CIA TRIAD

Confidentiality, Integrity & Availability
The CIA Triad

The CIA Triad—Confidentiality, Integrity, and Availability—is a guiding model in information security. A comprehensive information security strategy includes policies and security controls that minimize threats to these three crucial components.

The CIA triad guides the information security in a broad sense and is also useful for managing the products and data of research.

Confidentiality is limiting data access, integrity is ensuring the data is accurate, and availability is making sure it is accessible to those who need it.

Confidentiality refers to protecting information from unauthorized access. Maintaining confidentiality helps achieve multiple important goals, including ensuring privacy and avoiding ransomware attacks.

Confidentiality is important to protect sensitive information from being disclosed to unauthorized parties. This includes protecting data at rest, in transit, and in use. Common techniques used to maintain confidentiality include encryption, access controls, and data masking.

Confidentiality is a critical aspect of security, especially when sensitive or private information is involved. Healthcare Records can be a prime example in this regard.

Protecting patients' medical records is paramount. Hospitals and healthcare providers use data confidentiality measures to ensure that patient information, including diagnoses, treatment plans, and personal identifiers, remains secure and accessible only to authorized personnel.

Integrity means data are trustworthy, complete, & have not been accidentally altered or modified by an unauthorized user. The integrity of data may be compromised unintentionally by a system malfunction, errors in entering data, or forgetting to maintain an up-to-date backup. Integrity can also be compromised by malicious actors attempting to tamper with data.

Integrity is important to ensure that information has not been tampered with or modified in an unauthorized way. This includes protecting data from unauthorized modification, deletion or addition. Common techniques used to maintain integrity include digital signatures, message authentication codes, & data hashing.

A breach of integrity occurs when there’s a change in data.

Data corruption might occur when a software bug or hardware malfunction causes wrong transmission and storage of data, resulting in errors or inconsistencies.

When an attacker injects malicious software, such as a virus into the system, the virus might change data without the user's knowledge or consent, potentially causing damage or disruption.

Tampering refers to an unauthorized user physically accessing a computer or storage device and changing the data on it, either by deleting or altering the data or by adding false or misleading information.

Availability means data can be accessible when needed. Availability of data is crucial to daily operations of institutions. Without access to data, everything grinds to a halt, which is why medical and educational institutions are often targeted for ransomware attacks.

Availability is important to ensure that information and systems are accessible to authorized users when they need them. This includes protecting against denial of service attacks and ensuring that systems are highly available and can withstand failures. Common techniques used to maintain availability include load balancing, redundancy, and disaster recovery planning.

Some common causes of availability breaches include hardware or software failures, network outages, power outages, natural disasters and cyberattacks.

A hardware failure might cause a server to crash, preventing users from accessing its data or services. Network outages might prevent users from accessing data or systems over the internet. Power outages might prevent users from accessing data or systems that rely on electrical power. A natural disaster, such as a flood or earthquake, might cause physical damage to data centers or other critical infrastructure, disrupting access to data and systems. A cyberattack, such as a denial-of-service attack, might overwhelm a system with traffic, preventing legitimate users from accessing it.

Authenticity, and Non-repudiation

Along with Confidentiality, Integrity and Availability, Authenticity, and Non-repudiation are security properties that are used to ensure the security and reliability of information systems.

Authenticity is important to ensure that information and communication come from a trusted source. This includes protecting against impersonation, spoofing and other types of identity fraud. Common techniques used to establish authenticity include authentication, digital certificates, and biometric identification.

Non-repudiation is important to ensure that a party cannot deny having sent or received a message or transaction. This includes protecting against message tampering and replay attacks. Common techniques used to establish non-repudiation include digital signatures, message authentication codes and timestamps.

Authentication is used to verify identity. Identity is the claim that an individual is a specific person. Authentication is an attempt to verify a claim about identity.

If an e-mail comes from a bank and one can authenticate the e-mail, one can place a certain amount of trust in the contents.

If an e-mail comes from an adversary, but claims to come from the bank, and one is unable to authenticate the e-mail, one may distrust the contents of the e-mail.

Non-repudiation provides an assurance that the sender of data is provided with proof of delivery and the recipient is provided with proof of the sender's identity, so neither can later deny having processed the data.

Non-repudiation can achieved through cryptography, like digital signatures.

In online transactions, digital signatures ensure that a party cannot later deny sending information or deny the authenticity of its signature. A digital signature is created using the private key of an asymmetric key pair, which is public key cryptography, and verified with a corresponding public key.

Only the private key holder can access this key and create this signature, proving that a document was electronically signed by that holder. This ensures that a person cannot later deny that they furnished the signature, providing nonrepudiation.

Confidentiality, Integrity, Availability, Authenticity, and Non-repudiation (CIAAN) form the foundation of information security and are the key elements that must be protected in order to ensure the safe and secure handling of sensitive information.

THANK YOU