What's CIA?

C - Confidentiality (only those with permission should see it)
I - Integrity (what I'm looking at should be correct)
A - Availability (it should be readily available to a reasonable degree)

Attacks:

On Confidentiality
- Databases get exposed (Ashley Madison)

On Integrity
- Makes the data encrypted/hard to see

On Availability
- Creates downtime (DDOS)

Attacks are also rated Low/Medium/High based on how impactful they are to the system.

Security is hard because:

- The environment is constantly changing
- System must be usable on top of being secure
- The attacker only needs one way to get in, all avenues need to be protected
- The security features themselves can be attacked
- Requires regular monitoring
- Often an afterthought

One of the most common attacks is after a fix in the system (ex. Windows) has been released, the attacker uses the exploit listed to attack users before updating.

Security in a company is not important until there is a breach.

The more security that is in place, the more difficult it is to use the system.

What are we protecting?:

- Data (very important as data is effectively money)
- Communication facilities (ability to talk/discuss or even the network itself)
- Hardware
- Software (free once virus-checking software is out of the picture)

Passive attack is an attack where the attacker watches and observes to get sensitive data

Active attack is one in which access is used to deny service or compromise data
Inside attacks usually involve humans and can compromise the system to outside attacks from inside the security parameter.

Outside attacks exploit weaknesses in the system to attack from outside the security parameter.

Prevention/Detection

- Prevention - stopping the attack from happening in the first place
- Detection - noticing that an attack is happening, and recovering from the attack
- Recovery - recovering from the attack using backups or other means

The point of system security is to minimize the overall risk.

Fundamental Security Design Principles:

- Economy of Mechanism - AKA "Keep it simple stupid"
- Fail-safe default - default to no, code for inclusion, not exclusion
- Complete mediation
- Open design - do not implement security through obfuscation (hiding facts doesn't make it safe)
- Separation of privilege - break up privileges between users
- Least privilege - normal users do not need access to root
- Least common mechanism - organize privileges per user (what does the user need access to do their job in the system?)
- Psychological acceptability - make it reasonable to use
- Isolation - firewalls, create a wall to look at anything coming into the system
- Encapsulation
- Modularity
Layering

Least astonishment - make the system not confusing, try to make things intuitive for users

Most passwords are not hacked, they are stolen.

Port is a mailbox on a system
  each port corresponds to a different communication avenue
  anything under 1024 is reserved by kernel