Definitions and Terminology

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

CIA Triad

Confidentiality:

- Ensure the protection of the secrecy of data, objects, or resources.

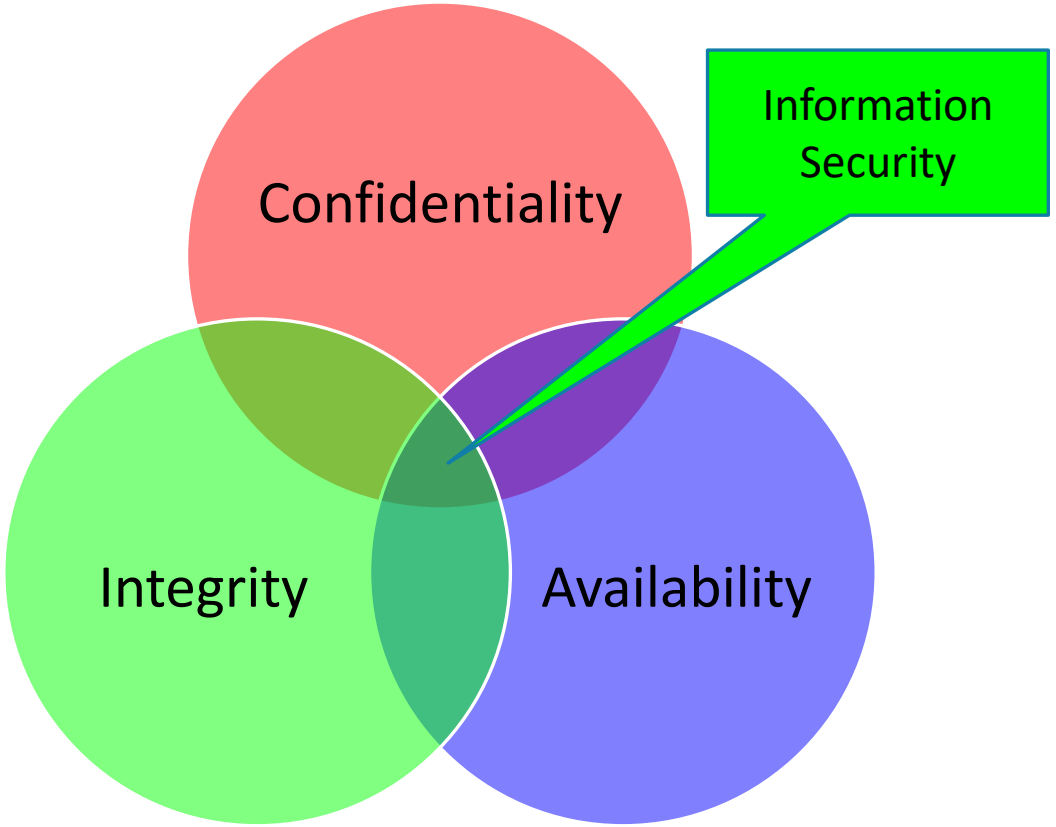
Integrity:

- Protect the reliability and correctness of data

Availability:

- Authorized subjects are granted timely and uninterrupted access to objects

These are considered the core requirements of computer security



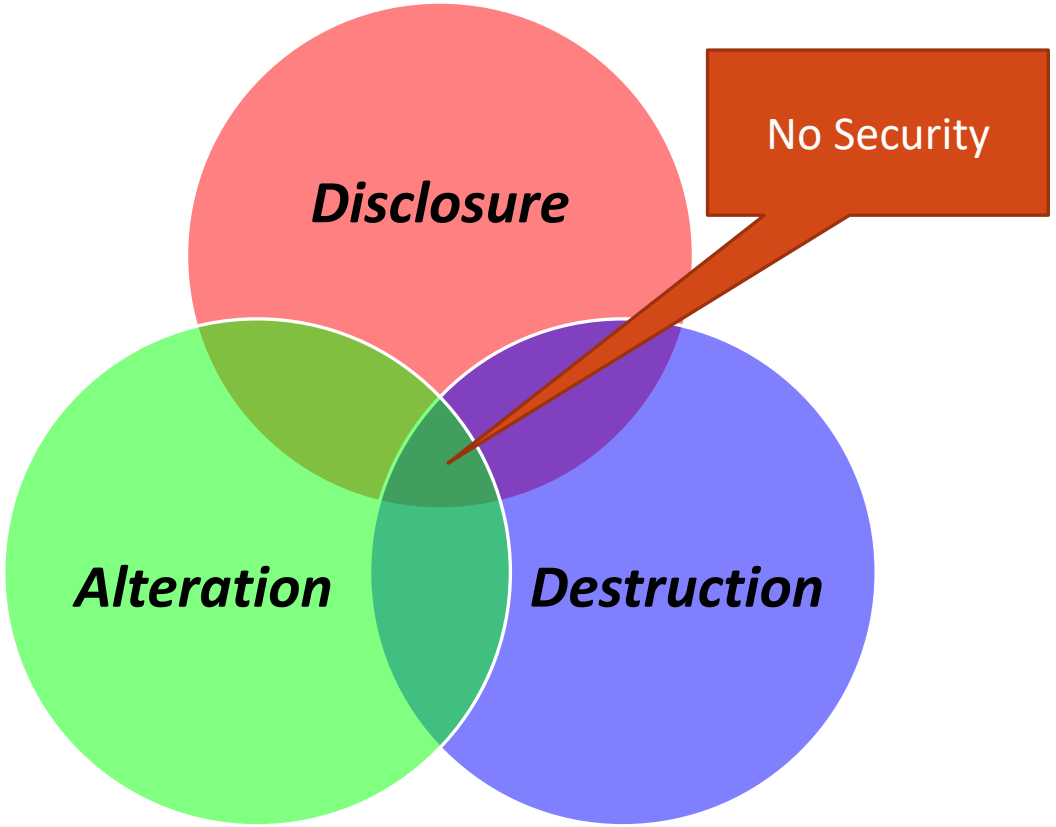
DAD Triad

The “Evil Twin” to the CIA Triad

Disclosure
- Material is accessed by unauthorized entities

Alteration
- Data is changed - either maliciously or accidentally

Destruction
- Resource is damaged, or made unavailable to users



Non-repudiation

A subject can not deny that they performed an action, or caused an event to take place

- Sending an email
- Signing a document
- Ordering products

There are many ways to establish nonrepudiation

- Digital certificates
- Session identifiers
- Transaction logs
- Many, many others

Nonrepudiation is critical to the concept of accountability. (i.e. – An entity can be held responsible for an action.)

Further reading: https://en.wikipedia.org/wiki/Information_security#Key_concepts

AAA Services

This refers to authentication, authorization, and accounting (or auditing)

However, there are actually five components:

- Identification
- Authentication
- Authorization
- Auditing
- Accounting

You can look up the definitions for each of these at the National Institute of Standards and Technology (NIST) Glossary

- https://csrc.nist.gov/glossary/

Other Terms

Defense in Depth (“layering”)
- Security controls/protections are placed in series so an attack must pass multiple protections to reach the objective

Threat
- Any potential event that could cause an undesirable outcome
- These can also include natural disasters such as a hurricane or earthquake

Vulnerability
- Flaw or weakness in a system that allows a threat to cause harm

Risk
- The possibility or likelihood (probability) that a threat will exploit a vulnerability and perform a malicious activity
- Still applies to natural disasters – a flood could submerge a server room

Risk Management
- The process of identifying, evaluating and prioritizing risk – followed by efforts to minimize those risks

Other Terms

Attack Vector (or Access Vector)

- The path or step an attacker takes to conduct their malicious activity
- May require multiple steps. Ex:
  - Gain remote access to computer system
  - Escalate privileges to root
  - Install malicious payload

Zero Day

- A vulnerability that was previously unknown (or unknown to the general public)
- In normal usage, it also means that an exploit exists for this vulnerability
- Usually allows attackers several days (or longer) to exploit freely

Dumpster Diving

- Searching through garbage receptacles for valuable information
- Source code, usernames, product manuals, configuration information, etc.

Malicious Software (Malware)

Trojan Horse

- A program that appears to do one thing (and may indeed do it) but that hides something else (such as deleting all of your data).

Virus

- A program that reproduces by attaching copies of itself to other programs, often carries a malicious "payload“

Worm

- Does not need to attach itself to another program to reproduce, attempts to gain access to other systems on a network and then copies itself to these new systems

Time (logic) bomb

- A program that is set to execute it's (often malicious) payload upon a certain condition being met. A time bomb is based on the payload being executed on a specific day or time (such as a Friday the 13th at midnight). A logic bomb will execute its payload upon a certain condition being met (such as not finding my name listed in the employee directory anymore -- IOW I got fired).

Malicious Software (Malware)

Bot

- Software that automatically performs certain actions, often grouped together in large "botnets" that are used for nefarious purposes
- This software will sit on your computer, waiting for an order from its controller to execute some action (such as sending out a large amount of SPAM or launching a Distributed Denial of Service (DDoS) attack against some computer or network)

Spyware

- Software designed to "spy" on the user's activities, may include active monitoring
- A keystroke logger would be an example where it records all keystrokes the user makes and then transfers this information to the owner of the spyware

Ransomware

- Software that holds a computer "hostage" while demanding a ransom
- Often this is done by encrypting all of the data on the computer and then telling the user they need to provide a certain amount of money (via something like Bitcoins) in order to get the key and decrypt their own data

Adware

- Software that automatically displays or downloads often unwanted advertisements.
- This type of software can be either malicious or simply annoying. A lot of game apps we download for free today force us to watch an ad in order to be able to play the game. While sometimes annoying, this would not be considered malicious.
- If the program is installed on my computer without my permission or knowledge, and then it forces me to watch ads at certain time, it would be considered malicious.

The Jargon File

Look up the following terms in *The Jargon File Glossary*

- *http://www.catb.org/jargon/html/go01.html*
- *Hacker*
- *Cracker*
- *Phreaking*
- *Hacker Ethic*

(You will be responsible for knowing these terms)