Week 13 - Wednesday

COMP 4290

Last time

- What did we talk about last time?
- Security planning
  - Security plans
  - Business continuity plans
  - Incident security plans

Questions?

Project 3

Hussein Al-Ani Presents

Physical Security

Natural disasters

- Flood
  - Water is problematic, but usually there's some warning
  - Hardware and software is replaceable
  - Data often is not
    - Backups should be made
    - Critical hard drives should be marked so that they can be removed first
- Fire
  - Fire is worse
  - There is usually less time to react and the threat to humans is bigger
  - Fire suppression systems for computing facilities should not use water
    - Using CO_2 or similar is good for computers but can kill humans
- Everything else
  - Have contingency plans
  - Insure physical assets
  - Maintain off-site backups of critical data

Power issues

- Power loss
  - Causes vary
  - In some countries, multiple power losses per day are routine
- **Uninterruptible power supplies** (UPS)
  - Stores energy when there is power so that you can keep your systems running when there isn't
  - Consumer UPSs are usually batteries
    - Not a good solution for a large data center
  - Large scale solutions are kinetic storage systems or generators
  - UPSs generally only give you enough time to save data and do a safe shutdown
- Surge suppressor
  - Power is not constant and can have **drops**, **spikes**, and **surges**
  - Surge suppressors are inexpensive and should be used for all computer power supplies
  - If possible, computers should be disconnected from power (and from phone and other outside lines) during a thunderstorm

Human vandals

- Unauthorized access
  - With networked systems everywhere, people eavesdropping on connections is easier
  - Normal employees are also using computing resources for personal use
- Theft
  - PCs, laptops, phones, tablets, and portable media are easy to steal
- Preventing access
  - Use a guard, a lock (traditional or swipe card)
- Preventing portability
  - PCs can be locked to the desk
  - Motion sensors to see when someone is where they shouldn't be
- Detecting theft
  - RFID tags

Disposing of sensitive information

- Shredding paper documents
  - Some kinds of tape can also be shredded
  - High sensitivity data should be burned after shredding
- Overwriting magnetic data
  - Deleting files does not stop digital forensics experts
  - Data on disks should be overwritten many times with random patterns of 1s and 0s (burning)
- Degaussing
  - Passing a disk through a magnetic field so intense that all data is lost
- Van Eck phreaking safeguards
  - Many computer components emanate electromagnetic radiation that can be reconstructed
  - Tempest is a government certification standard for blocking these emissions (meeting the standard can be expensive)
  - An entire building (such as the NSA headquarters near DC) can be shielded in copper to protect emissions

Backups

- Everything should be backed up, always
- A complete backup covers the current state of all data
- Revolving backups keep the last few complete backups
- A selective (or incremental) backup stores only the files that have changed since the last backup
- Ideally, you should have an offsite backup of all your data in case of fire or flood
  - Writing your critical data to a USB drive and keeping it at home or school or vice versa is a good idea for you guys

Recovery

- Networked storage can allow for continuous offsite backups and make recovery easier
- If a computing center is destroyed or unusable, a **cold site** or **shell** is a facility with power and cooling where you can quickly rebuild a data center
  - You have to supply the hardware
- A **hot site** has ready to run computer systems of the kind you might need
  - You can pay a monthly fee to be ready to move into such a site at a moment's notice
  - A kind of data availability insurance

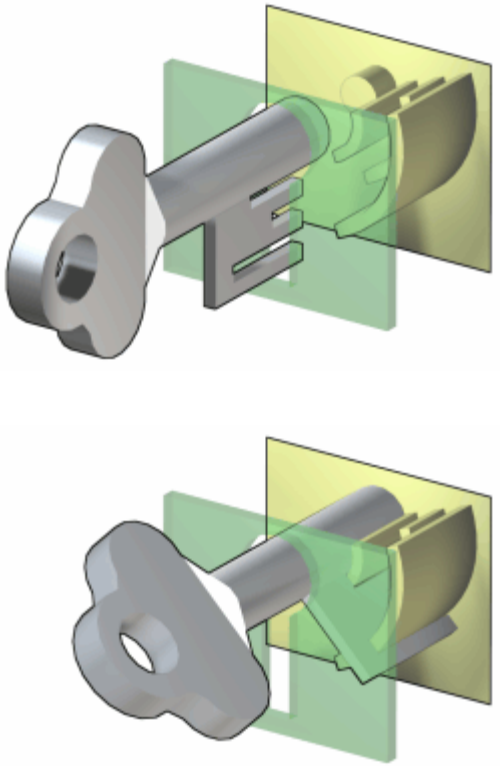
Lockpicking

Locks

- Locks have been in use since ancient times and probably developed independently in the great ancient civilizations
- Locks you are likely to run into are:
  - Warded locks
  - Wafer tumbler locks
  - Pin tumbler locks
  - Combination locks

Warded locks

- **Warded locks** have existed since antiquity
- The shape of the key must be able to pass through and around wards, shapes that could block poorly made keys
- Warded locks provide poor security but are still used for sheds, cabinets, and other low security applications

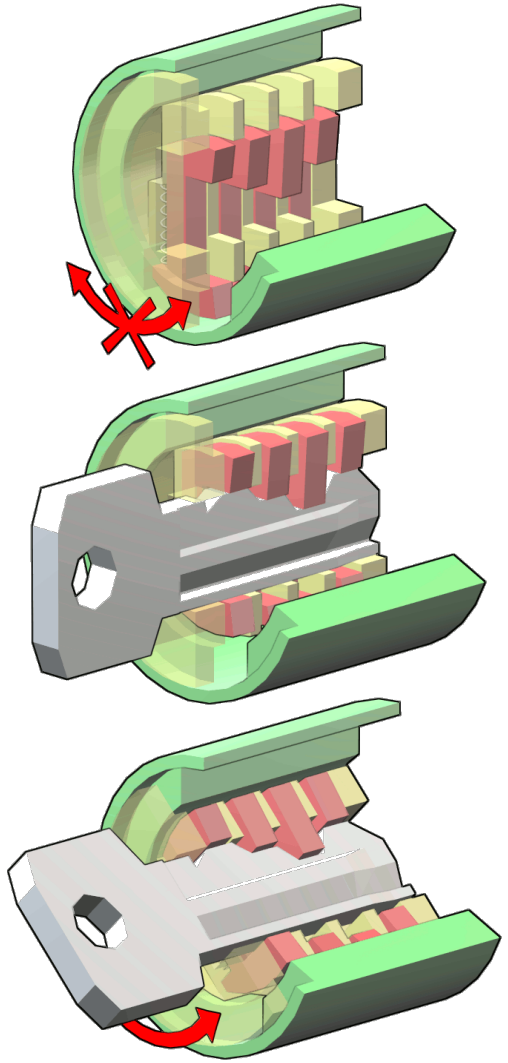


Skeleton keys

- All warded locks have the problem that they can be defeated by a **skeleton key**, a key stripped down to only the part needed to turn the mechanism
- In popular culture, the term skeleton key is often misused to mean old style keys for warded locks in general

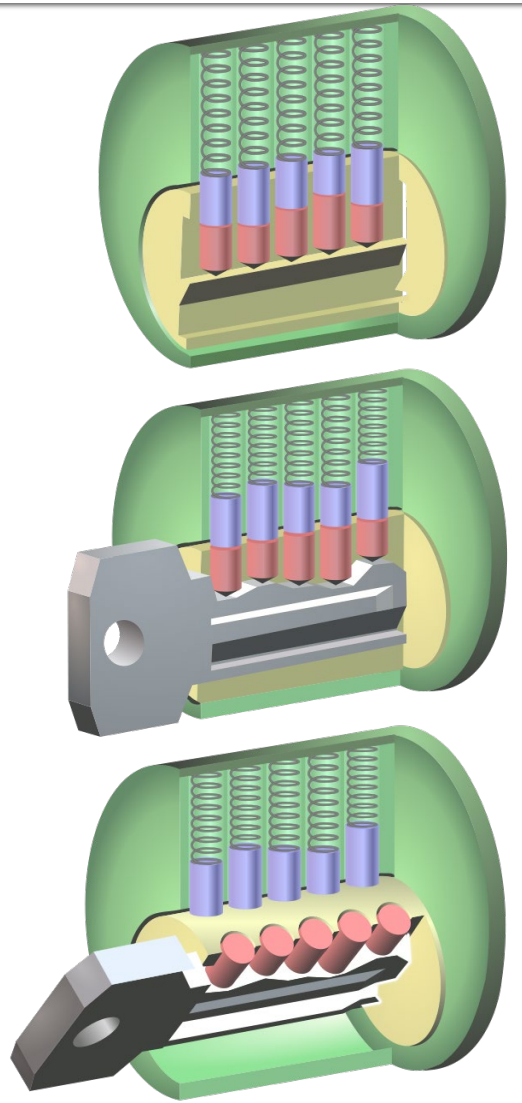
Wafer tumbler locks

- **Wafer tumbler locks** have better security than warded locks
- A series of wafers blocks the rotation of a plug
- When a key pushes each wafer up to an appropriate height, the plug is free to turn
- They are picked in the same way as a pin tumbler lock, but they are easier because you can't push them up too far and you can generally pick each wafer in sequence



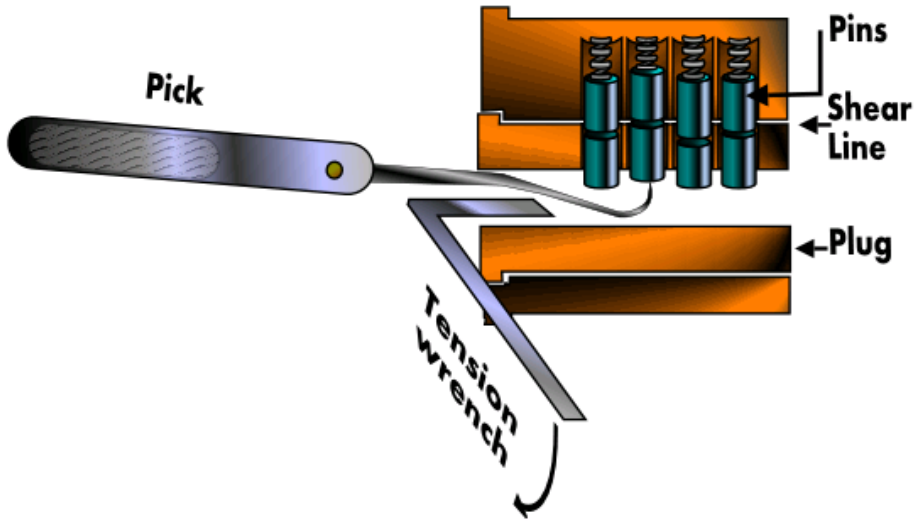
Pin tumbler locks

- Most house locks, office locks, and many car locks are **pin tumbler** locks
- Pin tumbler locks are similar to wafer tumbler locks
- A series of two part pins blocks the rotation of the plug
- A key that pushes all the pins up to their shear lines will allow the plug to turn
- Pins that are too high or too low will block the plug
- Pin tumbler locks can offer relatively high security at a reasonable cost



Picking locks

- Picking a pin tumbler (or wafer tumbler) lock is done by manipulating each pin (or wafer) into the correct position
- It is impossible to machine a lock perfectly, thus, if you try to turn the plug, one pin will be holding more pressure than the others
- If you can push that pin up to the shear line, it will snap in place, and another pin will now be holding more pressure
- If you can move through all the pins without letting any drop, the plug will turn



Tools of the trade

- You must apply a constant steady turning pressure while picking a lock
- This pressure is supplied by a **tension wrench**
- The wrench is usually just an L-shaped piece of spring steel
- **Picks** are also pieces of spring steel with a tip that is good for manipulating pins
- Popular picks include hook, ball, half diamond, and other types
- A pick set with a tension wrench and broken key extractor can be bought for around $20 on the Internet

Combination locks

- Removing combination locks without knowing the combination is called **bypassing** the lock
- Some techniques rely on hearing or feeling clicks made when turning the cams, particularly when pressure is applied to the shank
  - Multiple dial combination locks are vulnerable to this attack
- All combination locks can be bypassed by brute force (if you have the time)
  - Many of the methods rely on the fact that low-security locks are engineered with several digits of play
  - This play can be exploited for drastically reduced brute force times (usually still hours)

Ticket Out the Door

Upcoming

Next time…

- Protecting programs and data
- Intellectual property
- Information law
- Samuel Costa presents

Reminders

- Finish Project 3
  - **Phase 1 due Friday!**
  - **Files will be posted on Saturday**
- Read sections 11.1 and 11.2