**1 Introduction to Security**

Security Basics

* Computer security - Refers to a single devices protection (subset of network)
* Network security - Refers to devices and communication between devices
* Protection (prevent attacks) and fault tolerance (keep operating after attack)
* CIA
  + Confidentiality
    - Data secrecy: Keep data from unauthorized subjects
    - Privacy: Control who can access data
  + Integrity (authenticity)
    - Data integrity: Keep data from being modified
    - System integrity: Keep systems functioning as intended
  + Availability
    - Keep system running and responsive to legitimate clients
* Policy: Deciding hat CIA mean in a given context
* Mechanism: Implementation of policy i.e. firewalls, file system access controls

Security Goals

* Attack prevention: Impossible for the attack to succeed
* Attack detection: Low false positives, false negatives and detection delay
  + False positive: detected an attack that did not occur
  + False negative: attack missed by system
* Attack response: Retaliation, observation, recovery
* Attack recovery: Remedy the effects of the attack
* Examples of CIA threats and defenses:
  + C. Sniffing on open net using tools like WireShark, defended by encryptions and using secure networks
  + I. Email spoofing verified using PGP signatures
  + A. DDoS defended by replication and firewalls

Threats

* Breaking into Computer
  + Replay: Capture the data on the network to replay it at another time
  + Vulnerability: Weakness in the system that when exploited makes the system behave in a way that the system’s creator did not expect
  + Exploit: Set of steps that exercise the vulnerability
  + Examples are sniffing, breaking, social engineering, impersonating
* Attacking the Computer
  + DOS attack: Aims to disrupt a service by exploiting vulnerability or sending a lot of zombies to a service provider
  + Virus: A self replicating program that requires user action to activate
  + Worm: A self replicating program that does not require user action
* Stealing information - cipher breaking and anonymization hinders
* Pivoting target computer to attack others
  + IP spoofing: Using a false IP address in the sender field of IP packets

Challenges

* Tragedy of the Commons: Freedom to exploit a common resource quickly which destroys resource as individuals take for themselves
* Fighting a live enemy - constantly adapting and learning
* Scarce attack data, hard to replicate legitimate attack traffic