Week 10:

Access Control is the process of protecting a resource so that it is used only by those allowed to.

**ACCESS CONTROL FUNCTIONS**

**Identification**: Who is asking to access the asset?

Subjects supplying identification information - Username, user ID, account number.

**Authentication:** Can their identities be verified?

Verifying the identification information - Passphrase, PIN, biometric, password, OTP

**Authorisation:** What can the requester access and do?

Using criteria to determine what the subjects can do on objects.

**Accountability:** How are actions traced to an individual to ensure the person who makes data or system changes can be identified? Audit logs and/or real-time monitoring to track subject activities with objects.

**POLICY DEFINITION AND POLICY ENFORCEMENT PHASES**

**Policy Definition Phase:** This initial phase involves defining who has access to specific systems or resources and what actions they can perform. It is closely tied to the authorization phase.

**Policy Enforcement Phase:** In this phase, requests for access are either granted or rejected based on the authorizations defined in the first phase. This phase is closely tied to the identification, authentication, and accountability processes.

**TYPES OF ACCESS CONTROL**

**Physical Access Control:**

- Cards or fingerprints regulate access to physical resources.

- Smart cards, programmed with ID numbers.

- parking lots, elevators, and office doors.

**Logical Access Control:**

- Determines which users can access a system.

- Monitors and tracks user activities within the system.

- Restricts or influences user behaviours on the system, enhancing security and compliance.

**ENFORCING ACCESS CONTROL**

**The Security Kernel:**

A diagram of a security system

Description automatically generated - Acts as the central authority for enforcing access control in computer systems.

- Implements the reference monitor concept

**Enforcement Process:**

- A subject requests access to an object, which is intercepted by the security kernel.

- The security kernel consults its rules base or database to determine whether to allow or deny acces

- All access requests processed by the system are logged for future tracking and analysis, contributing to overall security management.

A green and yellow sign with white text

Description automatically generated

**AUTHENTICATION TYPES**

**Authentication by Knowledge: Something you know** Passwords, passphrases. PIN number.

**Authentication by Ownership: Something you own.**

Synchronous token- Calculates a number at both the authentication server and the device.

Time-based synchronization, i.e. software authenticator

Event-based synchronization, i.e. SMS one time password

Asynchronous token: Fixed, no calculation is needed if you prove you physically have it, you can access - USB token or Smart card.

A diagram of a computer

Description automatically generated

**Authentication by Characteristics: Something unique to you** - **Biometrics** Something Static. Fingerprint, facial recognition, hand geometry, Retina scan.

Something Dynamic such as What you do! Voice patterns, keystroke dynamics, signature dynamics

**Authentication by Location: Somewhere you are** – Location. Strong indicator of authenticity

**GENERAL PRINCIPLES**

Files and folders are managed by the operating system.

Applications, including shells, access files through an API.

* Access control entry (ACE) - Allow/deny a certain type of access to a file/folder by user/group.
* Access control list (ACL) - Collection of ACEs for a file/folder

An opaque identifier provided by the operating system, used by applications to access files and folders.

File operations.

* Open file: returns file handle.
* Read/write/execute file.
* Close file: invalidates file handle.

Files and folders are organized hierarchically, represented as a tree structure in Windows and a Directed Acyclic Graph (DAG) in Linux.

**ACCESS POLICIES**

Top of Form

Bottom of Form

**Closed Policy**: In this type of policy, all access is denied by default, except what is explicitly allowed.

**Open Policy**: This policy is the opposite of the closed policy. All access is allowed by default, except what is explicitly denied.

**Closed Policy with Negative Authorizations and Deny Priority**: This policy is a variation of the closed policy but includes explicit denials, which take priority over permissions.

**ACCESS CONTROL MODELS**

**Need to know** This principle ensures that subjects are granted access only to what they need to know for their work tasks and job functions.

**Least privilege** This principle ensures that subjects are granted only the privileges they need to perform their work tasks and job functions.

**Separation of privileges** This principle ensures that sensitive functions are split into tasks performed by two or more employees.

An access control model is a framework that dictates how subjects access objects.

It uses access control technologies and security mechanisms to enforce the rules and objectives of the model.

**THERE ARE FOUR MAIN TYPES OF ACCESS CONTROL MODELS:**

❐ \_Discretionary

(Rest are called non-discretionary)

❐ \_Mandatory

❐ \_Rule Based

❐ \_Attribute-based access control (ABAC)

**DISCRETIONARY ACCESS CONTROL**

Information owner decides who can access the system(s).

Allows entities to grant access rights, enabling them to authorize other entities' access to resources.

- Commonly used in operating systems like Windows, Macintosh, UNIX, etc.

Often implemented using an access matrix:

- One dimension: Identifies subjects attempting data access.

- Other dimension: Lists the objects that can be accessed.

**Access Control Lists (ACL):**

- Definition: List or file of users granted access privileges to a system or resource (e.g., a database).

- Contents: User ID and associated privilege(s) for that user and resource.

- Typical privileges: Read, Write, Update, Execute, Delete, Rename.

**User Provisioning:**

- Granting access to new employees - Includes checking management approvals before granting access.

Non-Discretionary Access Control:

- Access rules are controlled by a security administrator, not system owners or ordinary users.

- Sensitive files are write-protected to maintain integrity and are readable only by authorized users.

- Generally considered more secure than discretionary access control.

- Security is enforced and tamper-proof.

**MANDATORY ACCESS CONTROL (MAC)**

Determined by the sensitivity of the resource.

Access Decision Factors: Based on subjects, objects, and labels.

Common Usage: Often employed in military and government systems.

Labelling System: Objects are assigned classification labels (e.g., Top Secret, Secret, Confidential, Unclassified).

Subjects: Individuals or systems granted clearance to access objects within the information system.

Objects: Elements within the information system protected from unauthorized use or access.

**RULE BASED ACCESS CONTROL (RBAC)**

Uses specific rules to govern interactions between subjects and objects.

Operates on "if X then Y" programming rules, enabling finer-grained access control to resources. Before a subject access an object in a particular circumstance, it must satisfy a predefined set of rules.

**ATTRIBUTE-BASED ACCESS CONTROL (ABAC)**

Defines authorizations based on conditions related to properties of both the resource and the subject.

Strength: Flexibility and expressive power.

- Adoption Obstacle: Concern about the performance impact of evaluating predicates on both resource and user properties for each access.

- Interest: Considerable interest in applying the model to cloud services, despite adoption challenges.

**AUTHENTICATION, AUTHORISATION, AND ACCOUNTING (AAA)**

Employed with remote access systems like virtual private networks (VPNs) and network access servers for centralized access control.

Prevents remote attacks on internal LAN authentication systems and other servers.

If a separate system is used for remote access, only remote access users are affected in the event of a successful attack on this system.

AAA protocols are commonly utilized for mobile IP, providing access to mobile users with smartphones.

**CENTRALISED AND DECENTRALISED AAA**

Additional access control mechanisms are required - insecure networks to create a connection to the corporate local area network.

Centralised authentication, authorization, and accounting (AAA) servers

❐ \_RADIUS

❐ \_TACACS+

❐ \_DIAMETER

Decentralised Access Control: Access control is in the hands of the people closest to the system users.

❐ \_Password Authentication Protocol (PAP)

❐ \_Challenge-Handshake Authentication Protocol (CHAP)

❐ \_Mobile device authentication, Initiative for Open Authentication (OATH). For example, One-Time Password (OTP)

**REMOTE USER ACCESS AND AUTHENTICATION (RADIUS)**

RADIUS is a client/server protocol and software.

Enables remote access users to communicate with a central server to authorise their access to the requested system or service.

It allows companies to have a single administered entry point.

Provides standardization in security and a simplistic way to track usage and network statistics.

**TACACS+ ARCHITECTURE**

* TACACS+ uses TCP as its transport protocol, while RADIUS uses UDP.
* TACACS+ is the better choice for complex environments such as corporate networks.

Requires

* More sophisticated authentication steps
* Tighter control over more complex authorisation activities.

Any software that uses UDP as its transport protocol has to be ”fatter” with intelligent code. TACAS+ will be faster to transmit.

**DIAMETER**

* Developed to enhance RADIUS functionality and address its limitations.
* Utilizes TCP as its transport protocol, offering reliability and ordered data transmission.
* Provides similar functionalities as RADIUS and TACACS+ and extends support to wireless network access.
* Offers increased flexibility and capabilities to cater to the requirements of modern, intricate networks.
* Capable of addressing challenges like mobile IP, reflecting its adaptability to evolving network scenarios.
* Beyond AAA (Authentication, Authorization, and Accounting) functionality, Diameter incorporates features like roaming operations and protection against replay attacks.

**SINGLE SIGN-ON (SSO)**

Users maintain a single password for accessing all corporate and back-office systems and applications necessary for their tasks.

By utilizing only one password, the security of the entire access control system is supported, reducing the likelihood of password-related vulnerabilities.

SSO mechanisms include:

**KERBEROS:** A network authentication protocol that enables users to securely authenticate to various network services using a single set of credentials.

Through the utilization of symmetric-key cryptography.

Provided freely by the Massachusetts Institute of Technology (MIT).

Operates by assigning a unique key, known as a ticket, to each user upon login.

Enables users to authenticate once and subsequently access all resources based on the permission level associated with their ticket.

**FEDERATED IDENTITIES:** Allows users to access multiple systems or applications across different organizations using their credentials from a trusted identity provider, eliminating the need for separate login credentials for each service.