

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 they should not have access to
 - Success → loss of confidentiality
 - Reading or copying files that attacker should not have access to
 - Intercepting network packets
 2. **Modification:**
 - Attacker alters existing files, programs, packets, etc.
- Vulnerabilities in the System *
- Malicious Software (Malware) *

- Stack & Buffer Overflow Attacks *
- Security Design Principles *
- Principle of Least Privilege *
- Access Control Lists *
- SSL *