Network Security

C.I.A

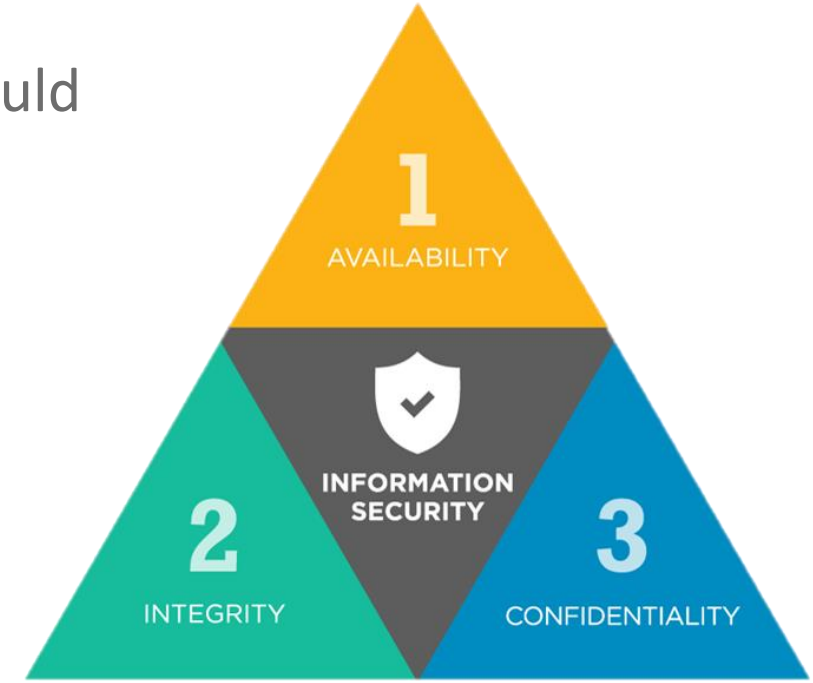
https://hermanka.github.io

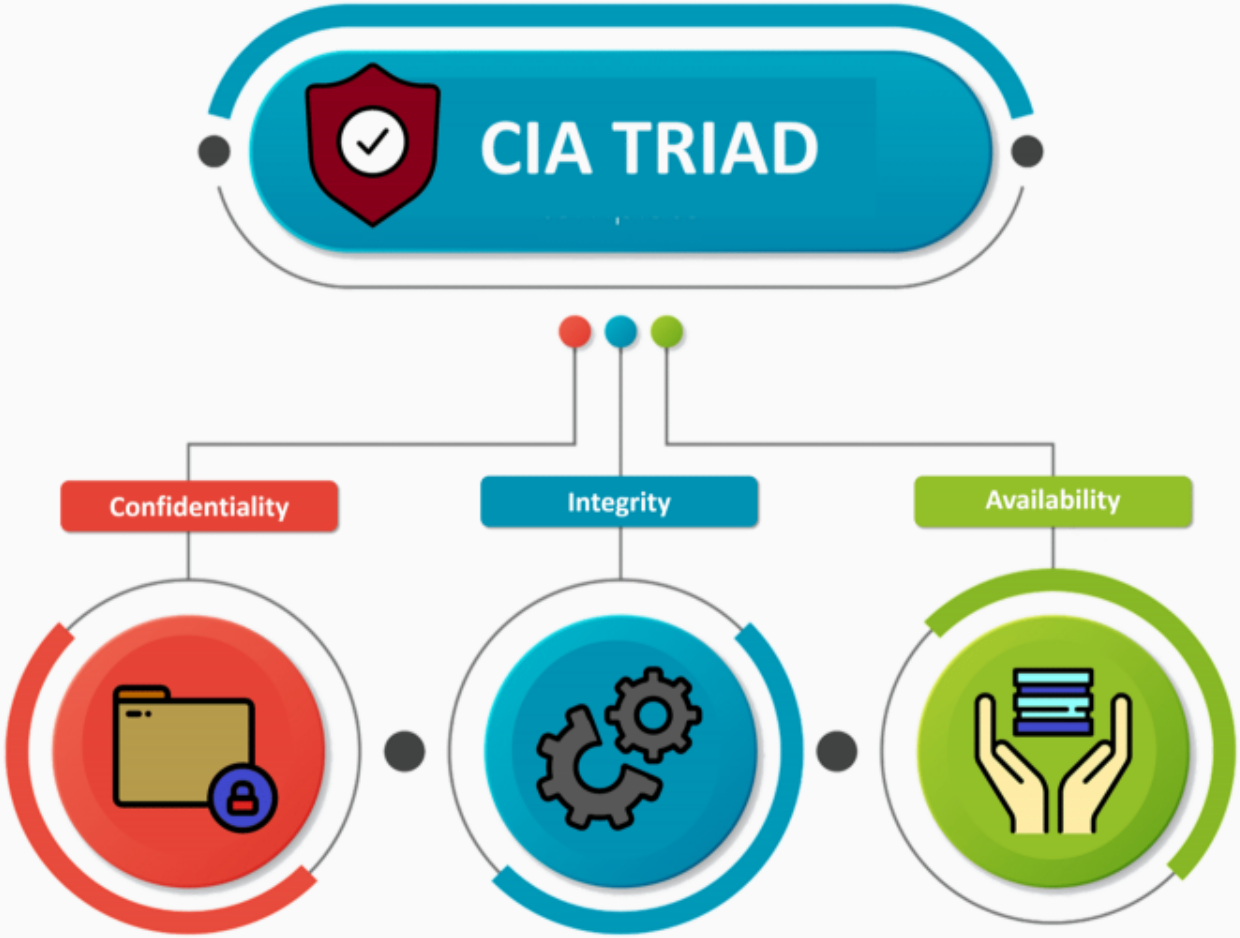
Computer Security Basics

- CIA Triad
  - Goals for implementing security practices
  - Confidentiality, Integrity, and Availability
- DAD Triad
  - Goals for defeating the security of an organization
  - Disclosure, Alteration, and Denial

CIA Triad

- Confidentiality
  - Confidential information should not be accessible to unauthorized users
- Integrity
  - Data may only be modified through an authorized mechanism
- Availability
  - Authorized users should be able to access data for legitimate purposes as necessary



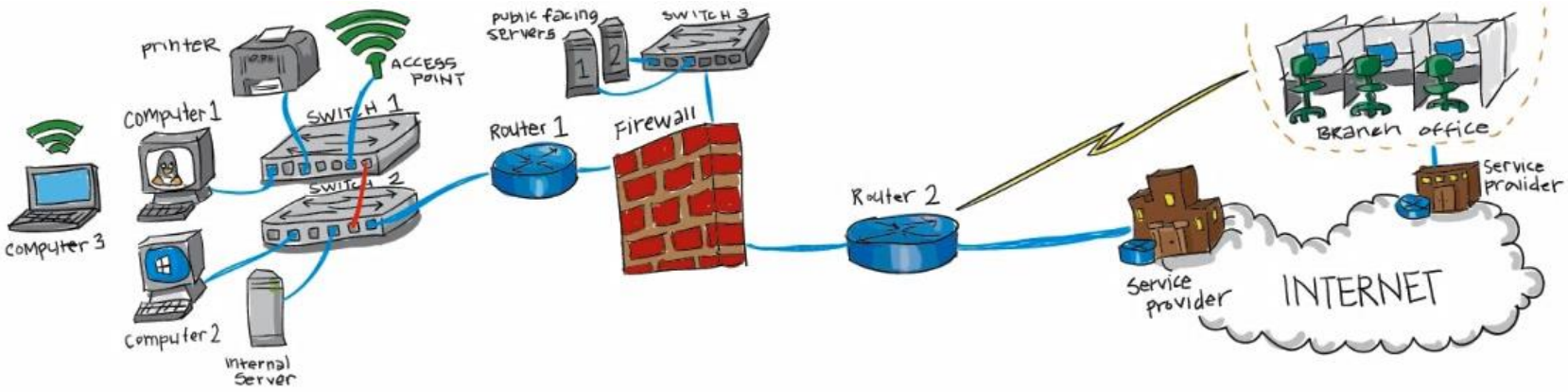


IDwebhost

Confidentiality

- How secure is the information?
- How secure does the data need to be?
- Confidential information should not be accessible to unauthorized users

- Best methods
  - Physical Protections
    Locked doors, security guards, security cameras, etc.
  - Electronic Protections
    Encryption, firewalls, 2FA, etc.



Integrity

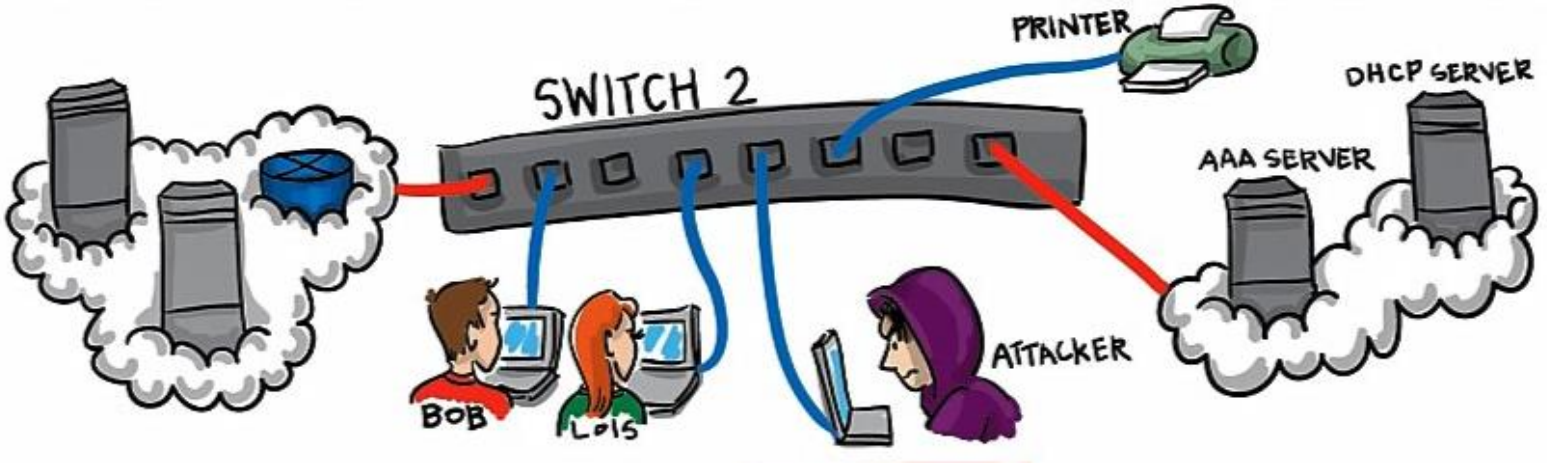
- How correct is the information?
- Has the data been modified during retrieval, in transit or in storage?
- Data may only be modified through an authorized mechanism
- Best methods
  - Hashing of files & informations
  - Checksums during data transmissions

=

```
79054025
255fb1a2
6e4bc422
aef54eb4
```

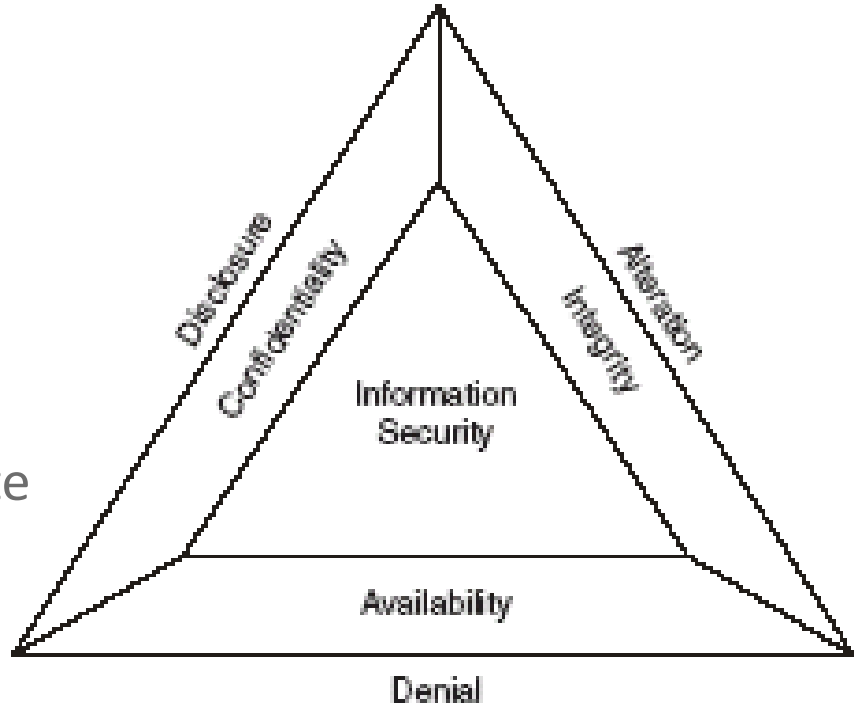
Availability

- How much uptime is the system providing?
- Is the data accessible by users at all times?
- Authorized users should be able to access data for legitimate purposes as necessary.
- Best methods
  - Redundancy in system design (components and data)
  - Backup strategies and disaster recovery plan



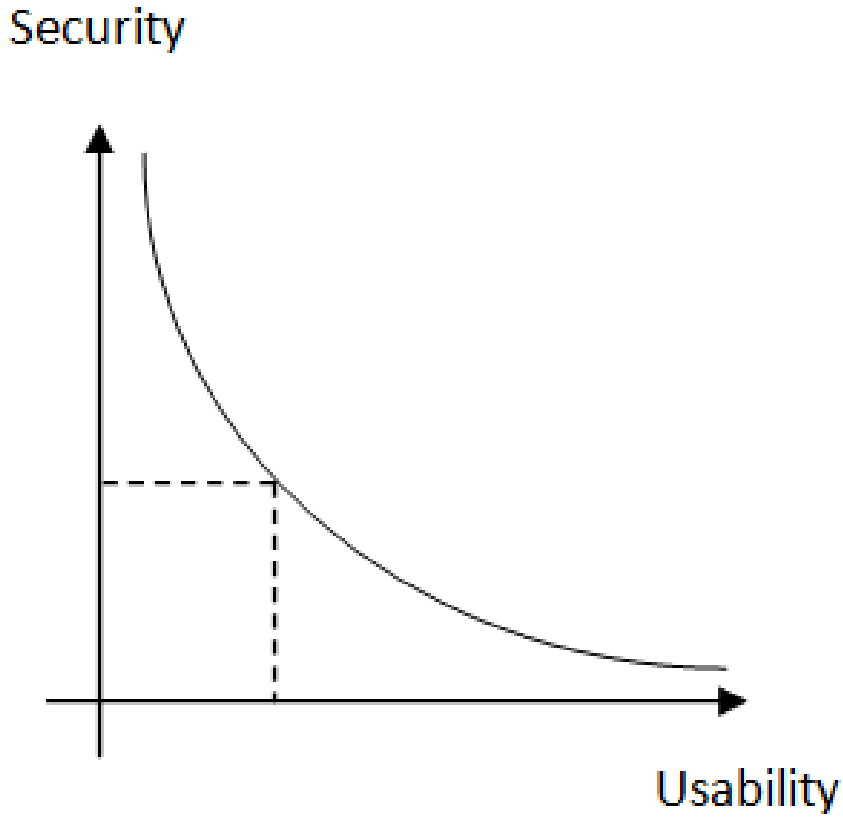
DAD Triad

- Disclosure
  - Unauthorized individuals gain access to confidential information
- Alteration
  - Data is modified through some unauthorized mechanism
- Denial
  - Authorized users cannot gain access to a system for legitimate purposes
- DAD activities may be malicious or accidental



Security vs Usability

- A tradeoff occurs between the usability of a system and the security of the system.
- As security increases, often usability decreases.

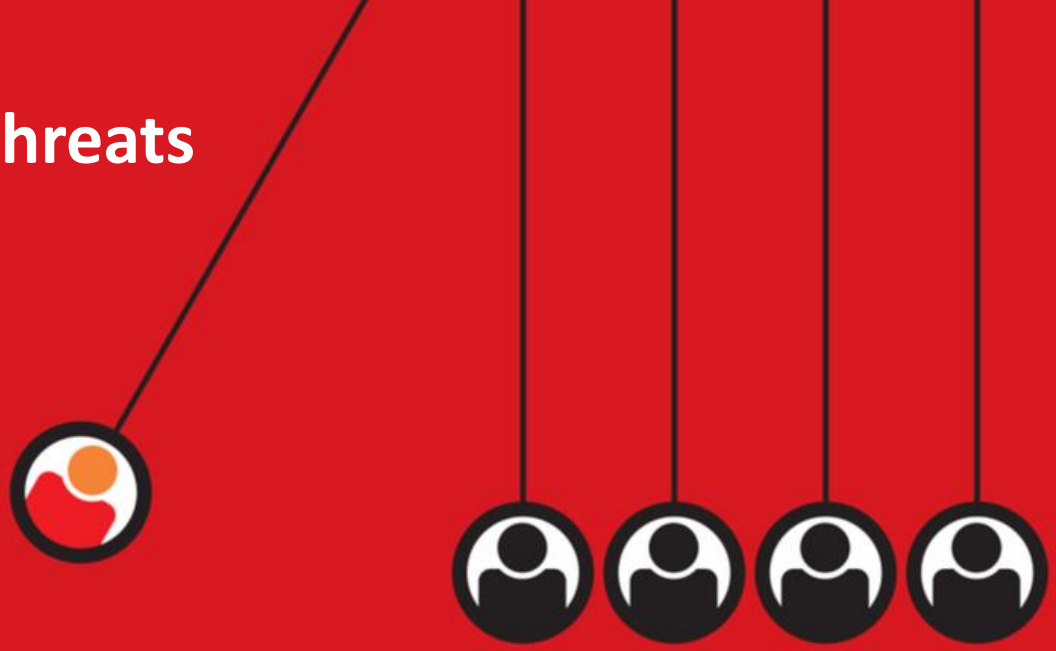


Risk Considerations

Component of Risk: Assets

- Any Item that has a value to the organization
- Examples
  - Information or Data
  - Network Equipment
  - Servers/Computers
  - Software
  - Personnel
  - Processes

Component of Risk: Threats



- Any condition that can cause harm, loss, damage or compromise of an asset
- Examples
  - Natural disasters
  - Cyber attacks
  - Breach of integrity of data
  - Disclosure of confidential data
  - Malware

Component of Risk: Vulnerabilities

- Any weakness in the system design, implementation,software code, or lack of preventive mechanisms.
- Examples
  - Software bugs
  - Misconfigured software
  - Misconfigured network devices
  - Improper physical security

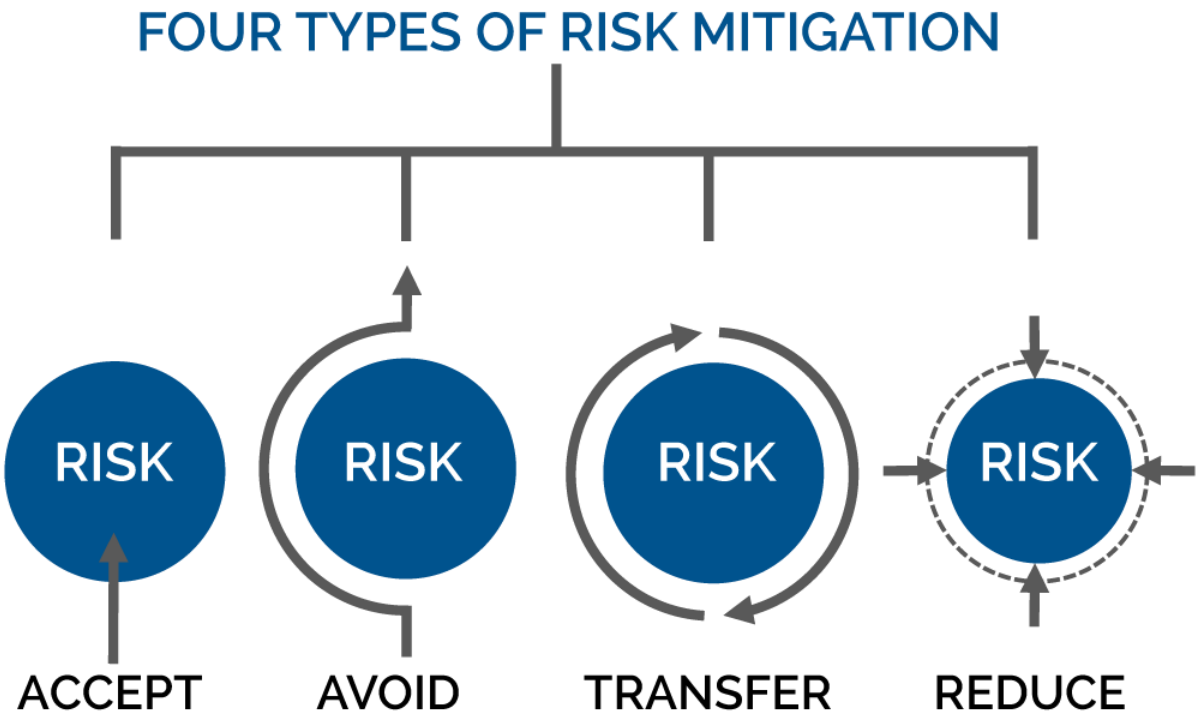
Component of Risk: Risk

- Probability (or likelihood) of the realization of a threat
- Vulnerability without a threat equates to no risk…

RISK = VULNERABILITY + THREAT

Risk Mitigation

- Main goal of security is to minimize risk to a level acceptable to the organization
- Our goal is not necessarily to eliminate all risks



Risk Acceptance

- Organization accepts the risk associated with a system's vulnerabilities and their associated risks
- Risk acceptance is common when the risk is low enough to not apply countermeasures, or adequate countermeasures have already been applied

Risk Avoidance

- Risk is too high toaccept, so the system configuration or design is changed to avoid the risk associated with a specific vulnerability
- Example
  - Utilizing Windows XP is too dangerous in 2020, therefore we would install Windows 10 instead to avoid risks.

Risk Transference

- Transfer the risk to a third-party, for example an insurer
- Example
  - Cost associated with replacing all the servers in a server farm due to a fire is too risky to accept, therefore we purchase fireinsurance for the servers