
DATA SECURITY

Objectives: By the end of this lesson, students should be able to:

- Evaluate different security settings for data and application security.
- Understand the theoretical basics of data and application security.
- Describe data encryption methods.
- Explain system mechanisms used to protect data.
- Implement and configure security applications like AppLocker and executable rules.

DATA SECURITY

Refers to the protective measures and strategies that ensure the confidentiality, integrity, and availability of data. Its primary goal is to safeguard sensitive information from unauthorized access, breaches, theft, or corruption.

APPLICATION SECURITY

Application security refers to the process of developing, implementing, and testing security features within software applications to protect them from vulnerabilities, threats, and attacks. Its goal is to ensure that an application is protected from malicious activities, unauthorized access, data breaches, and other risks throughout its lifecycle, from development to deployment and maintenance.

IMPORTANCE OF DATA SECURITY IN PROTECTING SENSITIVE INFORMATION

- Protection of Personal Information
- Trust and Confidence
- Legal and Regulatory Compliance
- Ethical Data Practices
- Data-driven Innovation
- Preserving Individual Autonomy

COMMON SECURITY THREATS AND VULNERABILITIES

1. MALWARE
2. PHISHING ATTACKS
3. RANSOMWARE
4. INSIDER THREATS
5. WEAK PASSWORDS
6. UNPATCHED SOFTWARE
7. DOS ATTACKS
8. MAN IN THE MIDDLE ATTACKS

WHY THE CIA TRIAD MATTERS

The CIA Triad matters because it provides a framework for understanding and addressing security risks. By focusing on confidentiality, integrity, and availability, organizations can better protect their data from theft, loss, and damage. This not only safeguards sensitive information but also helps maintain trust with customers and stakeholders.

Principles of Confidentiality, Integrity, and Availability (CIA Triad)

CONFIDENTIALITY

- Confidentiality ensures that sensitive information is only accessible to authorized individuals. It protects data from unauthorized access, ensuring that it remains private. Involves restricting data access strictly to authorized personnel.

INTEGRITY

- Integrity ensures that data is accurate, consistent, and unaltered during storage, transmission, or processing. It prevents unauthorized modification or destruction of data.

AVAILABILITY

- Availability ensures that authorized users have reliable access to information and systems when needed. Systems should function properly without downtime or unavailability due to attacks or other issues.

TYPES OF SECURITY CONTROLS

- **PREVENTIVE** - Security controls are measures designed to stop security incidents before they occur. They include access control policies that determine who can enter specific areas or systems, along with authentication processes to verify user identities.
- **DETECTIVE** - Security controls aim to identify and react to security incidents promptly. They encompass data encryption practices, audit trails, and logging mechanisms, vulnerability scanning techniques, penetration testing processes, and network monitoring strategies.
- **CORRECTIVE** - Data security controls are actions taken to fix problems after a security breach or failure. Their main goal is to reduce the damage, recover lost data or systems, and stop further harm.

What is Authentication, Authorization, and Accounting (AAA)?

Authentication, Authorization, and Accounting (AAA) is a three-process framework used to manage user access, enforce user policies and privileges, and measure the consumption of network resources.

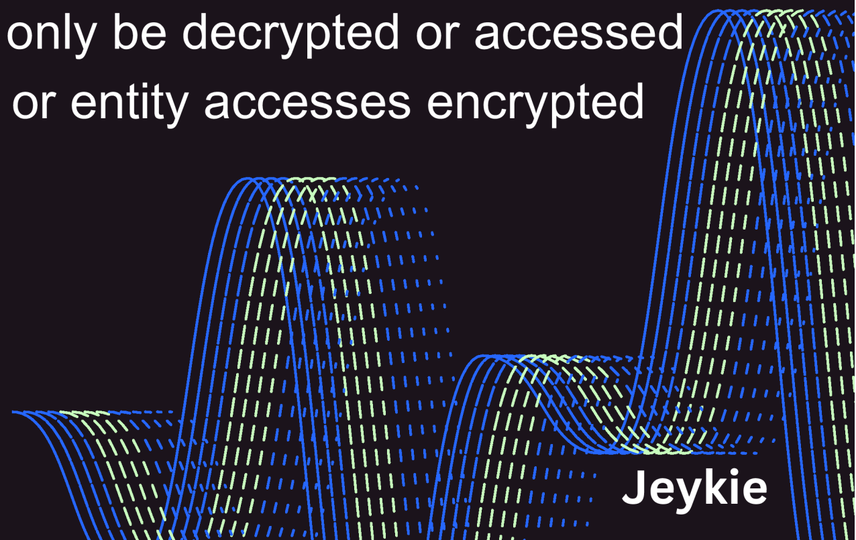
- **AUTHENTICATION** - Is the process of identifying a user and granting them access to the network. Most of the time, this is done through traditional username and password credentials.
- **AUTHORIZATION** - The authorization process enforces the network policies, granular access control, and user privileges. The cybersecurity AAA protocol determines which specific network resources the user has permission to access, such as a particular application, database, or online service.
- **ACCOUNTING** - Accounting helps in both security and operational evaluations. For instance, network administrators can look at user access privileges to specific resources to see about any changes.

AAA BENEFITS

- Improves Network Security
- Centralizes Protocol Management
- Allows Granular Control and Flexibility
- Provides Scalable Access Management
- Enables Information-Based Decision Making

DATA ENCRYPTION

Is a method of protecting data by encoding it in such a way that it can only be decrypted or accessed by an individual who holds the correct encryption key. When a person or entity accesses encrypted data without permission, it appears scrambled or unreadable.



IMPORTANCE OF DATA ENCRYPTION

- Data Confidentiality
- Data Integrity
- Compliance with Regulations
- Data Protection in Transit and at Rest
- Building Trust and Enhancing Privacy
- Mitigating the Impact of Data Breaches

SYMMETRIC VS. ASYMMETRIC ENCRYPTION

Symmetric - Symmetric encryption (or “private key” encryption) is the process of using a single key to both encrypt and decrypt data. It’s called “private key” because the use of a single encryption key necessitates that the key is always kept private.

Asymmetric - sender uses the recipient’s public key to encrypt the data. The recipient then uses their private key to decrypt the data. This approach allows for secure communication between two parties without the need for both parties to have the same secret key. Asymmetric encryption has several advantages over symmetric encryption, which uses the same key for both encryption and decryption.

COMMON ENCRYPTION ALGORITHMS

- The Advanced Encryption Standard (AES)
- Triple DES (Data Encryption Standard)
- RSA (Rivest- Shamir- Adleman)
- Blowfish
- Twofish

Operating system (OS)

Based security mechanisms are implemented within the software layer and work to protect the system from malicious activity, unauthorized access, and data breaches.

Operating System-Based Security Mechanisms

- User Authentication
- Access Control
- File Permissions
- Encryption
- Security Auditing and Logging
- Sandboxing

Hardware-Based Security Mechanism

- Trusted Platform Module
- Hardware Security Modules
- Hardware Firewalls

Access control lists (ACLs), user rights management, and file permissions.

Access Control Lists - are security tools that help control who can access certain resources, like files or folders, on a computer or network. Think of them as a set of rules that determine who is allowed to do what with those resources.

Types of ACLs:

- **Discretionary ACL (DACL)** - Specifies which users or groups are granted or denied access to an object. If a DACL is not set, the object will be accessible to everyone.
- **System ACL (SACL)** - Used to audit access to an object. When auditing is enabled, the system logs attempts to access the object (successful or unsuccessful) based on the rules defined in the SACL.

USER RIGHTS MANAGEMENT

It refers to the process of assigning and controlling what actions users can perform across the entire system, typically at a broader level than file or object permissions. These rights are often defined as privileges that control what a user can do within the operating system or network environment.

Key Concepts in User Rights Management :

- User Rights
- Group Membership
- Role Based Access Control

File Permissions

Are a security mechanism that controls access to files and directories based on a user’s identity or group membership. These permissions determine what actions a user can perform on a file or directory, such as reading, writing, or executing it.

Importance of regular updates and patch management.

Are crucial for keeping systems secure and running smoothly. When software developers discover bugs or vulnerabilities, they release updates to fix these issues. Installing these updates helps protect your devices from hackers who could exploit security gaps. Patches also improve performance and can add new features, making your software more efficient. Ignoring updates leaves your system exposed to risks and can cause it to become slow or unstable over time. By regularly updating your software, you ensure better security, functionality, and overall performance.

Importance of Software Updates and Patches :

- Enhancing PC Performance
- Boosting Workflow Efficiency
- Enhancing Security
- Ensuring Compatibility
- Unlocking Enhanced Features

APPLOCKER

AppLocker helps you control which apps and files users can run. These include executable files, scripts, Windows Installer files, dynamic-link libraries (DLLs), packaged apps, and packaged app installers. AppLocker is also used by some features of Windows Defender Application Control.AppLocker is a powerful tool for application control, allowing administrators to manage what software is allowed to run on their systems, thus providing a critical layer of security in modern IT environments.

Benefits of AppLocker

- Enhanced Security
- Granular Control
- Simplified Management
- Compliance

TYPES OF RULES

1. Executable Rules

Executable rules control the execution of standard applications that use the .exe and .com file extensions. These rules help ensure that only trusted and approved executable files are run on the system.

2. Windows Installer Rules

Windows Installer rules apply to .msi, .msp, and .mst file extensions, which are commonly used for software installation packages. These rules restrict or allow software installation using Windows Installer files, preventing users from installing unapproved applications.

3. Script Rules

Script rules control the execution of various types of script files, including:

- PowerShell scripts (.ps1)
- Batch files (.bat)
- VBScript files (.vbs)
- JScript files (.js)

Scripts are often used to automate tasks on a computer, but they can also be misused to run harmful code (like viruses). Script rules ensure that only trusted and safe scripts are allowed to run, helping to protect your system from malicious activity.

4. DLL Rules

Dynamic-link library (DLL) files, with the extensions .dll and .ocx, are often used by applications to extend functionality. However, they can also be exploited by malicious software. DLL rules control which DLLs are loaded by applications on the system.

Jane Carmel B. Duhig
Jeykie Rose R. Duhig