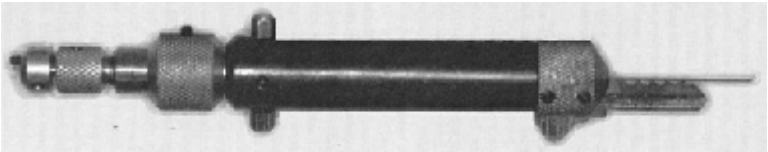


Figure 9. A pin lock decoder tool for measuring the bottom pins of a lock[35]

Bypass

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Bypass is the method to go around the locking mechanism and exploit the locking bolt without damaging the lock or the surrounding environment.

One technique of bypass is called shimming. A popular example of shimming is an attacker opening a lock door by sliding a credit card between the door and the locking bolt.

Common padlocks are highly susceptible to the shimming attack. The time to unlock a padlock with a shim takes the same amount of time if you were using the correct key or remembering the combination on the lock. Barry the Key gave a live demo of opening a popular brand combination padlock with a shim.[36] An attacker inserts a shim between the space of the shackle and the padlock. Any small thin object can be used as a shim. The shim forces the padlock's locking bolt to slide open. This technique works well because padlocks as well as many door locks have spring loaded locking bolts. The locking bolt is angled and spring loaded so that the user is able to secure the lock without using a key.

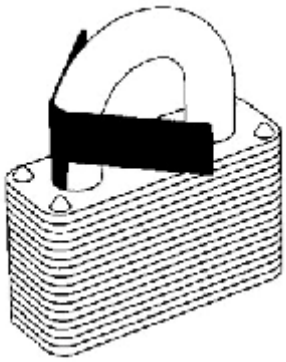


Figure 10. Opening a padlock with a shim [37]

Another bypass technique is called *"bypass picking"*.[38] The attacker ignores the locking mechanism altogether and moves the locking bolt to unlock the lock. Any object that can fit inside could work as long as the lock allows the locking bolt to be manipulated. In figure 11, the attacker moves the locking bolt that is held by a spring.

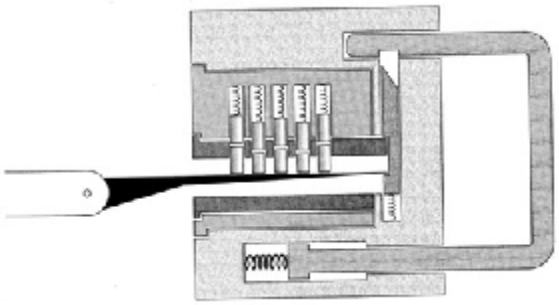


Figure 11. Bypass picking [39]

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Another quick bypass technique is to remove the plug from the lock. Without the plug there is no lock mechanism. Using a plug removal tool can work with certain mechanical locks. The tool was created for locksmiths to save time when changing for a new set of keys. The tool is small enough to be concealed in an attacker's pocket.

The Practice Board

An attacker would probably build up his skills before exploiting a lock in the real world. He could practice by purchasing a variety of deadbolts, door locks or padlocks from the local hardware store. Estate sales, flea markets and garage sales are also a good source for inexpensive locks.

Front Back

Figure 12. Picking practice board with deadbolt locks[40]

The above practice board was constructed with a few discarded pieces of lumber, several deadbolt locks, screws and paint. This practice board is similar to Matt Blaze's lock picking board.[41]

The pins were removed from four of the deadbolt locks using Greg Miller's instructions.[42] Each deadbolt lock is set for a pin stack of "n" level difficulty. This provides a platform for the student to learn different techniques at their own rate. For example a student can begin picking a deadbolt that is protected by 1 pin stack and advance to 5 pin stacks. Padlocks can be attached to the hook

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

located on the left side of the practice board. This practice board also allows the student to practice impact, decode, bypass or impression techniques.

Conclusion

Understanding the five methods to exploit a pin tumbler lock can help the security practitioner evaluate current or future key based pin tumbler locks in their overall security design. Besides their own requirements they should look for the following qualities in any key based pin tumbler lock:

- A lock that resists picking
- A lock that withstands impact
- A lock that prevents impression and decoding methods
- A lock that protects against bypass methods.

Selecting a lock that best matches the overall security design will help reduce the chance of intrusion or theft of property. Remember the common pin tumbler is a popular model of a key based mechanical lock that is widely used today.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Notes

[1] Granger, Sara. "Social Engineering Fundamentals, Part I: Hacker Tactics". 18 December 2001. URL: <http://www.securityfocus.com/infocus/1527> 1 December 2003

[2] Tobias, Marc. Locks, Safes, and Security Second Edition. Illinois: Thomas, 2000. 25

[3] See note 2

[4] Evans, Jim. "A Gazetter of Lock and Key Makers". 2002. URL: <http://www.localhistory.scit.wlv.ac.uk/Museum/locks/gazetteer/gazhaa-hog.htm> 26 November 2003

[5] Zara, Louis. Locks and Keys. New York: Walker And Company, 1969. 73

[6] Tobias, Marc. Locks, Safes, and Security Second Edition. Illinois: Thomas, 2000. 7

[7] Tobias, Marc. Locks, Safes, and Security Second Edition. Illinois: Thomas, 2000. 19

[8] See note 2

[9] McCloud, Mark. Visual Guide to Lock Picking Second Edition. Illinois: Standard Publications, 2002. 27

[10] See note 9

[11] Niday, Tammy. Personal Interview at Custom & Security Hardware. 1 Dec. 2003

[12] Tobias, Marc. Locks, Safes, and Security Second Edition. Illinois: Thomas, 2000. 303

[13] Blaze, Matt. "Notes on Picking Pin Tumbler Locks".7 November 2003. URL: <http://www.crypto.com/papers/notes/picking/ > 5 December 2003

[14] Johnson, Austin. "Splinter Cell Walkthrough". 13 November 2003. URL: <http://www.gamespy.com/articles/november03/scwalk/index16.shtml> 1 December 2003

[15] Blaze, Matt. "Notes on Picking Pin Tumbler Locks".7 November 2003. URL: <http://www.crypto.com/papers/notes/picking/ > 5 December 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[16] DefCon 11 Convention. Vendor Area. August 1st through 3rd 2003 Alexis Park Hotel Las Vegas, Nevada

[17] Pickmasters. "An Introduction to Fiber Picks". URL: <http://www.pickmasters.net/newcon/fiberpick-moreinfo.html> 5 December 2003

[18] Phillips, Bill. The Complete Book of Locks and Locksmithing Fifth Edition. New York: McGraw Hill, 2001. 335

[19] Blaze, Matt. "Notes on Picking Pin Tumbler Locks".7 November 2003. URL: <http://www.crypto.com/papers/notes/picking/ > 5 December 2003

[20] McCloud, Mark. Visual Guide to Lock Picking Second Edition. Illinois: Standard Publications, 2002. 37

[21] Tobias, Marc. Locks, Safes, and Security Second Edition. Illinois: Thomas, 2000. 59

[22] Ted the Tool. "Guide to Lock Picking". 1 September 1991. URL: <http://www.lysator.liu.se/mit-guide/mit-guide.html> 10 November 2003

[23] Barry the Key, Hans Unicorn. "Lockpicking with Barry the key and Hans Unicorn". 14 July 2000. URL: <http://www.connectmedia.waag.org/tool/h2k-lockpicking.wmv> 1 December 2003

[24] simple3 "LockPick Contest?" Online posting 5 August 2003. URL: <http://forum.defcon.org/showthread.php?t=2119&highlight=lock+picking> 10 November 2003

[25] DefCon 11 Convention. Awards Ceremony. 3 August 2003 Alexis Park Hotel Las Vegas, Nevada

[26] See note 23

[27] Demonstration of impact. Image created by Adobe Photoshop 5.5

[28] Tobias, Marc. Locks, Safes, and Security Second Edition. Illinois: Thomas, 2000. 603

[29] Mini-Blue "a little advise for me?… and a story…" Online posting 18 November 2003. URL: <http://lockpicking101.com/viewtopic.php?t=857> 1 December 2003

[30] Alth, Max. All about locks and locksmithing. New York: Hawthorn Books, 1972. 89

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

[31] Fennelly, Lawrence J. Effective Physical Security Second Edition. MA: Butterworth-Heinemann, 1997. 145

[32] Wanlass, Mark, Hall, Stan. "Impressioning Manual For Amateur Locksmiths" 1997. URL: <http://www.gregmiller.net/locks/impress.html> 26 November 2003

[33] Key blank and metal file. Image taken with a Cannon Digital Elf: PowerShot S230 under electronic flash

[34] Fennelly, Lawrence J. Effective Physical Security Second Edition. MA: Butterworth-Heinemann, 1997. 145

[35] Tobias, Marc. Locks, Safes, and Security Second Edition. Illinois: Thomas, 2000. 764

[36] Barry the Key, Glasser, Mark. "Lockpicking at Hope2k". 14 July 2002. URL: <http://www.connectmedia.waag.org/tool/h2k2-lockpicking-vcd.mpg> 1 December 2003

[37] McCloud, Mark. Visual Guide to Lock Picking Second Edition. Illinois: Standard Publications, 2002. 48

[38] McCloud, Mark. Visual Guide to Lock Picking Second Edition. Illinois: Standard Publications, 2002. 51

[39] See note 38

[40] Practice board. Image taken with a Cannon Digital Elf: PowerShot S230 under electronic flash

[41] Blaze, Matt. "Notes on Picking Pin Tumbler Locks".7 November 2003. URL: <http://www.crypto.com/papers/notes/picking/ > 5 December 2003

[42] Miller, Greg. "How to remove pins from a pin tumbler dead-bolt". URL: <http://www.gregmiller.net/locks/disassemble.html >10 November 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

References

Granger, Sara. “Social Engineering Fundamentals, Part I: Hacker Tactics”. 18 December 2001. URL: <http://www.securityfocus.com/infocus/1527> 1 December 2003

Tobias, Marc. Locks, Safes, and Security Second Edition. Illinois: Thomas, 2000.

Evans, Jim. “A Gazetter of Lock and Key Makers”. 2002. URL: <http://www.localhistory.scit.wlv.ac.uk/Museum/locks/gazetteer/gazhaa-hog.htm> 26 November 2003

Zara, Louis. Locks and Keys. New York: Walker And Company, 1969.

McCloud, Mark. Visual Guide to Lock Picking Second Edition. Illinois: Standard Publications, 2002.

Niday, Tammy. Personal Interview at Custom & Security Hardware. 1 Dec. 2003

Blaze, Matt. “Notes on Picking Pin Tumbler Locks”.7 November 2003. URL: <http://www.crypto.com/papers/notes/picking/ > 5 December 2003

Johnson, Austin. “Splinter Cell Walkthrough”. 13 November 2003. URL: <http://www.gamespy.com/articles/november03/scwalk/index16.shtml> 1 December 2003

Pickmasters. “An Introduction to Fiber Picks”. URL: <http://www.pickmasters.net/newcon/fiberpick-moreinfo.html> 5 December 2003

Phillips, Bill. The Complete Book of Locks and Locksmithing Fifth Edition. New York: McGraw Hill, 2001. 335

Ted the Tool. “Guide to Lock Picking”. 1 September 1991. URL: <http://www.lysator.liu.se/mit-guide/mit-guide.html> 10 November 2003

Barry the Key, Hans Unicorn. “Lockpicking with Barry the key and Hans Unicorn”. 14 July 2000. URL: <http://www.connectmedia.waag.org/tool/h2k-lockpicking.wmv> 1 December 2003

simple3 "LockPick Contest?" Online posting 5 August 2003. URL: <http://forum.defcon.org/showthread.php?t=2119&highlight=lock+picking> 10 November 2003

Mini-Blue “a little advise for me?… and a story…” Online posting 18 November 2003. URL: <http://lockpicking101.com/viewtopic.php?t=857> 1 December 2003

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Alth, Max. All about locks and locksmithing. New York: Hawthorn Books, 1972.

Wanlass, Mark, Hall, Stan. “Impressioning Manual For Amateur Locksmiths” 1997. URL: <http://www.gregmiller.net/locks/impress.html> 26 November 2003

Fennelly, Lawrence J. Effective Physical Security Second Edition. MA: Butterworth-Heinemann, 1997. 145

Barry the Key, Glasser, Mark. “Lockpicking at Hope2k”. 14 July 2002. URL: <http://www.connectmedia.waag.org/tool/h2k2-lockpicking-vcd.mpg> 1 December 2003

Miller, Greg. “How to remove pins from a pin tumbler dead-bolt”. URL: <http://www.gregmiller.net/locks/disassemble.html >10 November 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of the Information Security Reading Room Author retains full rights.

Last Updated: May 25th, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	Cyberjaya, MY	Jun 03, 2013 - Jun 08, 2013	Live Event
SANS Pen Test Berlin 2013	Berlin, DE	Jun 03, 2013 - Jun 08, 2013	Live Event
Industial Control Systems Security Training - Houston	Houston, TXUS	Jun 10, 2013 - Jun 15, 2013	Live Event
Security Impact of IPv6 Summit 2013	Washington, DCUS	Jun 14, 2013 - Jun 16, 2013	Live Event
SANSFIRE 2013	Washington, DCUS	Jun 14, 2013 - Jun 22, 2013	Live Event
SANS Canberra 2013	Canberra, AU	Jul 01, 2013 - Jul 13, 2013	Live Event
Digital Forensics & Incident Response Summit 2013	Austin, TXUS	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS London Summer 2013	London, GB	Jul 09, 2013 - Jul 16, 2013	Live Event
SANS Rocky Mountain 2013	Denver, COUS	Jul 14, 2013 - Jul 20, 2013	Live Event
SANS Mumbai 2013	Mumbai, IN	Jul 22, 2013 - Jul 27, 2013	Live Event
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	Washington, DCUS	Jul 22, 2013 - Jul 26, 2013	Live Event
SANS San Francisco 2013	San Francisco, CAUS	Jul 29, 2013 - Aug 03, 2013	Live Event
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	Bangalore, IN	Aug 05, 2013 - Aug 10, 2013	Live Event
SANS Boston 2013	Boston, MAUS	Aug 05, 2013 - Aug 10, 2013	Live Event
Critical Security Controls Summit	Washington, DCUS	Aug 12, 2013 - Aug 18, 2013	Live Event
Industrial Control Systems Security Training - DC	Washington, DCUS	Aug 12, 2013 - Aug 16, 2013	Live Event
SANS Thailand 2013	Bangkok, TH	Aug 19, 2013 - Aug 31, 2013	Live Event
SANS Virginia Beach 2013	Virginia Beach, VAUS	Aug 19, 2013 - Aug 30, 2013	Live Event
Mobile Device Security Summit 2013	OnlineCAUS	May 30, 2013 - Jun 06, 2013	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced