Dr. Ammar Haider
Assistant Professor
School of Computing

CS3002 Information Security

Introduction to Information Security

Content source: Whitman & Mattord, chapters 1-2, Stallings Chap 1

Course Outline

- Please refer to course outline for details of CLOs, evaluations and topic schedule

What Is Security?

- "A state of being secure and free from danger or harm; the actions taken to make someone or something secure."

Information Security

- The protection of information and its critical elements, including systems and hardware that use, store, and transmit that information
- Includes information security management, data security, and network security

Components of an Information System

Information system (IS) is the entire set of people, procedures, and technology that enable business to use information.

- Software
  - most difficult to secure
  - easy target
- Hardware
  - require physical security policies

Components of an Information System

- Data
  - Often most valuable asset
  - Main target of intentional attacks
- People
  - Weakest link
  - Target of social engineering
  - Must be well trained and informed

Components of an Information System

- Procedures
  - Written instructions for business tasks
  - Provide details on how system works
- Networks
  - Securing the data in transit
  - Block outsiders from access (firewalls)

Causes of Insufficient Security

- Networks are insecure: (most) communications are made in clear
- LANs operate in broadcast
- Geographical connections are not made through end-to-end dedicated lines but:
  - through shared lines
  - through third-party routers
  - weak user authentication (normally password-based)
- Software is not sufficiently tested, bugs and weaknesses remain

Causes of Insufficient Security

Weakest link in the chain: **Human beings**

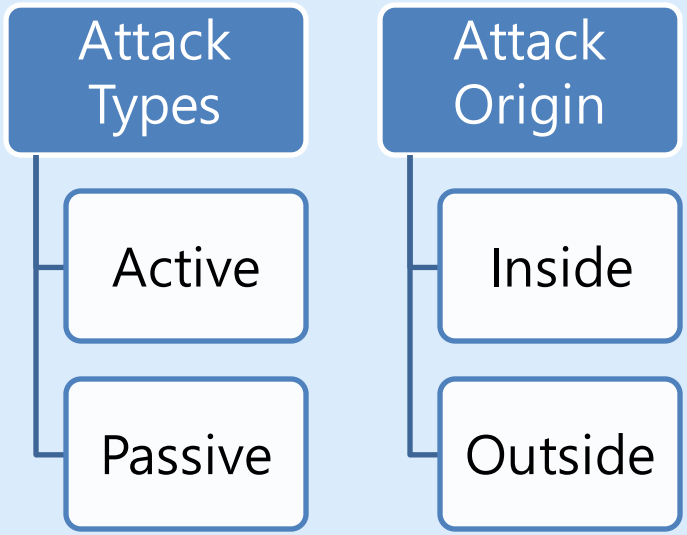
- Low problem understanding (awareness)
- Making mistakes when overloaded, stressed etc.
- Natural tendency to trust
- Complex interfaces/architectures can annoy or mislead the user and originate erroneous behaviors
- Naive users are an easy target (e.g. “do change immediately your password with the following one, because your PC is under attack”) …
- …but experienced users are targeted too

Causes of Insufficient Security

- "Defensive strategies are reactionary"
- "Thousands - perhaps millions - of system with weak security are connected to the Internet"
- "Increasingly complex software is being written by programmers who have no training in writing secure code"
- "Attacks and attack tools transcend geography and national boundaries"
- "The difficulty of criminal investigation of cybercrime coupled with the complexity of international law means that prosecution of computer crime is unlikely"

Threats to information security

- **Vulnerability**: weakness in an asset
- **Threat**: A potential security harm to an asset, caused by exploiting the vulnerability
- **Attack**: An act exploiting a vulnerability. Threat being realized.



Examples of Attacks/Threats

- Hacking
  - Deeply examine the target system
  - Bypass security controls using skills and/or fraud
  - After a successful attack, next step is **privilege escalation**
    - The higher the privilege, the more the possible harm

Examples of Attacks/Threats

- Expert hacker
  - Develop software scripts and program exploits
  - Will often create attack software and share with others
- Novice hacker
  - Use expertly written software to exploit a system
  - Do not usually fully understand the systems they hack

Examples of Attacks/Threats

- Password attacks
  - Cracking: guess or reverse-calculate a password
- Cracking techniques
  - Brute force: Application of computing and network resources to try every possible combination of characters of a password
  - Dictionary: Uses a list of commonly used passwords (the dictionary) as guesses

Examples of Attacks/Threats

- Brute forcing time estimate

Case-Sensitive Passwords Using a Standard Alphabet Set (with Numbers and 20 Special Characters)		
Password Length	**Odds of Cracking: 1 in (Based on Number of Characters ^ Password Length):**	**Estimated Time to Crack***
8	2,044,140,858,654,980	2.7 hours
9	167,619,550,409,708,000	9.4 days
10	13,744,803,133,596,100,000	2.1 years
11	1,127,073,856,954,880,000,000	172.5 years
12	92,420,056,270,299,900,000,000	14,141.9 years
13	7,578,444,614,164,590,000,000,000	1,159,633.8 years
14	621,432,458,361,496,000,000,000,000	95,089,967.6 years
15	50,957,461,585,642,700,000,000,000,000	7,797,377,343.5 years
16	4,178,511,850,022,700,000,000,000,000,000	639,384,942,170.1 years

Examples of Attacks/Threats

- Human error or failure
  - Carelessness of employees
  - Shoulder surfing
  - Social engineering
    - using social skills to convince people to reveal confidential information
    - Psychological pressure
    - Showing acquaintance with company's procedures and habits
    - Phishing: Sending spoofed but genuine-looking messages to targets

Examples of Attacks/Threats

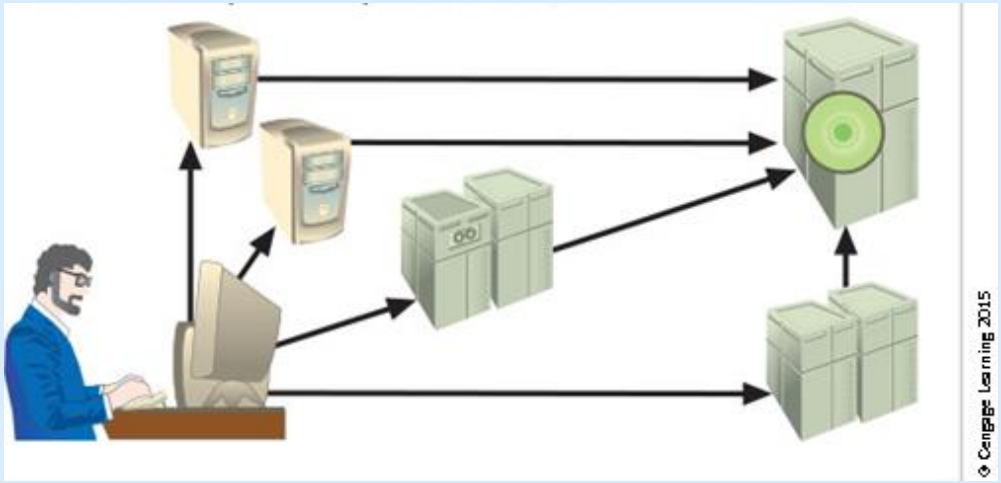
- Money extortion by blackmail
  - after data theft
  - after data hostage: ransomware
- Vandalism
  - e.g. defacing public websites
  - Destroy image of the business

Examples of Attacks/Threats

- Malware: malicious software
- Virus
  - Spreads quickly
  - Attached to a host file (exe, document)
- Worms
  - Do not require a host file
  - Can self-replicate and self-propagate over local network
- Trojans
  - Disguised as an essential or useful software

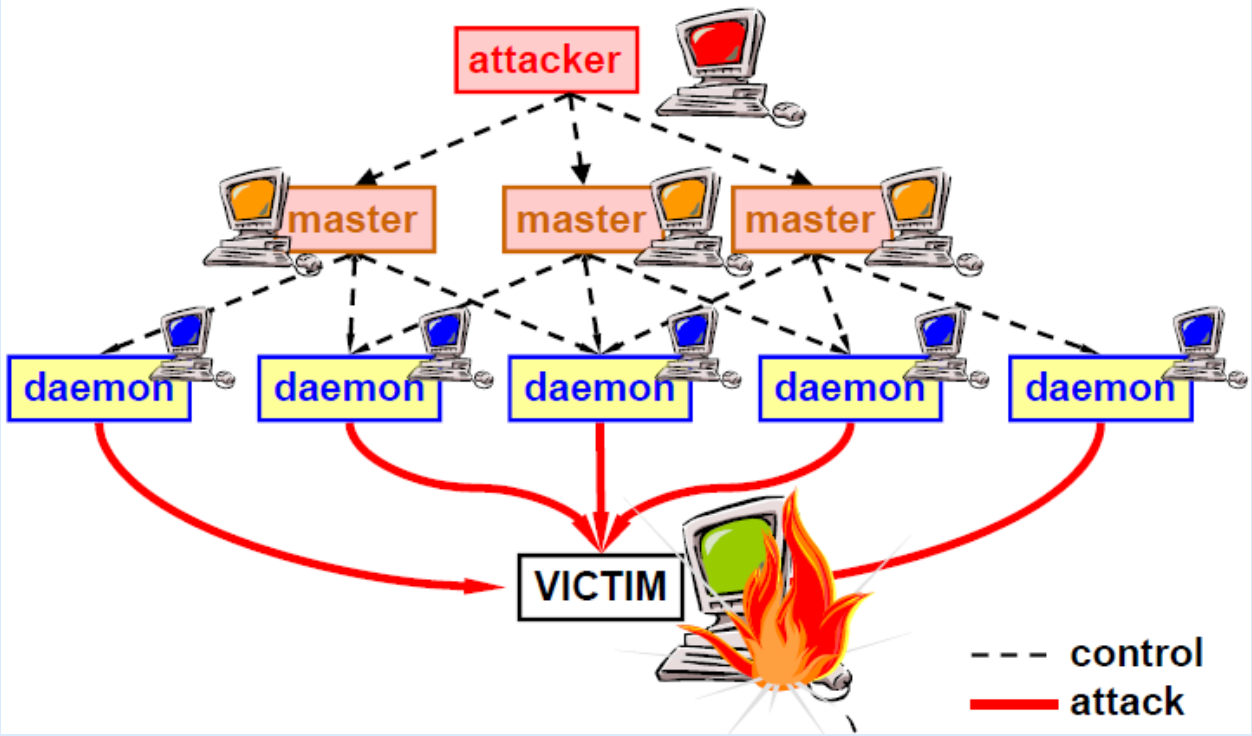
Examples of Attacks/Threats

- Bots: Used to launch Distributed Denial-of-Service (DDoS) attacks
  - Hundreds or thousands of devices are compromised (zombies) and remotely activated by attacker



Examples of Attacks/Threats

- Another visualization of DDoS attacks



Examples of Attacks/Threats

- Packet Sniffing
  - Monitor data traveling over the network
- IP Spoofing
  - Modify the sender address in IP header
- Man-in-the-middle (MITM) attacks
  - Hijacking the session to delete or forge the data in transit

Examples of Attacks/Threats

- Copyright Infringement
  - Piracy
- Internet Service Issues
  - Outage (downtime) or degradation
- Power blackouts and faults

Examples of Attacks/Threats

- Cyberterrorism
  - Attacks affecting widespread users
- Cyberwarfare
  - State-sponsored attacks against rival states

Examples of Attacks/Threats

- Forces of nature
  - Natural disasters
  - Require planning in advance:
    - disaster recovery plan
    - business continuity plan
    - incident response plan

Characteristics of Information

Any piece of information will have one or more of the following characteristics. Goal of information security is to maintain these characteristics.

Confidentiality

- Disclosure or exposure to unauthorized individuals or system is prevented

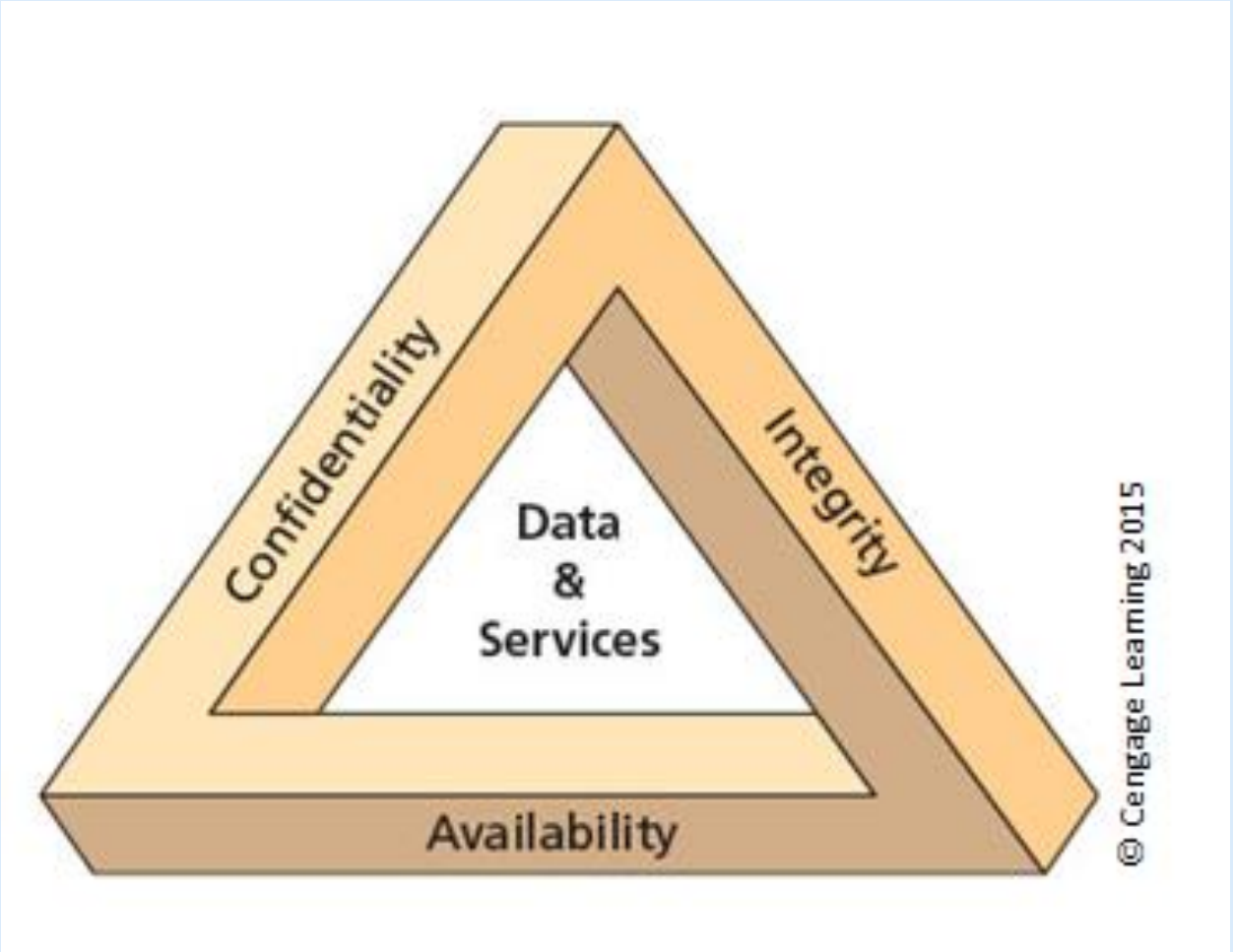
Integrity

- Information as a whole is complete, uncorrupted

Availability

- No interference or obstruction when information is needed

The C.I.A. triad



Characteristics of Information

Some more sub-characteristics worth mentioning

Accuracy

- Factual, free from errors

Authenticity

- Quality or state of being genuine, e.g., sender of an email

Utility

- Timeliness - No value if it is too late

Characteristics of Information

Some more characteristics worth mentioning

Possession

- Ownership of information

Accountability

- Actions of a user are uniquely traceable
- Helps in after-attack recovery and finding the culprit

Privacy

- Keeping individual's Personally Identifiable Information (PII) secret

Components of information security

Attacks and Consequences

Consequence	Attack
Unauthorized Disclosure	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or by-products of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.

Stallings, Table 1.2

Memorizing these terms is not required

Attacks and Consequences

Consequence	Attack
Deception An authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.

Stallings, Table 1.2

Memorizing these terms is not required

Attacks and Consequences

Consequence	Attack
Disruption.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation An unauthorized entity taking control of system services or functions	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

Stallings, Table 1.2

Memorizing these terms is not required

Attack Vectors and Surfaces

- Attack surfaces are different points that an unauthorized user can employ to compromise a system or network.
- Each attack surface has its associated risk, likelihood and impact.
- Source of input maybe hardware, software, or communication.
- Its is important to map out all entry points an attacker can abuse in a system.
  - Involves creating an architecture diagram.
  - Tests performed based on priority
  - Priority = ease of exploitation * impact of exploitation

Attack Surface Mapping

List all components

Prepare architecture diagram

Label components & communication b/w them

Identify attack vectors

Rate attack vectors

Threat Modeling: STRIDE

- Theoretical use cases considered to identify potential threats.
- Microsoft STRIDE
  - S: Spoofing of identity
  - T: Tampering with data
  - R: Repudiation
  - I: Information disclosure
  - D: Denial of service
  - E: Elevation of privilege.
- Requires realization of assets and vulnerabilities