Secure Computing Notes - Fall 2025

Day One:

Introduction to Secure Computing Part One

XAMPP - PHP

Course Objectives

Understand common threats, exploits, and develop software that is more threat-resistant.
Understanding securing information through

- Confidentiality (Encryption)
- Integrity (Digital Signatures)
- Authenticity (Digital Certificates)
- Access (passwords and permissions)

Disaster and Event recovery

Concepts:

Defense in Depth: Layers of security controls, controls can be physical, technical or administrative.

CIA: Confidentiality - How sensitive is the information and prevents it reaching the wrong people. Integrity - Assurance that data is not altered or destroyed in an unauthorized manner. Availability - Continuous operation of computing systems (Prevent denial of service attacks for example)

Common Terms:

Bug
Defect
Weakness

Exploits: an attack that takes advantage of vulnerabilities in applications, networks or hardware

Hacker (White, black or grey hat)
Intruder
Cracker

Spammer

Is all spam malicious?

A lot is things like spam emails like fashion nova not all malicious

NVD

National Vulnerability Database

Common Vulnerabilities and Exposures (CVE)

DLP (Data Loss Prevention)

Software designed to detect data leaks or breaches

Intrusion Detection / Prevention System (IDS/IPS)

Located behind the firewall on protected network

Detects and logs abnormal traffic based on signatures

Response capability based on signature = IPS

Firewall

Device at network perimeter which will filter out traffic as programmed by administrator

Web Content Filtering

Now used to block malware, but was originally used for stopping people from getting to specific websites

BlackList and Whitelist

Part 2 - Understanding Security

Physical Security - (Buildings, devices, hardware)
Network Security - (Connectivity, access, availability, audit)
Data Security - (Confidentiality, integrity)
Application Security - (exploits)

Goals - Protect confidentiality, maintain integrity, assure availability

Attack Trends - Growing incident frequency, and growing in randomness in victim selection.

Growing malevolence as well, most early attacks were not malicious, but now are the norm with significant financial loss.

Growing Attack Automation

Attacks are automated through the use of bots, rather than being human directed. Attack many computers and instruct them to attack others

Security ensures that users perform only tasks they are authorized to do, and can only have authorized information.