Locks and Keys
What Is Physical Security?

• Any physical object that creates a barrier to unauthorized access

• This includes: locks, latches, safes, alarms, guards, guard dogs, doors, windows, walls, ceilings, floors, fences, door strikes, door frames and door closers
Is Physical Security An IT Concern?

• You have been working hard to secure your network from cyber attacks
  – Redundant layers of antivirus programs, firewalls and intrusion detection systems should protect against every possible electronic method of entry

• But what if an attacker gains access to the server room or network wiring closet ...

• Is your network still safe?
Destructive vs. Nondestructive Entry

• **Destructive entry**
  – Involves using force to defeat physical security
  – Methods involve crowbars, bolt cutters and sledge hammers
  – Negative impact on IT resources is apparent
  – Remediation steps also obvious

• **Nondestructive entry**
  – Compromises security without leaving signs of a breach
  – Defeats intrusion detection
  – Greater and long-term threat
Compromising Locks

• For centuries, the lock has been one of the cornerstones of physical security
  – We rely on dozens of them every day to protect people and assets

• The trust most people place in locks is unwarranted
  – Most locks can be easily compromised with nondestructive methods
  – Sometimes within seconds and with readily available tools

• “Locks keep honest people honest”
Lock Picking

• Lock picking had been the exclusive art of locksmiths, professional thieves, spies and magicians for hundreds of years

• However, with the advent of the Internet, information about lock picking methods and tools has become readily available
  – E.g., YouTube has many lock picking videos
Pick vs. Bypass

Break open a lock in a nondestructive manner can be achieved either through:

• **Pick**: acting on the lock mechanism simulating the operation of the key
• **Bypass**: manipulation of the bolt without using the lock
1860: Yale Pin Tumbler Lock

- Modern version of the Egyptian single-pin design
- Utilizes two pins for locking
- Double-detainer theory of locking
- Created shear line
How Does a Pin Tumbler Lock Work?

1. When a key is not present, the pin stacks are pushed down by the springs so that the driver (top) pins span the plug and the outer casing, preventing the plug from rotating.

2. When the correct key is inserted, the ridges of the key push up the pin stacks so that the cuts of the pin stacks are aligned with the shear line.

3. The alignment of the cuts with the shear line allows the plug to be rotated.

Images from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2
How Does a Pin Tumbler Lock Work?

- If an inappropriate key is inserted, then the pins do not align along the shear line and the lock does not turn.

Figure 2.2: Opening a tubular lock: (1) Closed lock. Image included with permission [68]. (2) After inserting the key. Image included with permission [69]. (3) Open lock. Image included with permission [70].
LOCK PICKING

Photo by Dan Rosenberg included with permission.
Terminology

- shell or hull
- tumbler
- spring
- sheer line
- cylinder or plug
- keyway
- driver
- top or driver
- pin
- bottom or key

Image from http://en.wikipedia.org/wiki/File:Pin_tumbler_with_key.svg used with permission under Gnu Free Documentation License 1.2
Lockpicking Tools

- Feelers
- Scrubbers
- Tension tools

Photo by Jennie Rogers included with permission.
Feeler Picking

• Apply light tension
• Lift one pin at a time
  – Identify binding pin
• Lift binding pin until it reaches the shear line
• Setting the binding pin will rotate the lock slightly
• Find next pin and repeat the process
Scrubbing / Raking

- Apply light tension
- Work over pins back to front in a circular motion
  - attempting to pop them into the shear line with the combination of tension
- Good for beginners
- Usually employ snake pick or half diamond

Photo by Jennie Rogers included with permission.
The Math of Lock Picking

• Suppose we have
  – 40 different kinds of key blanks
  – 7 pin positions
  – 8 different possible pin heights
• Then the total number of possible locks is
  – $40 \times 8^7 = 83,886,080$
• Not all these are possible, however, as it is difficult to put long teeth next to small teeth.
Rights Amplification in Master Keyed Systems

Reverse engineer master key from change key

Each lock has $P$ pins, with $D$ potential cut heights

Create $D-1$ test keys for each pin position $p$

Cut all pin positions except $p$ as known change key
Rights Amplification (continued)

Query the lock until you find each pin position

i.e. To determine first key cut depth insert each of the D-1 test keys and determine which one does not bind to the pin

Repeat for each pin
Rights Amplification Statistics

Consumes $P(D-1)$ blanks

Can reduce to $P$ blanks and file down on the fly

But this looks suspicious

Search space is practically pruned by manufacturer specs

- maximum distance limit in legal adjacent cuts
- Older installations sometimes require MKs to be higher on the pin stack
Tubular lock

- Usually on car alarms or vending machines
- 6-8 pins
- Easy to pick with special tool
- The tool could become a new key

Images from http://en.wikipedia.org/wiki/File:Tubular_locked.png used with permission under Gnu Free Documentation License 1.2
Statistics

• 4-6 pins, 4-10 levels
• $10^6 = 1,000,000$ possible keys!
• The angular positions of the cylinders allow to obtain about 180 different positions $(180\cdot10)^6 = 3.4012224 \times 10^{19}$
• (Un) fortunately there is a need for some tolerance in locks
Combination Locks

• There are locks that do not require a physical key to be opened but a code

• Number of combinations is
  – Number of digits times
  – Length of combination

Combination Locks

• Inexpensive combination padlocks allow attacks based on reducing the space of possible combinations to try
  – The gears have a higher tolerance of the external disk combination
  – Nominal number of combinations is \(40^3 = 64,000\)
  – Possibilities can be reduced to about 80 by detecting critical gear points

E.g., see http://www.wikihow.com/Crack-a-%22Master-Lock%22-Combination-Lock
Bumping

• A different way of picking locks
• Virtually all traditional Yale and similar locks can be opened by bumping

• What lock pickers say about bumping:
  — RELIABLE
  — REPEATABLE
  — SIMPLE TO LEARN
Bump Keys

- Driver pins “jump” higher than the cylinder just for an instant
- If a light rotational force is applied, the cylinder will turn
- Lock bumping is a very fast method for opening the lock
- The lock is not damaged in any way
- Few key-pin locks cannot be bumped

Photo by Jennie Rogers included with permission.
Pick Gun

- **Manual and electronic pick guns** are a popular method for quick and easy ways of opening up doors.
- The pick gun is used in a similar way but usually has a **trigger** that creates an upward movement that must be repeated rapidly to open the lock.

Side Channel Attacks

• Rather than attempting to directly bypass security measures, an attacker instead goes around them by exploiting other vulnerabilities not protected by the security mechanisms.

• Side channel attacks are sometimes surprisingly simple to perform.