CSC369 Week 11 Notes

Hyungmo Gu

June 1, 2020

- Security *
  - Computer Security
    * Techniques for **computing** in the presence of adversaries
    * Four requirements of security
      1. **Confidentiality:**
         · Preventing unauthorized release of info
      2. **Integrity:**
         · Preventing unauthorized modification of info
      3. **Availability:**
         · Ensuring access to legitimate users
      4. **Authenticity:**
         · Verifying the identity of a user
    * Protection is about providing all of the above on a single machine
      · Is usually considered the responsibility of the OS
  - Cryptography
    * Techniques for communicating in the presence of adversaires
- Types of Threats *
  1. **Interception or eavesdropping:**
     - Attacker gains knowledge tey should not have access to
     - is attack on *confidentiality*
     - Reading or copying files that attacker should not have access to
     - Intercepting network packets
  2. **Modification:**
     - Attacker alters existing files, programs, packets, etc.
     - is attack on *integrity*
     - e.g. Starcraft map hack
  3. **Theft of Service:**

   - Happens when attacker installs daemon
   - Is attack on *availability*
   - e.g. installing Daemon Tools Lite to run favourite Starcraft without CD Key

4. **Fabrication:**
   - Attacker creates counterfeit objects (files, messages, etc) which appears to come from a trusted source
   - Is attack on *authenticity*
   - e.g. Fake TD Easyweb website

- Vulnerabilities in the System *
- Malicious Software (Malware) *
- Stack & Buffer Overflow Attacks *
- Security Design Principles *
- Princple of Least Privilege *
- Access Control Lists *
- SSL *