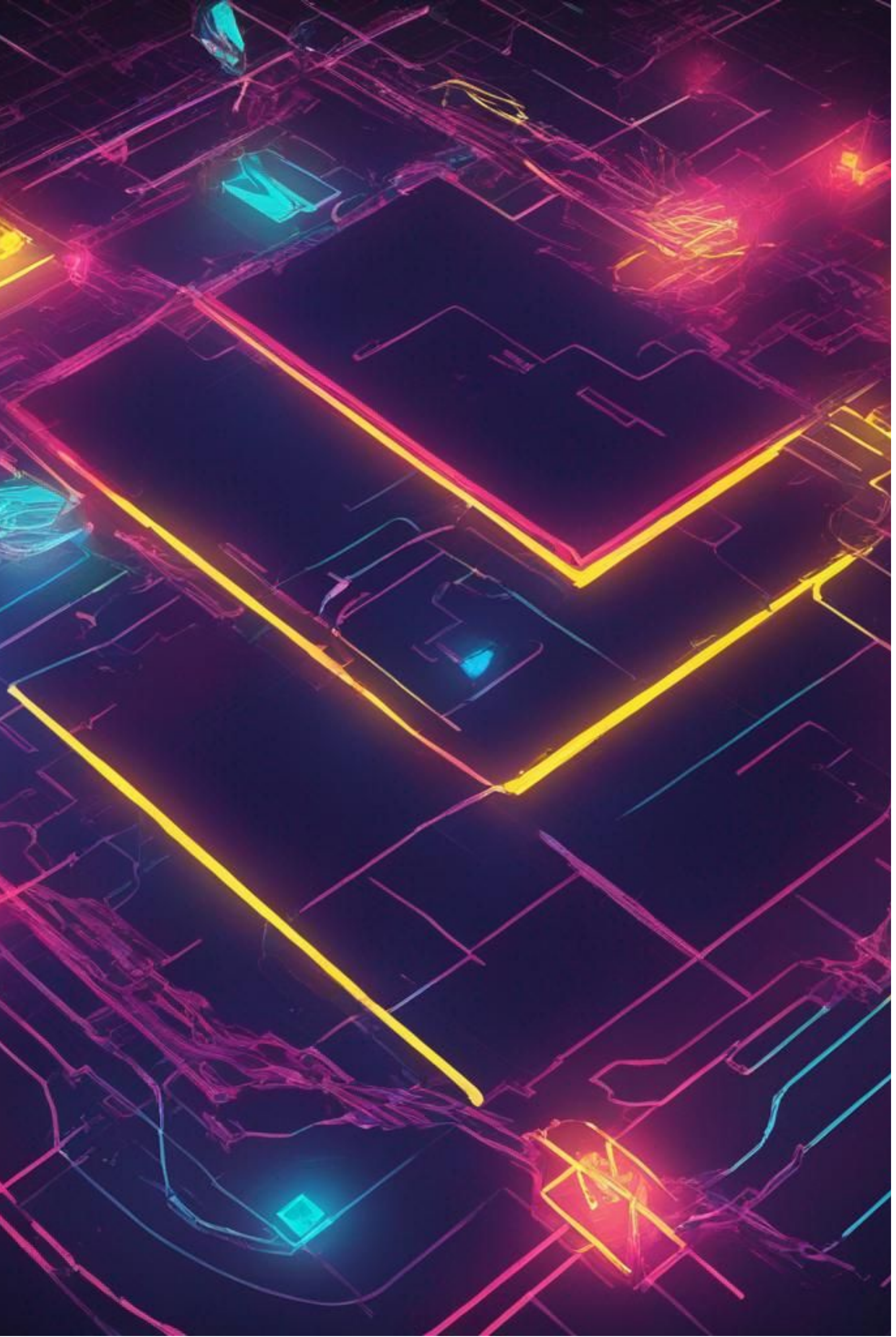

Securing the Digital Fortress

A Comprehensive Guide to Access Control in Information Security

CISSP Study Guide - IV

Introduction to Access Control

- **Objective:** Understand the principles of Access Control in information security.
- **Key Points:**

> - Protecting data from unauthorized access.
> - Balancing Confidentiality, Integrity, and Availability (CIA Triad).
> - Employing multiple security layers (Defense in Depth).

CIA Triad in Access Control

Confidentiality:

> Ensures non-disclosure to unauthorized entities.

- **Integrity:**

> Protects data from unauthorized modifications.

- **Availability:**

> Guarantees data access when needed.

- **Prevention Antonyms:**

> - Confidentiality vs. Disclosure
> - Integrity vs. Corruption
> - Availability vs. Destruction/Isolation

Default Security Stance

- **Options for Default Stance:**

> - **Allow-by-default:**
>
> Presumes open access unless specified.
>
> - **Deny-by-default:**
>
> Restricts access unless explicitly granted.

Defense in Depth Strategy

Strategy Layers:

- Policies and Awareness
- Physical and Perimeter Controls
- Internal Network Safeguards
- Host and Application Security
- Data Protection

Implementation Steps:

- Resource Identification
- User Identification
- Resource-User Relationship Mapping

Identification and Authentication

- **Identification:**

> Claiming an identity, typically via a username.

- **Authentication:**

> Verifying an identity via credentials, like passwords.

Authentication Factors

- **Three Factors for Robust Authentication:**

  - **Knowledge Factor:**

  Something a person knows (PIN, password).

  - **Ownership Factor:**

  Something a person has (smart card).

  - **Characteristic Factor:**

  Something a person is (biometric traits)

Password Types and Policies

- **Types of Passwords:**

> Standard, Combination, Complex, Passphrases, etc.

- **Password Management:**

> Proper account management and user account reviews.

- **Password Policies:**

> Define password life, history, complexity, and length.

Ownership and Characteristic Factors

- **Ownership Factors:**

> Include memory cards, smart cards, tokens.

- **Biometric Factors:**

> Involve physiological or behavioral characteristics (e.g., iris scans).

- **Biometric Effectiveness and Acceptance:**

> Ranked by security effectiveness and user friendliness.

Access Control Policies and Practices

- **Key Components:**

> Access Control Policy, Separation of Duties.

- **Access Levels:**

> No Access, Need-to-Know, Least Privilege.

- **Single Sign-On Systems:**

> Kerberos and SESAME, providing integrated authentication experiences.

Access Control Monitoring and Testing

- **Monitoring Tools:**

> IDS and IPS technologies.

- **Penetration Testing:**

> Simulates potential attacks to assess defenses.

- **Vulnerability Assessment:**

> Reviews standard practices, physical security, and systems.

- **Access Control Threats:**

> Includes password attacks, social engineering, malicious software, and more.

Access Control Categories and Types

- **Seven Main Categories:**

> Compensative, Corrective, Detective, etc.

- **Access Control Types:**

> Administrative, Logical/Technical, and Physical.

- **Access Control Models:**

> DAC, MAC, RBAC, etc.

Access Control Administration and Provisioning Life Cycle

- Administration Methods:

> Centralized vs. Decentralized control.

- Provisioning Life Cycle:

> Formal process for user account management.

Conclusion and Best Practices

Takeaways:

- Effectively managing access controls is critical for secure data.
- Employ a mixture of policies, technological solutions, and user training.
- Regular reviews and testing to adapt to evolving threats.

Information Security Buzz

Discover more at our InfoSec Knowledge Hub