Nifty Assignment – Lockpicking

Brian Leeper

University of Hawai'i Maui College

Table of Contents

Table of Contents **2**
Background **3**
Meta Information **3**
Supplies Needed **3**
Lockpick Set **4**
Locks **5**
Handout **6**
Assignment Instructions **6**
Lock #1 (clear introductory lock) **6**
Lock #2 (SEPOX lock) **7**
Lock #3 (Master Lock 140D) **9**
Check on learning **10**
Model grading criteria **10**

Background

Locks are an ancient technology that have maintained relevance in society throughout the centuries. Locks are an integral part of physical security—an oft overlooked component of information security. Locks are part of physical security systems which typically follow a defense in depth approach; as such, locks are not utilized as a stand-alone security mechanism but are implemented as one part of the whole system of physical security. Lockpicking is just one skill utilized to overcome a layer of physical security, an important component in electronic security. Much like more advanced cracking algorithms that employ a technique of trial and error, lockpicking provides a hands-on practical application of trial and error to open a lock, a rewarding exercise in and of itself.

Meta Information

Summary	Lockpicking – Identify various lock types utilized in physical security and implement techniques to overcome the most common lock, the pin tumbler.
Topics	Lock style variety, lockpick tools, lockpick techniques, physical security component
Audience	Appropriate for CS1 or later students at the start of a physical security lecture series as a part of information security. This assignment is engaging, hands-on and may be classified as a “CS Unplugged” exercise.
Difficulty	This is an introductory to intermediate level assignment, intended to be covered over the course of 1 to 3 days.
Strengths	Introduction to the vulnerabilities in locks, different lock types. Students also gain fun, hands-on learning with overcoming simple locks.
Weaknesses	May be difficult for some students to grasp ability to overcome locks.
Dependencies	Lockpick set(s), Padlock(s)
Variants	There are a variety of lock styles and the introductory intention of this course only covers one style in depth. Further research may be conducted on overcoming other locks.

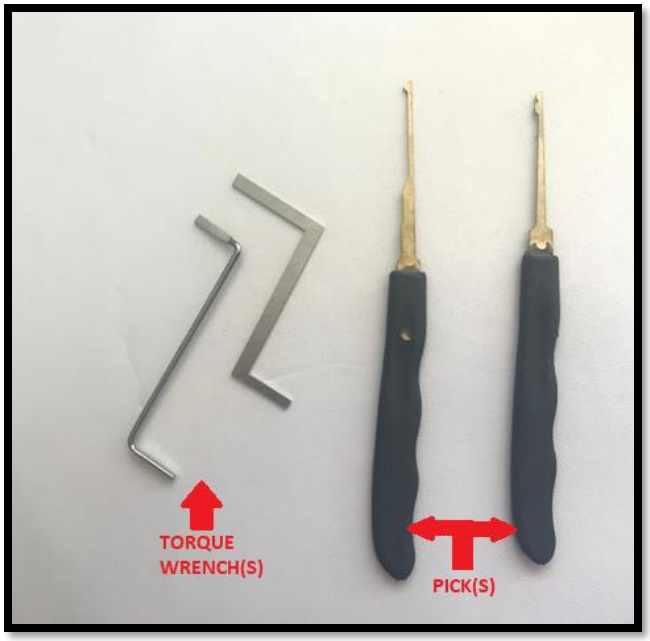
Supplies Needed

This assignment utilizes physical materials that must be purchased prior to the assignment. Two important supplies of note are a lockpick set and a small selection of locks. Due to the varying quality of locks between brand and manufacturing it is suggested that the common locks identified herein are utilized to teach the importance of physical security and lockpicking.

Lockpick set

The style or pick-count of the lockpick set utilized for the assignment does not matter as much as the set containing appropriate torque wrenches and a variety of picks or rakes (identified below). Pictured below are two separate lockpicking sets. Either set, or any similar, would suffice to complete the assignment.

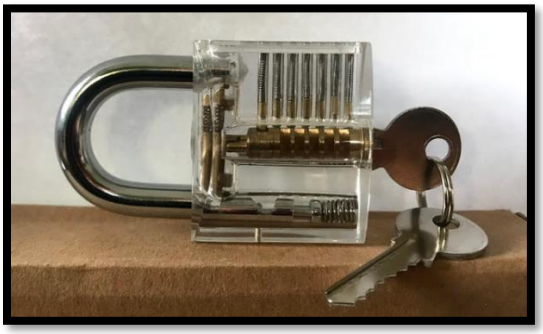
Included in the lockpick set should be a variety of torque wrenches and picks. Having a small variety is helpful when practicing on different locks. If the torque wrench is too small, it may bind within the lock and if the torque wrench is too large it will not fit within the keyway or will obstruct pick maneuvering. Pictured below are two examples of torque wrenches and picks included in one lockpick set.



Locks

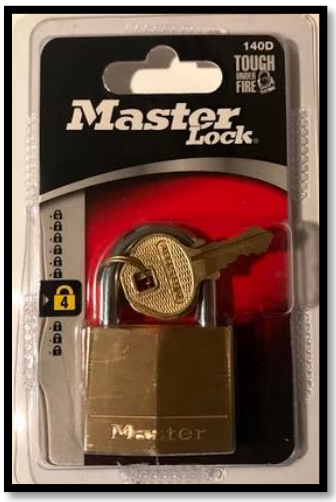
There are three recommendations for locks that fit within the specified scope of the assignment:

1. The clear, introductory lock that comes with most lockpick sets.



2. SEPOX, a heavily marketed Amazon brand that imitates a more secure brand (American Lock).

3. Master Lock 140D provides a challenge to the patient and persistent.



Handout

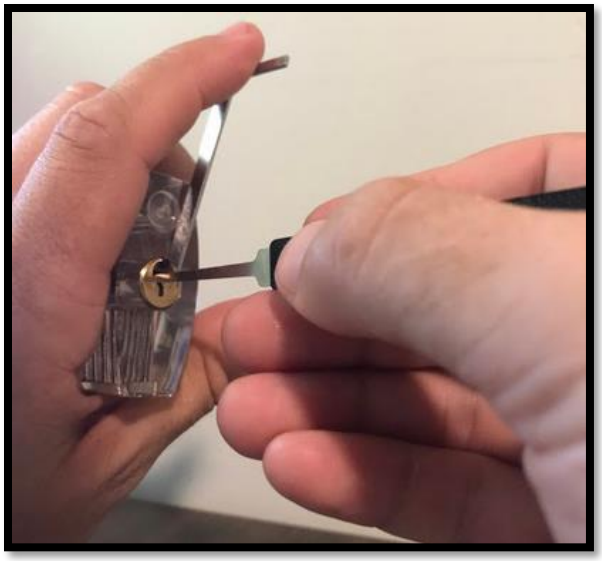
Assignment Instructions

1. Review the blogs at http://www.rekey.com/locksmith/types-of-locks and https://www.art-of-lockpicking.com/types-of-locks/ for information regarding a variety of common lock styles and implementations potentialities.
2. Review the article at https://www.scienceabc.com/innovation/pick-door-locks-pin-tumbler-sherlock-doors-open.html for an overview of the pin tumbler lock mechanism.
   2.1. The pin tumbler lock mechanism is the most widely recognized and utilized lock mechanism within the United States, present in many keyed locks and the basis of this assignment.
3. Pick your first lock (lock #1, the clear, introductory lock).
   3.1. The introductory lock is chosen for its simplicity and the inherent learning potential with being able to see the pins being manipulated within the casing.
   3.2. Insert the torque wrench into the top of the keyhole, opposite the pins (visible when you look into the keyhole).
   3.3. Hold the lock in a comfortable fashion with the keyhole facing you.

3.3.1. *EXAMPLE*: Right-handed picking—Form an ‘L’ with your left hand and with your right, place the lock into your left hand with the torque wrench towards the top. Wrap your thumb around the bottom of the lock. Place your index finger against the torque wrench and wrap your third, fourth, and fifth digits over the top of the lock. Your index finger will provide tension to the torque wrench.

3.4. Hold the pick as you would a dart, grasping it with your index finger and thumb, and insert the pick into the keyhole all the way to the back.

3.4.1.



3.4.2.

3.5. As you get near the back of the lock, begin applying very light tension to the torque wrench.

3.6. When the pick is at the back of the lock, begin drawing the pick forward, pushing gently against the key pins as you continue to provide even pressure on the torque wrench.

3.6.1. Do not provide all the leverage that you can against the torque wrench—only provide small amounts.

3.7. Reinsert the pick into the keyway, feeling for pins that are still protruding upwards as you insert the pick to the back and draw the pick forwards quickly, applying pressure against the pins.

3.7.1. The process of pushing and pulling the pick quickly against the pins is called zipping.

3.7.2. If the lock does not open within three to four zips, release tension on the torque wrench and reapply to loosen and release any binding pins.

3.8. Repeat the steps above until the lock is opened. The introductory lock may take less than 10 seconds to open but should not exceed 45 seconds. If it takes longer to open, continue practicing until it may be opened in less than 45 seconds.

4. Pick your second lock (Lock #2, SEPOX lock from Amazon).

4.1. The SEPOX lock was chosen for its heavy marketing within the Amazon marketplace and its imitation of a more secure and recognized brand, American Lock (see below for side-by-side comparison of lock images).

4.1.1.

4.2. Insert the torque wrench into the top of the keyhole, opposite the pins (visible when you look into the keyhole).

4.3. Hold the lock in a comfortable fashion with the keyhole facing you.

4.3.1. *EXAMPLE*: Right-handed picking—Form an ‘L’ with your left hand and with your right, place the lock into your left hand with the torque wrench towards the top. Wrap your thumb around the bottom of the lock. Place your index finger against the torque wrench and wrap your third, fourth, and fifth digits over the top of the lock. Your index finger will provide tension to the torque wrench.

4.3.2.

4.4. Hold the pick as you would a dart, grasping it with your index finger and thumb, and insert the pick into the keyhole all the way to the back.

4.5. When the pick is at the back of the lock, begin applying gentle pressure to the torque wrench. Rock the pick up and down within the keyway, keeping the pick entirely within the lock.

4.5.1. The process of rocking the pin up and down within the keyway is called rocking and may be performed with greater intensity.

4.5.2. If the lock does not open within a reasonable amount of time release tension on the torque wrench and try again. Consider applying the zip method as identified above in step 3.7.

4.6. Repeat the steps above until the lock is opened. The SEPEX lock may take less than 20 seconds to open but should not exceed 45 seconds. If it takes longer to open, continue practicing until it may be opened in less than 45 seconds.

5. Pick your third lock (Master Lock 140D).

5.1. The Master Lock 140D typically contains one-to-two security pins, providing a challenge to opening the lock.

5.2.

5.3. Utilizing the two methods identified above in steps 3.7 and 4.5 (zipping and rocking), the Master Lock 140D may be unlocked within 5 minutes.

6. Test different picks and torque wrenches in the locks to feel how different pick styles effect the pins.

Check on learning file

A check on learning definition matching activity is available.

Model grading criteria

Upon successful completion of this assignment, students should be able to identify, based on description, common locks implemented as part of physical security and a strategy utilized to overcome locks as part of physical security. Given the appropriate tools (lockpick set), the student should be able to pick the clear training lock and the SEPOX lock each within 45 seconds. The Master Lock 140D may prove more challenging and should be picked within 5 minutes.