LESSON NOTES

CYBERSECURITY

Domain 1.0 - General Security Concepts

1.2.1 - CIA Triad and AAA

Lesson Overview:

Students will:

- Be able to summarize authentication and authorization design concepts.

Guiding Question: How do the principles of the CIA Triad interact with authentication, authorization, and accounting framework to ensure the overall security of information systems?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

1.2 - Summarize fundamental security concepts

- Confidentiality, Integrity, and Availability (CIA)
- Non-repudiation
- Authentication, Authorization, and Accounting (AAA)
  - Authenticating people
  - Authenticating systems
  - Authenticating models

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

CIA Triad and AAA

CIA Triad

Confidentiality, Integrity, and Availability, also called the CIA Triad is the three fundamental principles of information security. This serves as a guiding framework for organizations to implement effective security measures and protect valuable data.

Confidentiality

This ensures authorized users are the only ones who can access confidential information. It prevents unauthorized access, disclosure, or theft of data. Examples include access control lists, encryption, and data masking.

Integrity

This guarantees that information remains accurate and complete, and hasn't been tampered with or modified in any unauthorized way. It protects data from accidental or malicious alterations, deletions, or forgery. Data integrity controls include checksums, digital signatures, and versioning systems.

Availability

This ensures that authorized users have timely and reliable access to information and systems when needed. It protects against disruptions, outages, or denial-of-service attacks that prevent legitimate users from accessing required data and resources. Redundancy, disaster recovery plans, and performance monitoring are key for maintaining availability.

Why is it important?

The CIA Triad is widely adopted because it provides a simple and understandable framework for developing and implementing security controls. By focusing on these three core principles, organizations can effectively balance various security risks and prioritize their resources accordingly. Additionally, the CIA Triad is flexible and can be applied to different types of information systems and organizations, regardless of size or industry.

Digital Forensics

Unfortunately, what we see on television shows like CSI drastically exaggerates the realism of gathering and examining forensic data. Forensics is the application of scientific knowledge to legal issues. Digital forensics uses scientific principles to provide assurance in explaining what has or has not happened on a computer system.

There must be ***non-repudiation*** with the evidence, or no doubt that it was not tampered with. This can also be done with hashing or running back ups/data through a one way algorithm to get a checksum. These checksums are the results from the hashes, and they can be compared against one another to

make sure the evidence has not been tampered with. The earliest known state of the data, or when it was collected, is known as the provenance. It is important to have this state to know if something has been tampered with. Preserving, or keeping of the data, is important. The original data must still exist as it might be used as evidence.

AAA

The AAA framework is a way to understand security issues surrounding the accessibility of individuals within an organization. When logging into a network to gain access to resources, the user provides identification with a username and password. This process of identification passes through the ***authentication***, ***authorization***, and ***accounting*** (AAA) framework.

Authenticating People

Authenticating people involves verifying their identity to make sure they are who they claim to be. This is crucial for protecting sensitive information, preventing unauthorized access, and maintaining security in various contexts. There are many ways to accomplish this. Some examples include:

- Knowledge based methods – passwords, PINs, or security questions
- Possession based methods – key cards, USB tokens, smart cards
- Biometric methods – fingerprint scanners, facial recognition, or voice recognition
- Multi-factor authentication – this is a combination of two or more of the above

Authenticating Systems

Authenticating systems involves verifying the identity of a device, computer, or application to ensure it is authorized to access resources or communicate with other systems. This is crucial for protecting networks, data, and resources from unauthorized access, malicious activity, and potential breaches. The key methods for this similar to authenticating people but are slightly different.

- Credentials-Based Authentication – username and password, API keys or digital certificates
- Token-based Authentication – hardware tokens or software tokens
- Biometric Authentication – device fingerprinting or behavioral biometrics
- Mutual Authentication – Client and Server authentication
- Zero Trust Architecture – Assumes no system is trustworthy

Authorization Models

Authorization models define the rules and policies that govern who can access what resources or perform what actions within a system. They are essential for enforcing security, ensuring compliance and protecting sensitive data. There are some things to consider when choosing an authorization model. The complexity of your system and access requirements, the sensitivity of your data, any compliance requirements you have, the ease of management required, and how flexible you need access to be. There are five models:

- **(ACLs) Access Control Lists** – These assign access permission directly to specific users or groups for each resource. They are simple and straight forward, but with large systems they can become very complex.

- **(RBAC) Role-Based Access Control** – These assign permissions to roles like "admin", "guest", "editor", rather than individual users. Users are then assigned roles based on their responsibilities. This simplifies the management and enhances security.

- **(ABAC) Attribute-Based Access Control** – These grant permissions based on attributes, for example a user's department, location, device type, time of day and so on. They are very granular and flexible, allowing for finely detailed access control. This is well suited for a complex environment with dynamic access needs.

- **(RuBAC) Rule-Based Access Control** – This allows rules to define access conditions, often expressed as if-then statements. It can be combined with other models for greater flexibility. It also allows for customization and adaptation to specific security requirements.

- **(MAC) Mandatory Access Control** – not to be confused with "Media Access Control Address", this enforces access restrictions based on security labels assigned to users and resources. It is centrally controlled by the system and often used in high-security environments. MAC offers a high degree of protection but can be less flexible for user-specific needs.