CSCE 201 Notes

Asset – Something of value.

Threat – Type of action with potential to cause harm.

Threat Agent – Person or element with power to carry out a threat.

Vulnerability – Flaw or weakness that allows a threat agent to bypass security.

Exploit – Taking advantage of a vulnerability.

Risk – The possibility of an exploit taking place.

Will Be Reassessed:
Gramm Leach GLBA
Database Security Breach Act 2003
HIPPA

Cyberterrorism – Premeditated, politically-motivated attacks against computer systems. It is intended to cause panic, provoke violence, or cause financial catastrophe.

Possible Targets: Traffic Lights, Banking, Air Traffic Control

Who attacks? Cybercriminals, Spies, Insiders, Cyberterrorists, Hacktivists, Gov. Agencies, Script Kiddies

Cybercriminals

Generic Def:
People who launch attacks against other users and their computers.

Specific Def:
A loose network of highly motivated attacks, many of which belong to organized gangs of attackers.

Targets:
Individuals and Businesses
Businesses and governments

Surface Web – Anything that can returned by a search engine

Deep Web – Any database that requires some sort of authentication to access its contents

Dark Web – Information that has been intentionally hidden and cannot be accessed through a standard browser

Skiddies are attackers who lack the knowledge necessary to perform an attack on their own. They often use automated attack software, often referred to as an "exploit kit" from other attackers.

Over **40%** of attacks require little or no skills.

Skill Chart:

Amount of skill needed to carry out an attack:

No skills (13%)
Low Skills (28%)
Moderate Skills (44%)
High Skills (15%)

Brokers

"Bug bounty" – When a vendor sponsors an event where they will handsomely reward an individual who can successfully hack/circumvent their software and reveal vulnerabilities

Spies

People hired to break into a computer and steal information.

They do not randomly attack unsecured computers. They are hired to attack a specific computer system.

Goals:

Break into a computer system.
Take information without drawing attention to their actions.

Skill level: Highly excellent.

Insiders

An organization’s own employees, contractors, or business partners.

Attacks are most often the sabotage or theft of intellectual property.

Most sabotage comes from employees who have recently been demoted, reprimanded, or left the company.

Cyberterrorists

Goals of a cyberattack:

Deface electronic information (spread misinformation and propaganda)
Deny service to legitimate computer users
Cause critical infrastructure outages and corrupt vital data

Attacks may be ideologically motivated

Hacktivists

Are motivated by ideology. They are typically attack specific websites to promote a political agenda, or to retaliate for a specific prior event.

Aaron Swartz
Swartz downloaded about 2.7 million federal court documents stored in the PACER (Public Access To Court Electronic Records) database managed by the Administrative Office of the United States Courts.

PACER was charging 8 cents per page for information that Carl Malamud, who founded the nonprofit group Public.Resource.org, contended should be free, because federal documents are not covered by copyright.

Government Agencies

May instigate attacks against own citizens or foreign governments.

Question on State Notification and Security Laws

Password Authentication

3 main types of authentication:

What you have
What you are
What you know

Example:
Key fob used to lock car
Facial characteristics
Uses memorized combination to open locker

The primary means of authentication on a computer system has two components

- Username
- Password

A password is a combination of letters, numbers, and special characters known only to the user.

Passwords are not considered a strong defense against attackers.

- Passwords can be weak.
- Passwords are subject to different types of attacks.

Password weaknesses

- Human beings can only memorize a limited number of items.
- Long, complex passwords are difficult to memorize.
- Users must remember multiple passwords for multiple accounts.
- Users may take shortcuts that compromise security.