
**How Locks Work**

A mechanical lock is made up of three parts: the cylinder, the hull, and pins. The pins, when aligned correctly, allow the cylinder to turn in the hull, unlocking the device. Pins are set to different heights that correspond to the heights of a key. In terms of computer security, these pin heights can be considered a password or capability. We can represent a key as a series of pin positions.

**Lock Picking**

Lock picking is an iterative process that lifts each pin in the cylinder in order to open the lock. Pins can be lifted one-at-a-time because of mechanical imperfections. It is almost impossible to set the pins in a cylinder in a perfectly straight line. When applying torque to the cylinder, one pin will "bind" and prevent the cylinder from turning further. This pin is then pushed up, allowing the cylinder to turn further and trap a new pin. The steps are as follows:

1. Insert tension wrench, apply torque.
2. Iteratively push each pin up the bound pin is discovered.
3. Push this pin up. The pin does not fall back down because of the torque.
4. Repeat until all pins have been pushed up.

Joe presented sample lock on piece of wood and two sets of lock picks for people to play with. Multiple students were able to pick the lock throughout the remainder of the presentation.

**Bump Keys**

A bump key is a key where every key is filed to the lowest position. It is physically employed in much the same manner as those swingy balls office art. The key is inserted into the lock and hit with a hammer from above. The force is transferred from the bump key to the bottoms of the pin to the middle cut sections of the pin, which raise out of the cylinder and allow the door to be open. Bump keys work better on cheaper locks and older locks that are more broken in. Bump keys do not work if there is a large shift in pin size because of gravity.
Master Keys

Master-Keyed mechanical locks work by using pins that are cut in two places. One of the cuts is used for an (unprivileged) change key that opens a single lock, while the other is reserved for a master key that opens many locks. In much the same way that lock picking searches the keyspace of the pins, one can also search the keyspace for the master key. This is a privilege escalation attack. With a valid change key, one can create keys that test a single pin at a time until the other acceptable pin height is discovered. A minimum of $Pins + 1$ keys is required, a very small number, by setting the current pin to the tallest height and then filing it down. This attack requires up to $Pins(Heights − 1)$ probes but may as little as two dollars.

Shims

Shims are an attack against padlocks. They differ in that they bypass the cylinder to attack the locking mechanism itself. Shims can be made by taking slices of aluminum can, wrapping it around the inside of the lock, and pushing down. When the shim is slid into the padlock it moves the locking mechanism open.

Applied Security

Challenge: make a bump key and a master key for Deschutes Hall. This would only require 8 blank keys (6 keys for pin testing, 1 for the master, 1 for the bump). Deschutes uses Schlage D series locks. Joe was unable to purchase Schlage D keys from True Value because Schlage requires special authorization to ship this key. Joe tried to call the UO Lockshop and ask for some blanks, but they were also unwilling to fulfill his request. In act, the UO has paid five figures to make sure blanks were not available for their locks.

The representative from the UO Lockshop was very helpful though. It turns out that Blaze’s attack would not work well anyway because the UO employs a five level lock system (change keys, sub-master, master, grand master, great grant master, great great grand master). Multi-level security! We realized that students with offices on the second floor must have sub-master keys, since our key also works on the stairwell door. Professor Butler must have a master key since his can open all graduate student doors.

Bump keys might not work because of the tightness of the milling. In fact, 5% of the change keys the UO Lockshop gives out do not fit into the cylinder because the milling is so tight. UO does not use pick resistant pins though. This leaves only UO padlocks vulnerable. Joe set out to shim the padlock to the roof of Deschutes Hall, but it was not necessary because the padlock was open, proving that physical world security is just as laughable as the digital world’s.

Questions

Kofi Appiah asked a question about pick resistant locks. Joe shared MIT Guide to Lock Picking and a graph of the Pressure required to move pins. Joe also discussed lock scrubbing, which is a faster type of picking that iteratively pushes up the lowest remaining pin.