Utenti, sistemi e sicurezza

Un sistema informatico viene tipicamente usato da molti utenti:

- alcune risorse devono essere **protette**
- altre risorse devono essere **condivise**
- le politiche di sicurezza impongono un **confinamento**
  - gli utenti possono operare solo su certe risorse e non su altre
- molti modelli sono stati sviluppati per esprimere **politiche di confinamento.** Per confinare bisogna:
  - **distinguere** gli utenti
  - **identificare l'operazione** richiesta
  - **identificare l'oggetto** su cui l'operazione opera
  - **prendere una decisione** (operazione ammessa o negata)

Tali requisiti sono alla base di due modelli:

- **AAA** nato in ambito telecomunicazioni con scopi non di sicurezza
- **REFERNCE MONITOR** nato in ambito militare per semplificare la certificazione dei sistemi

Poi abbiamo

- MAC e DAC altri modelli per le politiche di accesso
- Utenti non distinti tutti gli utenti indistinti hanno gli stessi diritti

AAA

Authentication, Authorization, Accounting

- RFC (*Request For Comments*) 2903, anno 2000
- orientato alle reti
- radius è un "AAA protocol"
- accounting: contabilizzazione del consumo delle risorse

L'attenzione era sull'accesso a servizi di connettività, non su sicurezza

AAA e la sicurezza

AAA è ora associato sopratutto alla sicurezza non solo di reti, ma anche di sistemi sw e sistemi operativi.
È più corretto parlare di **Authentication, Authorization e AUDITING** (infatti l'accounting non è molto rilevante in ambito sicurezza)

Autenticazione

- Identifica l'utente (es. con username e password)
- l'utente è rappresentato nel sistema in qualche modo
  - nei sistemi operativi l'utente e rappresentato da uno o più processi con adeguate informazioni collegate al processo
  - nelle reti può essere una firma elettronica o un identificatore di utente in una sessione
  - tale informazione è input alla fase di autorizzazione

IdUtente ↔ Utente umano

- Ciascun utente umano dovrebbe essere rappresentato da uno e un solo identificatore
- Più identificatori per un utente
- Più utenti per un identificatore

Autorizzazione

è in realtà composta di tre fasi

- richiesta di accesso
- controllo di accesso
- autorizzazione

Auditing

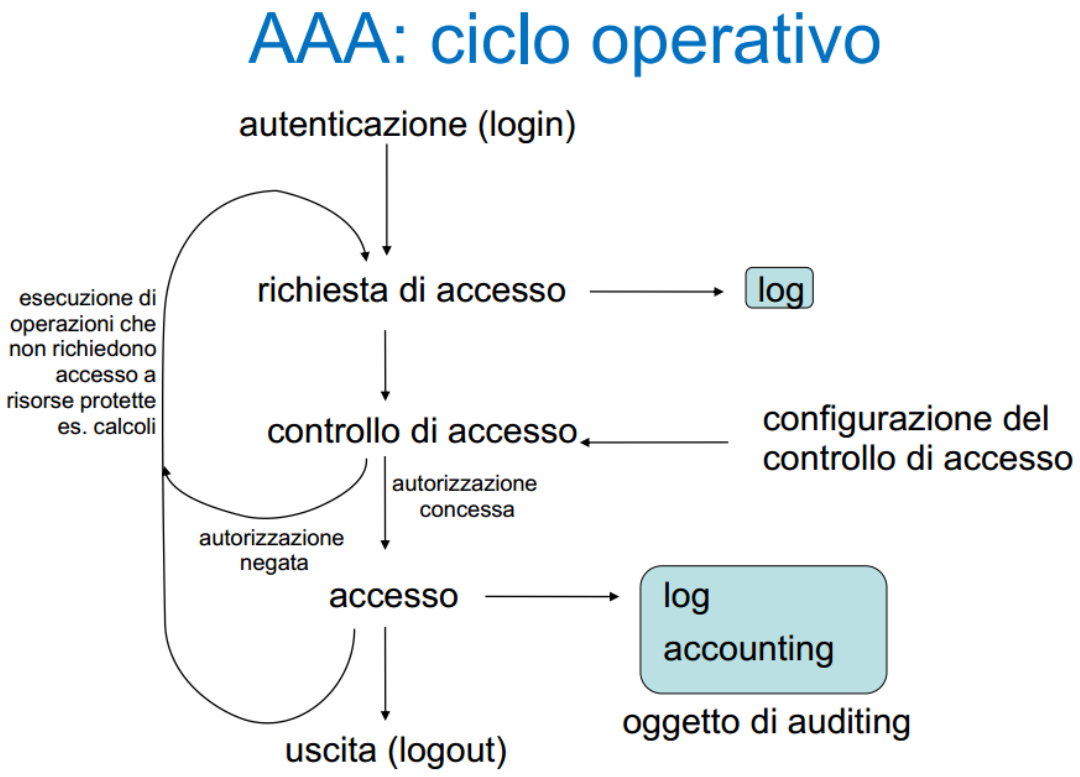
tipici eventi oggetto di auditing nel modello AAA

• autenticazione (riuscita o negata)
• richiesta di accesso
• autorizzazione per una richiesta di accesso (concessa o negata)
• risultato di una operazione

Fuori dal modello AAA molti altri eventi possono essere oggetto di auditing. Può essere fatto a vari livelli:

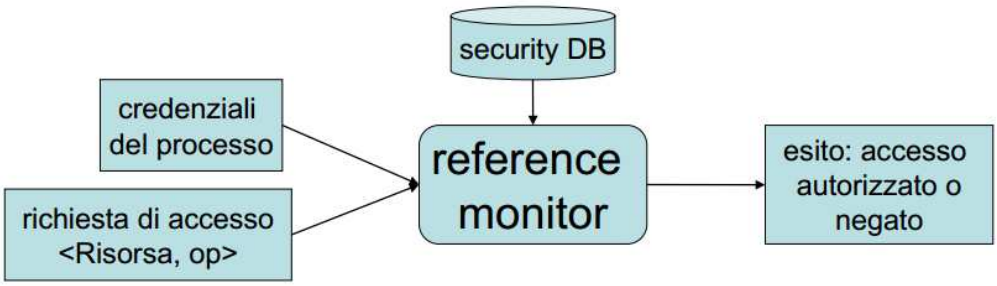
- access auditing
- log auditing
- system security auditing
- network security auditing
- auditing di procedure (iso 27001)
- auditing di competenze di persone (CISSP – SSCP e CISA – CISM)
- ecc.

Auditing = controllo o verifica di adeguatezza



Reference monitor

- parte del s.o. che effettua il controllo di accesso
- caratteristiche:
  - invocato ad ogni richiesta di accesso
  - a prova di intrusione (nessuna vulnerabilità)
  - abbastanza piccolo da essere verificabile
- introdotto nel 1972 in James Anderson
- richiesto in certe certificazioni



Reference monitor: realizzazioni

Sistemi senza reference monitor

- Windows 3.x, 95, 98, Me (controllo di accesso limitato)
- Linux <2.6 (controllo di accesso efficace ma architettura senza r.m.)

Sistemi con reference monitor

- Windows NT, 2000, XP, 2003, Vista, 7, 10
- Linux >2.6 (Linux Security Modules)

Modelli per le politiche di controllo di accesso

DAC: Discretionary (**Discrezionale**) Access Control

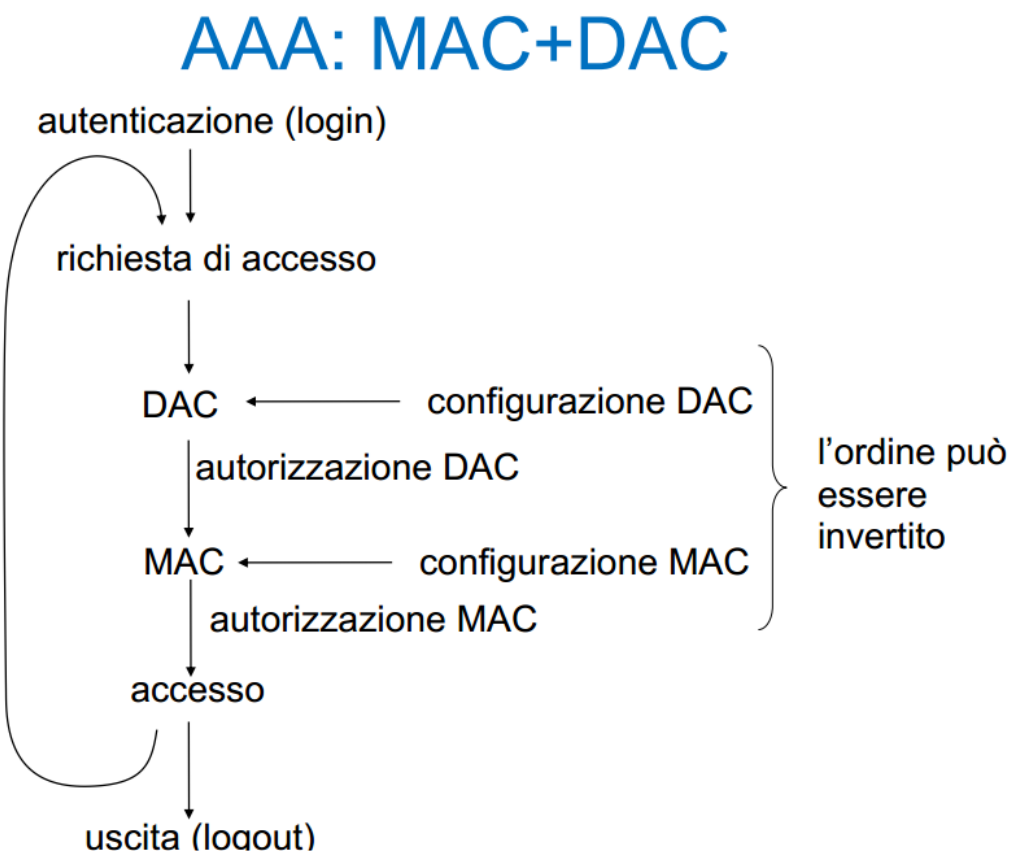
- gli utenti hanno il diritto per cambiare i diritti sulle risorse (es. il proprietario U1 di un file può dare, a sua discrezione, il diritto all'utente U2 di accedere a tale file)
- implementazioni: Linux, Windows NT/2000/XP/2003/Vista/7
- il più diffuso
- flessibile
- sicurezza delegata agli utenti (tipicamente al proprietario della risorsa)

MAC: Mandatory (**Obbligatorio**) Access Control

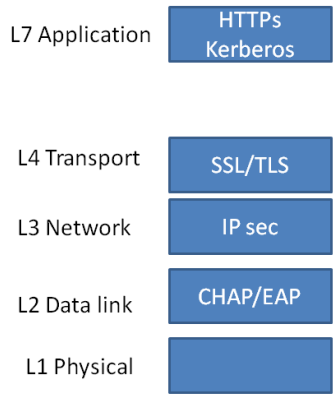
- gli utenti NON hanno il diritto di cambiare i diritti sulle risorse
- i diritti sono configurati dall'amministratore
- non è detto che l' amministratore esista
- implementazioni: Linux, Windows
- considerato il più sicuro
- molto scomodo per gli utenti (se due utenti devono scambiare un file devono chiamare l'amministratore)
- usato molto in ambito militare e sui server

MAC+DAC

- i sistemi con MAC tipicamente supportano anche DAC
- accesso consentito se sia i controlli mandatory che quelli discretionary danno autorizzazione
- permette di avere isole di discrezionalità confinati da muri obbligatori; es.
  - il web server è separato dagli utenti da una configurazione MAC
  - ma MAC non isola gli utenti tra di loro, essi sono eventualmente isolati mediante DAC



Livelli ISO/OSI e sicurezza



- Ai livelli più bassi del protocollo ISO/OSI i meccanismi di sicurezza garantiscono le tre **AAA**
  - Autenticazione
  - Autorità
  - Auditing - Accounting
- Le tre AAA vengono verificate a **livello due ISO/OSI** dove si ha l'accesso diretto al canale
- Ai **livelli superiori** bisogna garantire la **segretezza dei dati**

CHAP/EAP (Challenge-Handshake Authentication Protocol)

(Sottoprotocollo di PPP)

- È usato nelle connessioni punto punto per esempio nelle connessioni per i sottoscrittori di contratti
- Un host richiede l'accesso alla rete pubblica connettendosi ad un ISP
- I processi e i dispositivi che concedono l'accesso alla rete sono detti **NAS** (Network Access Server)
- Il protocollo CHAP viene attivato prima di uno scambio dati
- È un protocollo sfida/risposta dove il client viene autenticato dal server
  - Il client CHAP si presenta al NAS con il proprio username
  - Il NAS invia il pacchetto di challenge contente un ID e un nonce
  - Il client risponde con un pacchetto ed un codice di Hash
  - Il NAS calcola il suo codice di Hash sulla base dei dati ricevuti e lo confronta con l'Hash del client
  - Si può avere successo o fallimento

IPsec (IP security)

- Insieme di protocolli che garantiscono il RID (Riservatezza Integrità Disponibilità)
- Garantisce la comunicazione sicura end-to-end
- Ipsec è completamente trasparente alle applicazioni
- Una volta installato e avviato su un sistema, le applicazioni non si accorgono che Ipsec agisce

SSL/TLS (Secure Socket Layer / Transport Layer Security)

- Ha lo scopo di garantire l'autenticazione, la riservatezza e l'integrità dei dati inviati da una applicazione
- Agisce sia con chiave simmetrica che asimmetrica
- TLS è un insieme di protocolli che si collocano tra il livello 4 e il livello 7
- TLS agisce sulla porta TCP con la quale si sta lavorando
- I sottoprotocolli fondamentali di TLS sono:
    - Handashake – opera a livello 7 preliminare, negozia i parametri della sicurezza e li stabilisce
    - Record – opera a livello 4, crea pacchetti dati dell'applicazione con cifratura simmetrica e ne garantisce l' integrità
- TLS è trasparente alle applicazioni
- La fase di Handshake è la più critica; gli interlocutori devono autenticarsi tramite chiavi asimmetriche. Al termine dell'handshake si crea una connessione definitiva; si possono aprire successivamente più sessioni senza negoziare da capo

https (Hyper Text Transfer Protocol over Secure Socket Layer)

- Seleziona l'uso di TLS se il protocollo è HTTPS
- Scatta il TLS handshake

RADIUS (Remote Authentication Dial In User Service)

- In molti casi gli apparati NAS si trovano ad autenticare dei grandi archivi
- È spesso necessario delegare l'autenticazione a un server fidato che opera come centro di distribuzione delle chiavi **KDC** (Key Distribution Center)
- Il protocollo RADIUS è uno dei più diffusi per l'autenticazione basato su un account con centro di distribuzione delle chiavi
- RADIUS è un protocollo client/server di livello 7 trasportato da UDP sulle porte 1812 e 1823

Kerberos

- Protocollo basato su un centro di distribuzione delle chiavi, è un applicativo del livello 7
- Utilizza crittografia simmetrica con lo schema sfida/risposta
    - La novità di kerberos è l'introduzione di un AS (Authenticator System)
    - L'host richiedente si accredita presso l'AS che di dà gli strumenti per autenticarsi presso il **TGS** (Ticket Granted Service)
    - Il TGS restituisce un ticket per accreditarsi verso l'interlocutore