Autorizzazione e controllo accessi

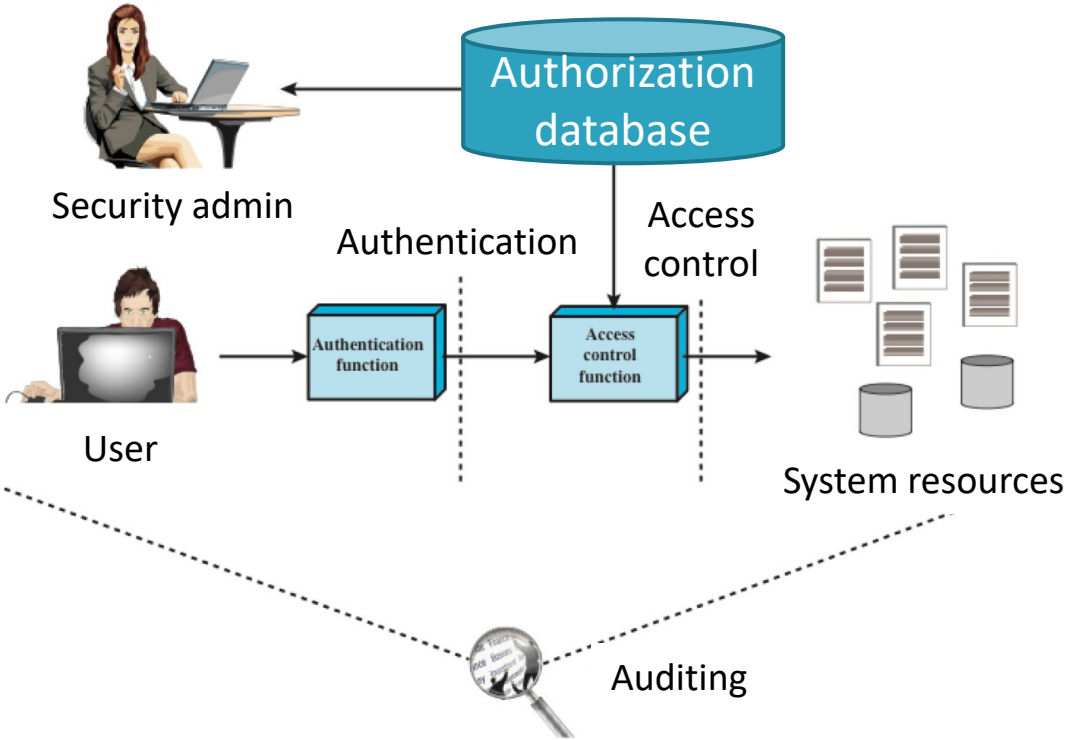
Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati.
- Modelli e tecniche per autorizzazione e controllo dell’accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

Indice

- Tecniche di autenticazione e multi-factor authentication
- Protocolli di autenticazione
- Gestione delle password e dei certificati.
- Modelli e tecniche per autorizzazione e controllo dell’accesso
- Privileged Identity and Access Management (PAM)
- Cenni sulla segregazione e segmentazione delle reti

Controllo degli accessi



Politiche di gestione degli accessi

- Verificare ogni accesso
  - Tenere traccia degli accessi di ciascun utente
- Applicare il principio del *minimo privilegio*
- Verificare l'accettabilità del *tipo di uso* richiesto
  - Memorizzare le azioni svolte dagli utenti con un livello di dettaglio proporzionato al valore delle risorse e al rischio
- Requisiti per controllo accessi secondo NIST

Politiche di gestione degli accessi

- Verificare ogni accesso
  - Tenere traccia degli accessi di ciascun utente
- Applicare il principio del *minimo privilegio*
- Verificare l'accettabilità del *tipo di uso* richiesto
  - Memorizzare le azioni svolte dagli utenti con un livello di dettaglio proporzionato al valore delle risorse e al rischio
- Requisiti per controllo accessi secondo NIST

Politiche di gestione degli accessi

- Verificare ogni accesso
  - Tenere traccia degli accessi di ciascun utente
- Applicare il principio del *minimo privilegio*
- Verificare l'accettabilità del *tipo di uso* richiesto
  - Memorizzare le azioni svolte dagli utenti con un livello di dettaglio proporzionato al valore delle risorse e al rischio
- Requisiti per controllo accessi secondo NIST

Politiche di gestione degli accessi

- **RBAC** – Role Based Access Control
  Utenti raggruppati in base al *ruolo*. A ciascun ruolo sono associati specifici *privilegi* di accesso
- **ABAC** – Attribute Based Access Control
  Privilegi definiti in base ad attributi dell'utente e al contesto d'uso.

Politiche di gestione degli accessi

- **RBAC** – Role Based Access Control
  Utenti raggruppati in base al *ruolo*. A ciascun ruolo sono associati specifici *privilegi* di accesso
- **ABAC** – Attribute Based Access Control
  Privilegi definiti in base ad attributi dell'utente e al contesto d'uso.

Politiche di gestione degli accessi

- **DAC** – Discretionary Access Control
  A ciascun utente sono assegnati i privilegi di accesso alle risorse
- **MAC** – Mandatory Access Control
  A ciascun oggetto è assegnata una *classe* di riservatezza.
  A ciascun soggetto è assegnato un livello di riservatezza a cui ha accesso (*clearance*).
  Accesso consentito se *clearance* >= *classe*

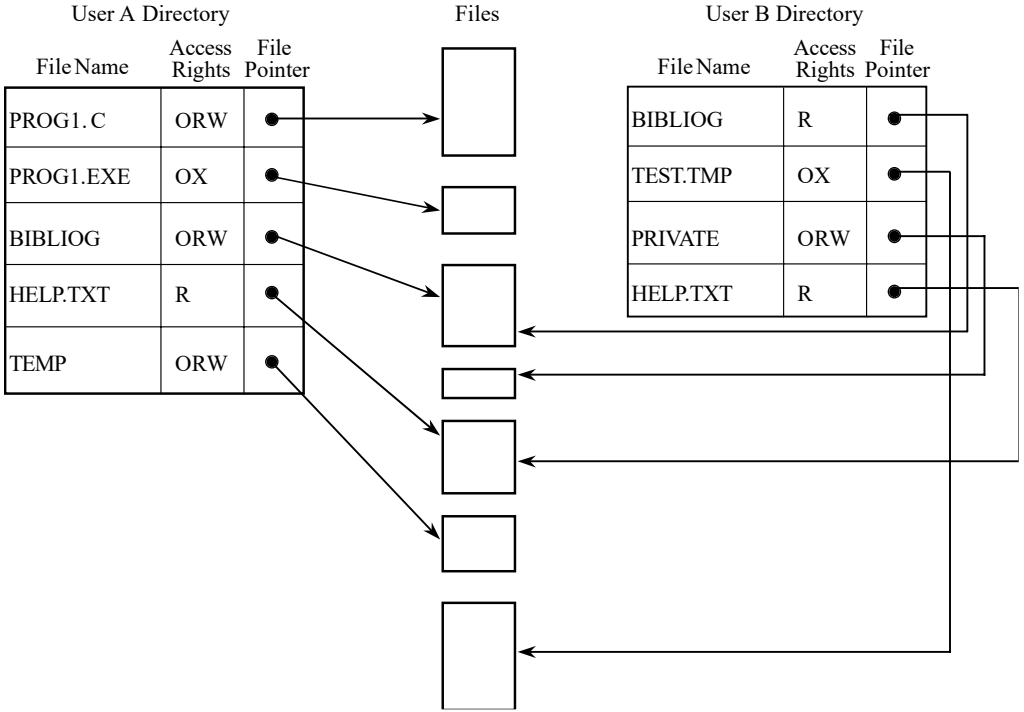
Politiche di gestione degli accessi

- **DAC** – Discretionary Access Control
  A ciascun utente sono assegnati i privilegi di accesso alle risorse
- **MAC** – Mandatory Access Control
  A ciascun oggetto è assegnata una *classe* di riservatezza.
  A ciascun soggetto è assegnato un livello di riservatezza a cui ha accesso (*clearance*).
  Accesso consentito se *clearance* >= *classe*

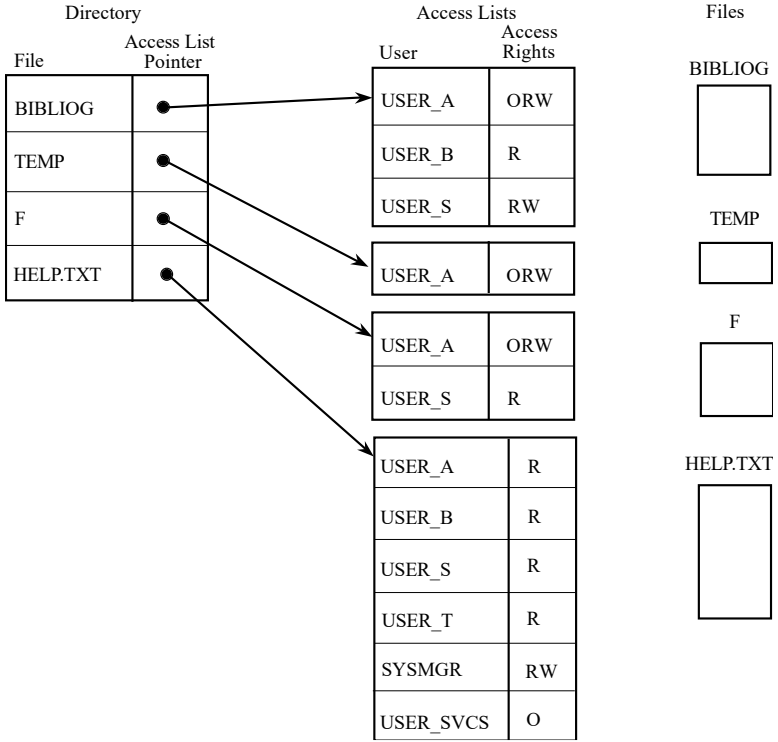
Implementazione del controllo degli accessi

- Access control directory
- Access control list
- Procedure-oriented access control
- Role-based access control

Access control directory



Access control list

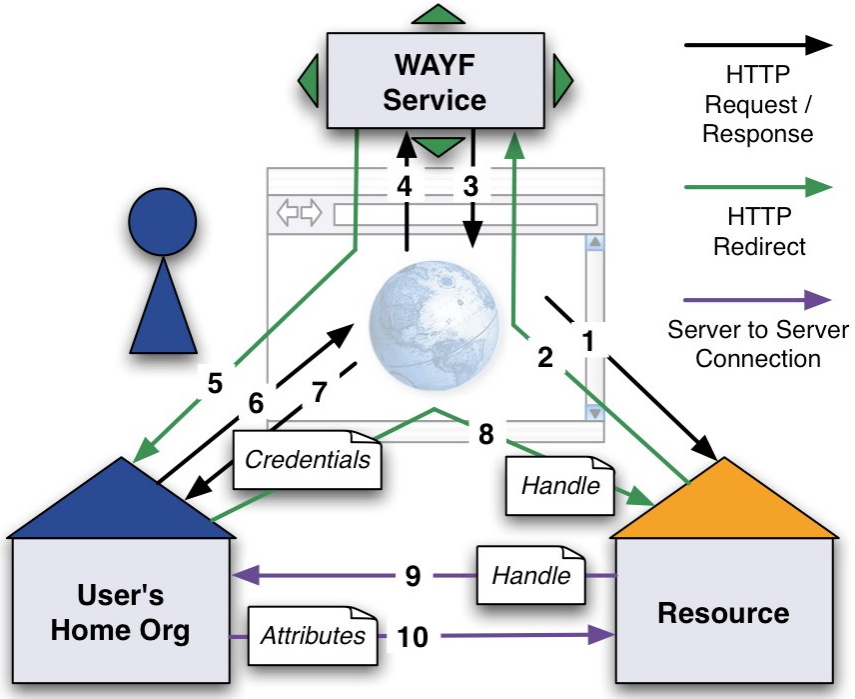


Servizi di directory

- Archivi gerarchici per memorizzare
  - Identità
  - Certificati
  - Gestione dei permessi
- LDAP – Lightweight Directory Access Protocol
  - Utilizzato in diversi prodotti commerciali (Microsoft, IBM, ecc.)
  - open-source: openldap

Security Assertion Markup Language (SAML)

- Standard XML per l'autenticazione centralizzata e l'invio di autorizzazioni
  - Usato ad es. da Shibboleth, SPID



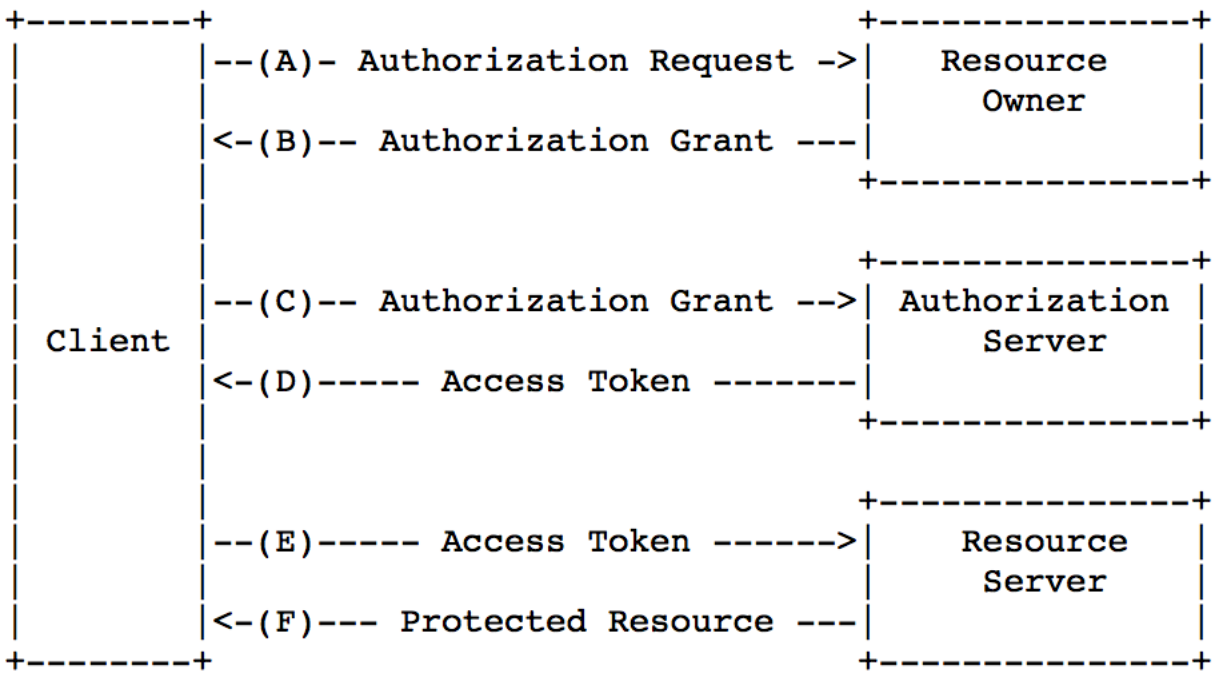
WAYF = Where Are You From

OAuth

- Standard IETF (RFC 6749) che consente a una risorsa di chiedere l'autorizzazione all'accesso da parte di un utente a un servizio *terzo* rispetto a utente e risorsa.
  - Ad es., autenticazione su un sito web delegata a Facebook, o Google, o Linkedin o altri
  - Autenticazione gestita dal servizio terzo. L'utente autorizza l'invio al sito web di alcune informazioni identificative

OAuth

Protocol Flow



Approfondimento 1:
Requisiti controllo accessi NIST

- NIST SP 800-171

	Basic Security Requirements
1	Limit information system access to authorized users, processes acting on behalf of authorized users, or devices
2	Limit information system access to the types of transactions and functions that authorized users are permitted to execute.
	Derived Security Requirements
3	Control the flow of CUI in accordance with approved authorizations.
4	Separate the duties of individuals to reduce the risk of malevolent activity without collusion.
5	Employ the principle of least privilege, including for specific security functions and privileged accounts.
6	Use non-privileged accounts or roles when accessing nonsecurity functions.
7	Prevent non-privileged users from executing privileged functions and audit the execution of such functions.
8	Limit unsuccessful logon attempts.
9	Provide privacy and security notices consistent with applicable CUI rules.
10	Use session lock with pattern-hiding displays to prevent access and viewing of data after period of inactivity.

CUI = controlled unclassified information

Approfondimento 1: Requisiti controllo accessi NIST

- NIST SP 800-171 (continua)

Derived Security Requirements	
11	Terminate (automatically) a user session after a defined condition.
12	Monitor and control remote access sessions.
13	Employ cryptographic mechanisms to protect the confidentiality of remote access sessions.
14	Route remote access via managed access control points.
15	Authorize remote execution of privileged commands and remote access to security-relevant information.
16	Authorize wireless access prior to allowing such connections.
17	Protect wireless access using authentication and encryption.
18	Control connection of mobile devices.
19	Encrypt CUI on mobile devices.
20	Verify and control/limit connections to and use of external information systems.
21	Limit use of organizational portable storage devices on external information systems.
22	Control CUI posted or processed on publicly accessible information systems.

CUI = controlled unclassified information