Keys Open Doors

Joe Pletcher
University of Oregon
Physical Security
Disclaimer

• Don’t get caught
• Don’t be stupid
• No really, don’t get caught
• For real, don’t go breaking into things. It’s an invasion of privacy, it’s not that cool, and it’s probably illegal
• These things can break locks. That’s damage to other people’s property. Don’t do it
• If you’re going to do something stupid or cool, invite me so I can watch or participate
Keys Open Doors: Outline

- Basic outline of locks
- Lock picking
- Bump keys
- Making Master keys
- Shims
- Applied Security
- Conclusions
Locks
Locks
Locks
Locks

• We have “pins” (5) of different heights
• The key is cut to different heights
• The key is inserted and causes the gaps in the pins to line up
• This lets the cylinder turn, and the lock opens!
• We can view a key as a password (or a capability!)
Does this make sense

• This is important
• No really, the rest of the presentation isn’t going to make sense
• Tell me if you don’t understand
• We can represent a key as a series of positions.
  – For Example: pin 1: 4, pin 2: 2, pin 3: 5
  – This would be a 3 pin lock with the key 425
Picking

- Iterative process
- We’re going to apply some torque to the cylinder
- This will cause one or more pins to “bind”
- From there, we can push that pin up
  - This will let the cylinder turn ever so slightly
  - Traps the pin
Picking
Picking
What’s happening here

• We have a tension wrench applying torque to the cylinder
• This causes a pin to stop the cylinder from turning
• We can push that pin up, which causes the cylinder to turn slightly, and “sets” that pin
• Repeat until all pins are set
Does this make sense?

• We’re covering a lot quickly
• This exploits a mechanical flaw in locks
  – The pins are not usually set in a perfectly straight line
  – We’re talking really, really small tolerances
  – Imagine brute forcing a password where we know when a character is correct
• This is one way we can exploit this mechanical system. There are others
Bump Keys
Bump Keys
Bump Keys

• This works better on cheaper locks
• This works better on older locks
• This will not work if there is a large shift in pin side (ex: a 1 next to a 9)
  – Why? Gravity
• This is way easier. You need a blank and a hammer
Master Keys

• Start with a base case. We have a 5 pin lock, and we add a gap to a single pin
  – For example, let's say our key is 12345
  – Let's cut our last pin to also accept 1
  – Now we also accept 12341
Master Keys
Master Keys

• (Finally) The Blaze paper
• Just like we can search the keyspace with a pick, we can search for a master
• Pretend we have a change key that’s 44444 and the master that’s 11111. That means 44441, 444411, 44111, etc all work
• So, cut a 44449 key, and file down the first pin until it works (and isn’t 4 obviously)
• Repeat
Master Keys

• This takes \#pins + 1 keys
• Requires P(D-1) probes, but we get a ton of “free” probes by cutting the highest position first
• Under two US dollars
Shims

• Attacks against padlocks
• Note, that picking, bump keys, and master key attack all also work against padlocks
• This is basically the “opening a door with a credit card” trick you see in movies
• Attacking the latching portion of the lock
Shims
Shims
Shims

- Shims are pretty straightforward
Applied Security

• The fun stuff!
• So, after all this, lets see if we can’t pull some of this stuff off
• Let’s make a UO master key for Deschutes!
• And a bump key!
• We just need blanks…
Applied Security

- So it turns out that we have something called Schlage D series locks
- I’ll just head down to True Value and pick some up
- “…D Family restricted key blanks are not stocked by locksmiths or other dealers. Schlage requires a letter of authorization from the end user before shipping restricted keys…”
- So I end up calling the UO lockshop, asking for some blanks…
Applied Security

• However, the UO lock guys were very, very helpful
• UO has paid five figures to have blanks not be available
• The Blaze attack will work on any two level lock
• UO uses a five level lock system
  – Change keys, sub-master, master, grand master, great grand master, great great grand master
Applied Security

• Bump keys might work, but probably not due to the tightness of the milling
  – 5% of change keys on UO’s campus don’t even fit into the locks

• UO does not use pick resistant pins

• So that leaves us with shims… what is protected by padlocks?
Applied Security
Applied Security

• Ladders to the roof are protected by padlocks
• Padlocks can be opened with shims…
• No one is in Deschutes on the first day of classes…
Applied Security
Applied Security
Applied Security

• The really funny part – it was just open. I didn’t shim anything

• Lesson: Physical World Security is just about as relaxed as online security

• So, while I was getting on the roof I noticed something else. Another tool you can use to get past the doors…
Applied Security

- Yes, the hinges are inside the door
Conclusions

• Security by obscurity doesn’t work
• Locks function largely by obscurity
  – Case in point: the first time I tried to pick a lock it took me 20 minutes
• Physical World Security has many parallels to Fake World Security
• All locks can be defeated. This is why good locks only offer time assurances