Computer Security:
- Various measures to protect computer related assets from a variety of attacks.
- All about minimizing overall risk.

CIA: Confidentiality, Integrity, Availability
- **Confidentiality**: preserver authorized restrictions on disclosure of information.
- **Integrity**: Guarding against and insuring information is not improperly modified or destroyed.
- **Availability**: Insures a timely access to information and that systems work promptly.

Security Difficulties:
1) Computer Security is not as straight forward as it first appears.
2) Mechanisms to defend against attacks might also be vulnerable to attacks.
3) Because mechanisms are at risk of being attacked they can be complex and hard to understand at first.
4) Must decide where to place various mechanisms both in the physical aspect and logical aspect.
5) Mechanisms usually involve “secret” info that the participant must obtain. Complications arise in how to create, distribute, and protect this info.
6) Battle of wits between attacker and designer.
   - Attacker only needs to find one hole in security.
   - Designer has to find and fix all of the holes in system.
7) Users don’t see need for security until it is too late
8) Requires regular monitoring or system.
   - Big problem for small businesses
9) Security is usually an afterthought once the system is designed.
10) The more security a system has the harder the system becomes to use.
11) Dynamic
12) Even when fixes are released attackers are quick to find a way around the fix.

What Gets Attacked (Assets):
- Data: Most common thing to be attacked, Data is money.
- Network Access
- Hardware
- Software

Attack Types:
- **Passive**: all about getting to data, does not affect system.
- **Active**: gets data, but also attempts to alter system.
- **Outside**: Denial of service by attacking a port.
- **Inside**: Usually involve humans, angry engineer.

How to Stop Attacks:
- **Prevention**: stopping the attack from ever happening. Best way of doing things
- **Detection:** noticing that something has changed and then doing something about it. Usually recovery.
- **Recovery:** Restore and/or fix changes.
  - Reloading the entire system

**Basic Design:**
- **Economy of mechanism:** keep things simple.
  - More complex mechanisms introduce more problems
- **Principal of least privilege:** only give someone as many privileges as they need to complete a task.
- **Fail Safe Default:** can only enter when give permission to enter.
  - Inclusion, not Exclusion.
- **Complete Mediation:** Every time someone does something, check and make sure they are allowed to do it.
- **Open Design:** Allow people to see code and attempt to break it.
- **Least common mechanism:** Split up tasks among available mechanisms
  - Don’t have one server do every job, it will crash
- **Isolation:** put up firewalls
- **Modularity**
- **Encapsulation**
- **Layering**
- **Least Astonishment:** Don’t confuse the people using the mechanism.
- **Psychologically Acceptable:** Can’t be too hard to use.

**Categories of Vulnerability:**
- Corrupted (loss of Integrity)
- Leaky (loss of confidentiality)
- Unavailability or very slow (loss of availability)

Threats are potential security risk to assets. It is a threat until it is done then it is an attack.

**Threat Consequences:**
- Unauthorized disclosure:
  - **Exposure:** Data is directly released to unauthorized entity.
  - **Interception:** an unauthorized entity accesses data as it is travelling between to authorized points
  - **Inference:** an unauthorized entity indirectly accesses the data by collecting other related data and inferring from that.
  - **Intrusion:** an unauthorized entity finds a way around security to get to data.
- Deception:
  - **Masquerade:** an unauthorized entity gains access to a system or performs malicious acts by posing as an authorized entity.
  - **Falsification:** false data deceive an authorized entity.
  - **Repudiation:** an entity deceives another by falsely denying responsibility for an act.
- Disruption:
- **Incapacitation**: Prevents or interrupts system operation by disabling system component.
- **Corruption**: Slightly modify functions or data which causes system modifications.
- **Obstruction**: overwhelm the system with commands to stop it from working.
  - **Usurpation**: privilege escalation
    - **Misappropriation**: someone assumes unauthorized logical or physical control of system resource.
    - **Misuse**: causes a system component to perform in a way it is not meant to perform.

**Ports**: a mail box on a system. A way to communicate with a system.

**Assurance**: Degree of confidence on security.

**Evaluation**: system of examining for security.