

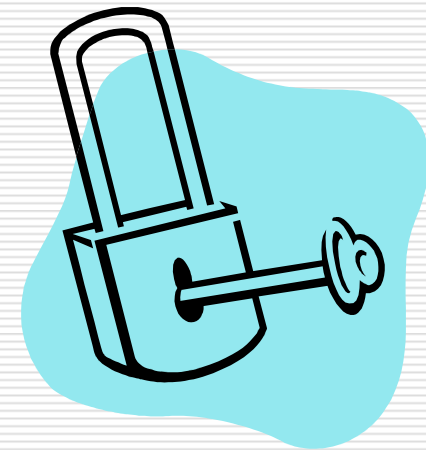
**Esperti nella gestione dei sistemi
informativi e tecnologie informatiche**

**Sistemi avanzati di gestione
dei Sistemi Informativi**

Docente: Eduard Roccatello
Email: eduard@roccatello.it
Sito: <http://www.roccatello.it/teaching/gsi/>

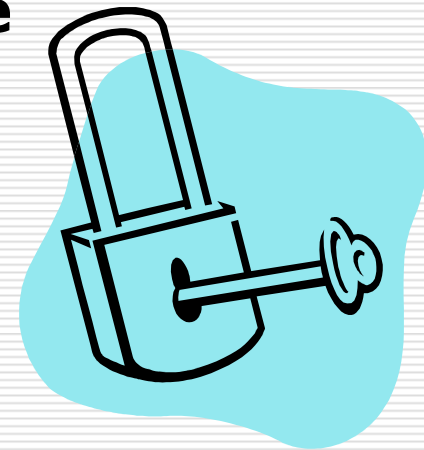
Sistemi di autenticazione avanzati

- **Un sistema di autenticazione centralizzato** deve permettere di **accertare l'identità** degli utenti per tutti i servizi disponibili, **evitando la duplicazione** del database contenente le **credenziali**.

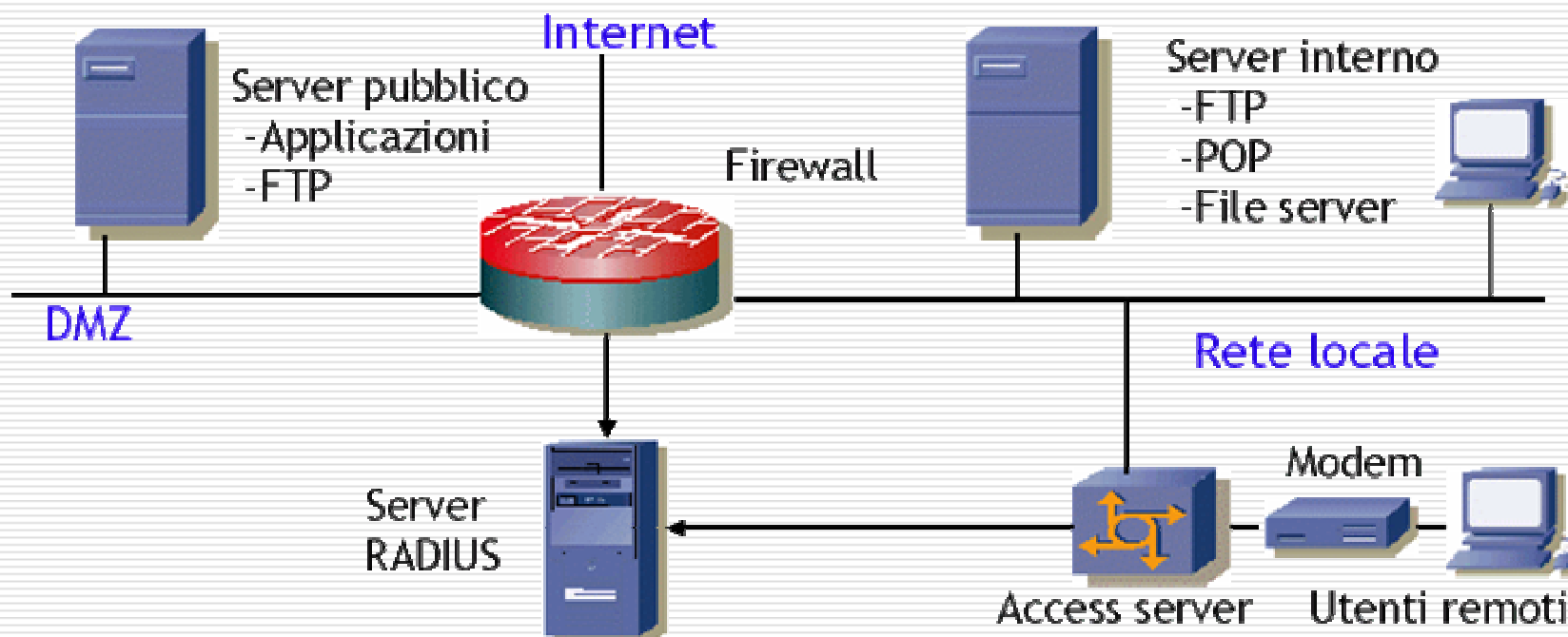


Sistemi di autenticazione avanzati

- Se è in grado di fornire anche l'autorizzazione, deve permettere **l'accesso ai servizi in base ai permessi** di cui l'utente dispone.



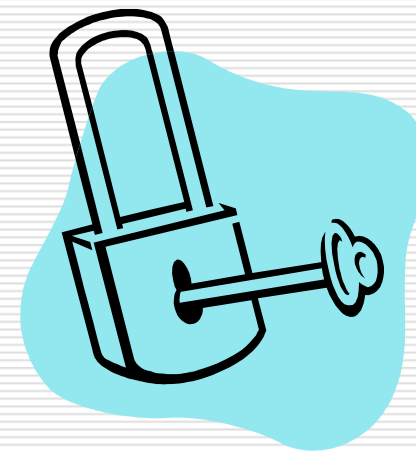
Sistemi di autenticazione avanzati



Per i 4 servizi **autenticazione ed autorizzazione vengono effettuati localmente** da ogni sistema, la complessità di gestione ed i rischi di accessi non autorizzati sono facilmente immaginabili.

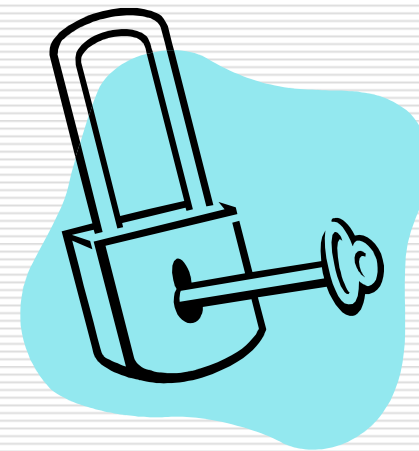
Sistemi di autenticazione avanzati

- ❑ Un sistema centralizzato che possa operare in tale situazione deve poter **dialogare con sistemi eterogenei**.
- ❑ Oltre ai server, anche i client che richiedono di autenticarsi possono essere di diversa natura.
- ❑ Un requisito fondamentale è la **capacità di interagire con il maggior numero di sistemi**.



Sistemi di autenticazione avanzati

- ❑ **Posso fornire un sistema di autenticazione avanzato sia in ambiente Linux che in ambiente Windows**
 - **Linux**
 - ❑ LDAP
 - ❑ NIS / NIS+
 - **Microsoft Windows**
 - ❑ Active Directory
 - ❑ Samba (con server **Linux**)

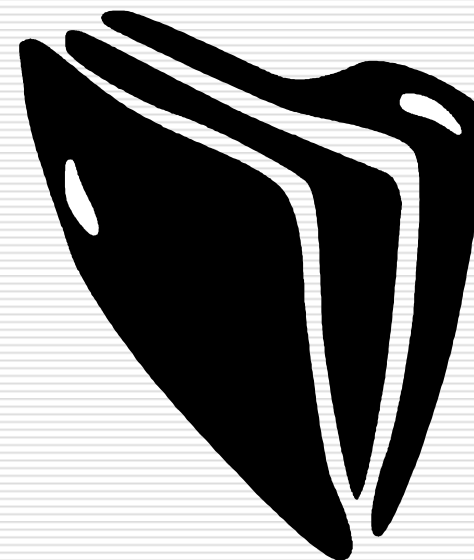


Introduzione ai servizi di Directory

- ❑ **LDAP** (Lightweight Directory Access Protocol) è uno standard aperto per l'erogazione di servizi di directory tramite una rete.
- ❑ È basato sullo standard **X.500** e su **TCP/IP**.
- ❑ Ne esistono diverse implementazioni tra le quali spiccano **Microsoft Active Directory**, **IBM Directory Server** e **Oracle Directory Service** in ambito commerciale e **OpenLDAP** nell'ambito del software libero.

Introduzione ai servizi di Directory

- ❑ **LDAP** deriva da **DAP**, che è un protocollo molto complesso basato sul modello OSI (7 strati) e **richiede un ammontare significativo di risorse.**
- ❑ **LDAP** è progettato per funzionare su TCP/IP (solo 4 strati) ed **offre la maggior parte della funzionalità di DAP ad un costo ridotto.**



Cos'è una Directory?

- Una directory è un **database ottimizzato per la ricerca** e la lettura di informazioni riguardanti oggetti presenti all'interno di una rete. Le informazioni sono **basate su attributi**.

- I servizi di directory possono essere di **2 tipi**:
 - I **servizi di directory locali** permettono di accedere ad informazioni in un contesto molto ristretto (es. servizio finger su un singolo host).

 - I **servizi di directory distribuiti** permettono la partizione e la replica dei dati su differenti macchine per bilanciare il carico di lavoro (es. DNS).

Cos'è una Directory?

- ❑ La gestione delle informazioni in LDAP è basata sul concetto di entry. Un **entry** è una **raccolta di attributi che fanno riferimento ad identificatore** chiamato Distinguished Name (DN).
- ❑ Ogni **attributo** ha un **tipo** ed uno o più **valori**. I tipi sono tipicamente sequenze mnemoniche, come "cn" per il nome o "mail" per l'e-mail.
- ❑ La sintassi dei valori dipende dal tipo di attributo. Un attributo "cn" contiene il nome di un utente.
- ❑ Il formato testuale di una entry è chiamato **LDIF**.

OpenLDAP – LDAP Opensource

- ❑ OpenLDAP è **un'implementazione "Open Source"** di strumenti a supporto del protocollo LDAP.
- ❑ OpenLDAP è stato **adottato dalle maggiori distribuzioni Linux** e usato soprattutto per l'autenticazione, supporta la distribuzione dei carichi di lavoro, fornisce brevi tempi di risposta e permette la replica delle informazioni.
- ❑ Le principali applicazioni della suite OpenLDAP sono **slapd** e **slurpd**. Si tratta di due demoni che gestiscono le informazioni contenute nella directory (slapd) e la replica delle stesse (slurpd).

OpenLDAP – LDAP Opensource

- Il funzionamento di LDAP si basa sul **paradigma client-server** e su una gestione gerarchica degli oggetti presenti nella directory.
- LDAP permette una **distribuzione uniforme** dei dati, **tempi di risposta ridotti** nella lettura del contenuto degli oggetti e la possibilità di **replicare le informazioni** su server distinti per un **bilanciamento del carico di lavoro** nella rete.

OpenLDAP – Vantaggi e svantaggi

□ VANTAGGI

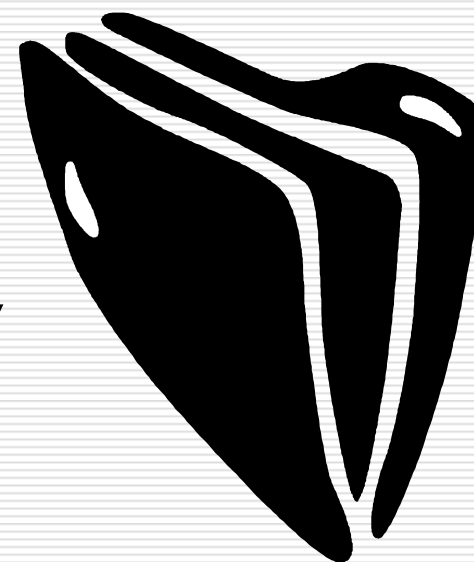
- Centralizzazione delle informazioni
- Semplicità nella gestione degli account (anche via interfaccia Web)
- Scambio di informazioni nativo con Microsoft Active Directory
- Replica delle informazioni tra più server OpenLDAP

□ SVANTAGGI

- Tempi di configurazione
- Perdita di prestazioni

Windows e i servizi di Directory

- ❑ Vi sono **molte differenze** fra Windows 2000 Server, e successivi, e la versione precedente del sistema operativo di rete di Microsoft, Windows NT 4 Server.
- ❑ Cambiamenti sul fronte della **flessibilità di gestione**, della **sicurezza**, dell'apertura agli **standard** e della **scalabilità**.
- ❑ Il miglioramento è stato possibile attraverso la **revisione di molti aspetti** base del sistema e attraverso l'introduzione di nuove strutture.



Windows – Concetto di dominio

- ❑ L'unità di amministrazione di Windows Server è il **dominio**.
- ❑ Indica un **insieme di computer che eseguono l'autenticazione** e ricevono l'elenco degli utenti accreditati da un controller centrale denominato "Primary Domain Controller" (PDC).
- ❑ Nel PDC ci sono le **liste degli utenti e dei gruppi**, più i relativi diritti. Vengono impostate dal sysadmin.
- ❑ Tutti i **client eseguono il login sul PDC** e da questo ricevono l'eventuale conferma di accesso.
- ❑ Tutte le informazioni sul dominio sono memorizzate in locale all'interno del sistema operativo server.

Windows – Problemi di scalabilità

- ❑ Se ho due domini separati **posso integrarli fra di loro attraverso un meccanismo di accesso fiduciario.**
- ❑ Gli utenti si autenticano localmente e ottengono tutte le autorizzazioni per lavorare sulle rispettive reti interne. Ogni rete contiene però gli elenchi dei soli utenti locali. Purtroppo alcuni utenti della filiale hanno bisogno di accedere al sistema della sede centrale per ottenere informazioni. **Devo effettuare un trasferimento delle informazioni verso il server principale.**
- ❑ Il sistema di trasferimento basato sulla fiducia è comodo per realtà modeste ma **risulta poco scalabile.** Realtà ampie, dotate di decine di succursali con diversi PDC dedicati per reparti, sono realizzabili con molta difficoltà entro questo modello.

Windows – Active Directory

- ❑ E' il **sistema integrato e distribuito di directory service** adottato dai sistemi operativi Microsoft a partire da **Windows 2000 Server**.
- ❑ In Active Directory sono integrate tutte le applicazioni per la **gestione dei servizi di rete e dominio**.
- ❑ **Utilizza vari protocolli** tra cui LDAP, Kerberos e DNS.
- ❑ In Active Directory LDAP viene usato come una base di dati che memorizza in forma centralizzata tutte le informazioni di un dominio di amministrazione, col vantaggio di mantenere tutta questa **informazione sincronizzata** tra i vari server di autenticazione di accesso alla rete.
- ❑ Possono gestire da una singola installazione con pochi centinaia di oggetti a **grandi installazioni con milioni di oggetti**.

Active Directory – Gerarchia

- ❑ La directory è strutturata all'interno della rete secondo una **modalità gerarchica**.
- ❑ Non è sensato avere un'unica directory per le informazioni di tutta la rete e di tutti i domini che fanno parte della propria organizzazione. Una raccolta monolitica di informazioni implica infatti un carico maggiore durante le ricerche dei dati e comporta problemi di memorizzazione, di mantenimento dei dati e di banda passante.
- ❑ **La directory è perciò partizionata per zone**: a ogni dominio della rete corrisponde una partizione.
- ❑ Per migliorare l'efficienza nelle ricerche si è provveduto comunque a **memorizzare una serie di attributi di tutte le informazioni in un catalogo centrale di riferimento**. Attraverso questo meccanismo si hanno i vantaggi di una struttura distribuita e la velocità di un archivio globale.

Samba – PDC e AD Opensource

- ❑ Samba è un progetto open source che fornisce **servizi di condivisione di file e stampanti** a client SMB/CIFS. Permette di ottenere interoperabilità tra sistemi diversi e può girare su piattaforme che non siano Microsoft Windows.
- ❑ Samba utilizza il **protocollo TCP/IP** utilizzando i servizi offerti sul server ospite.
- ❑ Quando correttamente configurato, permette di interagire con client o server Microsoft Windows come se fosse un file e print server Microsoft agendo da **Primary Domain Controller (PDC)**, può inoltre prendere parte ad un dominio **Active Directory**.

Samba – Problemi della versione 3.x

□ **FUNZIONALITÀ**

- **File server**
- **Print server**
- **Wins server**
- **Domain Controller NT4 compatibile**
- **Domain Server**
- **Domain Workstation (winbind)**

□ **LACUNE**

- **Mancano tutti i protocolli di sincronizzazione “nativi”**
- **Non è possibile avere DC misti MS+Samba**
- **Non è possibile avere wins secondari**

Samba 4 – Il futuro

- **Supporto completo ad Active Directory**
 - Comporta l'integrazione con Kerberos, DNS, LDAP, CLDAP, ecc..
- **È necessario**
 - Completo emulazione di tutte le RPC
 - Supporto di MSRPC e SMB su più trasporti
 - Implementazione di altri protocolli
 - Heimdal e MIT per Kerberos
 - openLdap* per LDAP
 - BIND come DNS Server