Sguardo d'insieme

Silvia Arezzini

Programma *Prima parte*

- AAA

  Autenticazione Autorizzazione Accounting

- Sistemi di Autenticazione

- Storia di Kerberos e sue implementazioni

Perche' AAA

Che legami ci sono tra queste 3 A e…

KERBEROS?

Il legame e' il numero 3

3 teste CERBERO il cane guardiano degli inferi e…

3 A

AAA

Cosa si intende per :

- Autenticazione

  PROCESSO DI VERIFICA DELL' IDENTITA'

- Autorizzazione

  PROCESSO DI VERIFICA DELL' AMMISSIBILITA' DELLE ATTIVITA' RICHIESTE DA PARTE DI UN SOGGETTO GIA' AUTENTICATO

- Accounting

  PROCESSO DI CORRELAZIONE TRA LE ATTIVITA' ESEGUITE SU UN OGGETTO ED IL SOGGETTO CHE LE HA INVOCATE

AUTENTICAZIONE

PROCESSO DI VERIFICA DELL' IDENTITA'

In italiano in effetti sarebbe più giusto parlare di IDENTIFICAZIONE ma è invalso l'uso del termine autenticazione per l'assonanza con il termine inglese "authentication"

In cosa consiste?

Una caratteristica (fisica o in generale personale) o qualcosa di posseduto o qualcosa di conosciuto. O una combinazione di queste caratteristiche.

Diversi tipi di autenticazione:

Quella tipica di cui parleremo spesso è: User to host

(Ma non dimentichiamo le altre: Host to host / User to user)

Perche' non vanno dimenticate…

- Host to user
  - serve per identificare con certezza un server web
    (ad esempio quello della propria banca …)

Autenticazione USER to HOST

- Cosa significa?

  Un utente si fa identificare dal sistema per accedere alle informazioni in esso contenute.

  Quali informazioni?

  Quelle che e' AUTORIZZATO a conoscere

AUTORIZZAZIONE

- ***Processo di verifica dell'ammissibilita' delle attivita' richieste da parte di un soggetto gia' autenticato***

- Processo che permette di controllare che l'accesso alle risorse venga garantito solo a coloro che hanno delle predeterminate caratteristiche

In altre parole:

- Il sistema di autorizzazione individua quali attività può svolgere e a quali risorse ha diritto di accedere, uno USER già correttamente identificato.

Autorizzazione

- Autorizzazione

  Molto piu' legata al servizio che si sta erogando
- Puo' esserci autenticazione centralizzata, ma autorizzazione diversificata a seconda del servizio che si sta accedendo.
- File systems distribuiti tipo NIS:

  anche autorizzazione

Autorizzazione

- Autorizzazione UNIX
- USERID e GID e risorse assegnate in base al gruppo
- ACL nei file systems di rete NFS e AFS ad esempio

Con riferimento ad un unico punto di autenticazione si assegnano permessi sulle risorse, cioe' si autorizzano categorie di utenti a disporre delle risorse stesse.

ACCOUNTING

- ***Processo di correlazione tra le attivita' eseguite su un oggetto ed il soggetto che le ha invocate***

- **meccanismo con cui si tiene traccia delle azioni svolte e delle risorse utilizzate da ciascun soggetto autorizzato.**

- **Registrazione di eventi relativi ad autenticazioni ed autorizzazioni**

AAA

- 3 caratteristiche volte nella stessa direzione:

  PROTEGGERE UN SISTEMA

Proteggere un sistema

Salvaguardare:

- INTEGRITA’
- RISERVATEZZA
- DISPONIBILITA’

Dei dati presenti in un sistema

INTEGRITA'

- Protezione dei dati dalla alterazione o modifica non autorizzata

  - E anche qualcosa di piu'…

    Impedire che possano avvenire cancellazioni o modifiche a causa di interventi non autorizzati o a causa di eventi non facilmente controllabili (incendi, allagamenti…)

RISERVATEZZA

- Impedire che qualcuno possa volontariamente o involontariamente accedere all'informazione senza essere autorizzato

DISPONIBILITA’

- Far si’ che non venga impedito l’accesso all’informazione a chi ne ha invece l’autorizzazione

Un meccanismo "serio" AAA

- Dovrebbe garantire i dati.
- Le prime due A (Autenticazione e Autorizzazione) sono fondamentali
- Talvolta si genera confusione fra Autenticazione e Autorizzazione

- Attenzione…

Da ora in poi parleremo di *AUTENTICAZIONE*

Concentriamoci sulla autenticazione...

USER che si identifica per farsi riconoscere da un HOST

Come?

- Con qualcosa che è
- Con qualcosa che possiede
- *Con qualcosa che conosce…*

Essere autenticato significa disporre di valide credenziali

Qualcosa che si conosce… 1

- Ad esempio username e password
  - Il metodo più conosciuto… e pericoloso
    - Sniffing se trasmesse in chiaro
    - Attacchi tramite dizionario
    - Disattenzioni (annotare la password)
- PASSWORD USA e GETTA (ONE TIME PASSWORD)
    - Valida per un unico accesso. Se intercettata è inutile non si può riusare
    - Necessità di possedere un dispositivo di generazione… che può essere rubato…

Qualcosa che si conosce… 2

- Sistemi a SFIDA (Challenge-Response)

  Anche qui c'e' una password

  La password pero' non viene inviata sulla rete, ma viene usata per effettuare un calcolo che ne dimostra la conoscenza

Sistemi a sfida

Il sistema trasmette all'utente un numero casuale (sfida)

L'utente immette la password, ma la risposta che viene trasmessa è il risultato di un calcolo effettuato sulla sfida e sulla password:

F(sfida, password)

Se F è di tipo asimmetrico un attaccante non può risalire alla password e quindi non può calcolare le risposte alle nuove sfide

Se la sfida non viene mai ripetuta, un attaccante non può riutilizzare le risposte alle vecchie sfide

Chiavi simmetriche e asimmetriche

- SIMMETRICA
  - esistenza di un'unica chiave utilizzata per codificare il testo in chiaro e per decodificare quello cifrato.
- ASIMMETRICA
  - la chiave usata per cifrare e decifrare non e' la stessa. Infatti una e' utilizzata solo per cifrare(in genere la chiave pubblica) e l'altra solo per decifrare(in genere la chiave privata). Di conseguenza le due chiavi devono essere fortemente connesse tra di loro. La chiave pubblica, come dice il nome, deve esser resa pubblica a tutte le persone che vogliono parlare con me in maniera sicura. La chiave privata è solamente mia e va accuratamente protetta.

Qualcosa che si conosce… 3

- Sistemi di autenticazione a terzo fidato

La password non viene usata per accedere direttamente alle applicazioni ma per ottenere un lasciapassare (ticket) generato dal sistema centrale di autenticazione ed accettato dalle applicazioni

Consentono di centralizzare la gestione dei diritti di accesso alle diverse applicazioni

Sistemi di autenticazione

- PAP

(Password Authentication Protocol)

Passano in chiaro sulla rete username e password

- CHAP & MS-CHAP

(Challenge-Handshake Authentication Protocol)

Il client invia lo username e il server risponde con un “challenge”

Il client esegue l’hash del challenge assieme alla password e lo reinvia al server

Il server, che conosce la password, esegue lo stesso calcolo e compara i due valori verificando la correttezza.

Ad intervalli casuali viene riproposto dal server un challenge al client

- Kerberos

Un esempio di autenticazione con terzo fidato

Sistemi di autenticazione

Non solo password… Anche certificati

(qualcosa che si possiede)

- PKI (Public Key Infrastructure)

  Prevede l'utilizzo di certificati contenenti la chiave pubblica ed informazioni relative all'utente.

  I certificati vengono rilasciati dalla

  Certification Authority (CA)

- Interrelazioni e collegamenti fra sistemi diversi

Kerberos

- Nasce al MIT negli anni ’80 nel momento di passaggio dall’ uso di terminali di un mainframe all’ uso di workstation.

(Progetto Athena)

Vedi parte successiva…

Kerberos

- Prevede per ogni sistema di gestione delle utenze (realm)
  - un server di autenticazione centralizzato
  - un server per la gestione dei ticket
- E' possibile configurare realm diversi in modo che l'utente di un sistema possa chiedere servizi ai server di un altro sistema
- Utilizza metodi di crittografia simmetrica
- Due versioni, 4 e 5

Kerberos

- Password in chiaro solo nel client e per il minimo tempo possibile
- Autenticazione che vale per una sola sessione

Perché KERBEROS

- Perchè permette autenticazione in sistemi distribuiti
  - Con risorse eterogenee (sistemi,servizi server, applicazioni DBMS)
  - sistemi di tipo diverso (Unix, Windows ecc…)
  - sistemi logicamente e fisicamente separati

- Perchè permette di amministrare centralmente l'autenticazione mediante uno o più

  Authentication Services/Servers

Per capirne di piu'….

- Kerberos risponde a questa esigenza:

  Fare in modo che i server di un sistema distribuito, aperto, con utenti e workstation siano in grado di limitare l'accesso alle utenze autorizzate e possano autenticare le richieste di servizi.

  Autenticazione e Autorizzazione…

Kerberos risponde a requisti di:

Sicurezza

- un'operazione di intercettazione della rete non permette di ottenere le informazioni necessarie per sostituire un utente

Affidabilita'

- Per tutti i servizi che si affidano a kerberos la mancanza di kerberos significa negazione del servizio. Quindi i server di kerberos sono replicati in modo tale che ognuno dei sistemi sia in grado di supplire alla mancanza di un altro (master e slave)

Trasparenza

- Gli utenti non sanno che c'e' kerberos, immettono solo una password come in un sistema tradizionale

Scalabilita'

- Il sistema e' in grado di supportare un gran numero di client e server. L'architettura e' modulare e distribuita

Come funziona?
Spiegazione naif… seguiranno i complicati dettagli

- Kerberos 4
  - L'utente scrive username
  - Il client kerberos invia un messaggio all'Authentication Server di kerberos segnalandogli che un certo username sta cercando di registrarsi.
  - Il server kerberos controlla il proprio DataBase e se lo username e' autorizzato invia un Ticket Granting Ticket codificato con la password dell'utente in questione.
  - Il client su cui l'utente sta facendo login a questo punto chiede allo user di digitare la password e prova a decodificare il ticket codificato che ha ricevuto dal server.
  - Se la decodifica ha successo la workstation client dimentica la password e inizia ad utilizzare il Ticket.

. . . .

- Kerberos 5
  - L'utente scrive username e password
  - Il client kerberos invia un messaggio all'Authentication Server di kerberos. Il messaggio contiene lo username e l'ora corrente codificata con la password
  - L' authentication server controlla lo username, determina la password e decodifica l'ora codificata.
  - Se il server decodifica l'ora corrente allora crea un Ticket granting ticket che codifica con la password e lo invia al client che lo fornisce all'utente.

In realta'…

- La procedura e' un po' piu'complicata e la vedremo nel dettaglio in seguito.

- Questa prima idea del funzionamento deve servirci per capire i termini della questione, poi approfondiremo.

Da kerberos 4 a kerberos 5

- La 4 richiede DES (problemi non solo sulla sicurezza , ma a suo tempo anche per l'esportabilita')
- Nella 4 si richiede l'impiego solo di indirizzi IP. La 5 e' multiprotocollo.
- Durata dei ticket
- Difficolta' nel gestire autenticazione fra diversi realm.

PASSWORD e kerberos

- Versione 4: mantenere la password nel client il minor tempo possibile

  Vulnerabilita' ad attacchi che indovinano offline la password. Un aggressore potrebbe farsi dare un TGT e poi cercare di decifrarlo con un dizionario
- Versione 5: la workstation deve dimostrare al KDC che l'utente conosce la password corretta.

  Il TGT codificato potrebbe essere intercettato da un aggressore mentre viene inviato dal server alla workstation e attaccato con una ricerca della chiave…

La scelta della PASSWORD!

I limiti di kerberos

- Servizi kerberizzati
- Sicurezza del server.

  Se il server e' compromesso TUTTI devono cambiare le password.
- Server sempre disponibile

Un attimo di respiro...

- Fine prima parte

Programma *Seconda parte*

- Introduzione al concetto di Directory Server
- LDAP

Cosa e' un Directory Server

- Un **Directory Server**
  è un programma (o un insieme di programmi) che, provvedendo ad organizzare e memorizzare informazioni su risorse condivise disponibili in rete, offre un SERVIZIO appunto di INFORMAZIONI

- Un **Directory Server**
  fornisce, di fatto, uno strato di astrazione tra le risorse di una struttura e gli utenti.

Il termine **directory** richiama direttamente alla ordinata struttura dei dati dove viene immagazzinata l'informazione.

DIRECTORY

- Ma cosa e' una "Una Directory"?
  - è una lista di informazioni relative ad oggetti, ordinate in qualche modo, e tali da fornire dettagli relativi agli oggetti cui si riferiscono.

- Uno degli esempi usati comunemente, è l'elenco telefonico, ma non è ovviamente il solo (Mall Directory, Museum Directory, Cataloghi, Guide dei programmi TV, …)
  - Nell'elenco telefonico, gli oggetti sono gli intestatari di un contratto telefonico (con un qualche provider); i loro nomi sono ordinati in ordine alfabetico; le informazioni relative agli oggetti, sono il numero telefonico, l'indirizzo, ...

Piu' in dettaglio…

- Una DIRECTORY che contiene informazioni "stampate" su un qualche tipo di supporto, e' "statica".
- Nel mondo dei sistemi di calcolo e delle reti, la Directory contiene informazioni accessibili on-line.

  E' quindi di solito "dinamica", "flessibile", puo' essere "personalizzata" e resa "sicura".

Esempi di DIRECTORY

- Directory legate ad applicazioni specifiche, come il file aliases di sendmail
- Directory legate a Sistemi Operativi di Rete come NIS
- Directory legate ad uno specifico scopo (e quindi non estensibili) come il DNS
- Directory generiche e basate su standard, come la directory X.500 e LDAP

Directory Services

- Chiarito cosa e’ una DIRECTORY vediamo ora cosa intendiamo per Directory Service:
  - L’insieme di software, hardware, processi, politiche, procedure amministrative necessari per fare in modo che le informazioni contenute nella Directory siano accessibili agli utenti della Directory.

Terminologia

- Capita spesso di usare il termine DIRECTORY al posto del piu' corretto DIRECTORY SERVICES
  - Si e' cioe' portati a identificare la struttura con i servizi offerti
  - Attenzione quindi. In questo ambito e' essenziale pensare a un complesso e sofisticato sistema formato da numerose parti che interagiscono fra loro. Non dimentichiamolo…

Sistema complesso formato da:…

- Le informazioni contenute nella Directory
- Il software del server che contiene tali informazioni e che ne permette l'accesso
- Il software dei client per l'accesso alla Directory
- L'hardware, i sistemi operativi e l'infrastruttura di rete
- Le politiche che definiscono chi può accedere, ed aggiornare le informazioni memorizzate, il tipo di informazioni, …
- Le procedure di mantenimento e monitoraggio della Directory
- Il software per il monitoraggio del Directory Service

Directory Server e DataBase

Un Directory Server

è spesso considerato un database.

Lo è ma di un tipo molto particolare:

è un database specializzato, con caratteristiche assai differenti dai tradizionali database relazionali.

- Accessi quasi esclusivamente in lettura
- scrittura limitata agli amministratori di sistema o ai proprietari delle singole informazioni.

I Directory Server sono ottimizzati per la lettura, quindi, di fatto, non sono adatti per immagazzinare informazioni aggiornate di frequente.

Piu' in dettaglio…

- I DataBase general-purpose sono pensati per applicazioni "write-intensive".
- Una Directory si usa invece quando si ha a che fare con dati che sono letti molto più spesso di quanto sono scritti o aggiornati.
- Il fatto che una Directory sia ottimizzata per applicazioni "read-intensive" ha implicazioni su altre caratteristiche della Directory (come la replicabilità)

5 parole chiave

- *Schema*
- *Distribuzione*
- *Repliche*
- *Prestazioni*
- *Transazioni*

Schema

- In una Directory o in un DataBase, lo “schema” è un insieme di regole che definiscono il tipo di informazioni, le regole che tali informazioni devono osservare ed il modo con cui tali informazioni si comportano.
- Lo Schema può essere esteso in funzione delle necessità delle applicazioni che usano la Directory.
- In una Directory è infatti possibile aggiungere attributi nuovi agli oggetti esistenti, senza dover toccare le informazioni già esistenti, anche nel caso si stia aggiungendo una primitiva.

Distribuzione dei dati

- I dati contenuti in una Directory, possono risiedere fisicamente su di un singolo server ovvero essere distribuiti su più server.
- In una Directory la distribuibilità dei dati è un fattore fondamentale nel disegno della Directory stessa.

Repliche

- Avere molte copie dei dati in posti differenti aumenta l'affidabilità, la disponibilità e la prestazione di una Directory.
- Le Directory non ha una stringente richiesta di consistenza dei dati, che possono temporaneamente essere disallineati nelle varie repliche. Questo permette di ottenere prestazioni elevatissime ed alta disponibilita' (al limite una directory può essere replicata in ogni client...)

Legami tra distribuzione e repliche

- Quando una directory è distribuita, le informazioni contenute possono essere partizionate e replicate insieme.
- La distribuzione dei directory server e la modalità in cui i dati sono partizionati e/o replicati determina il livello di prestazione e di disponibilità della directory.

Prestazioni

- Una Directory può dover gestire migliaia o decine di migliaia di richieste al secondo.
  - ogni singola operazione di lettura da una Directory è molto più semplice rispetto ad una transazione gestita da un DataBase
- Il rapporto tra lettura e scrittura di dati in una Directory è molto alto, ma questo non vuol dire che possiamo dimenticarci delle prestazioni in scrittura
  - Una frequenza di aggiornamento di 1 volta al mese, significa avere una media di circa 1500 aggiornamenti all'ora per una Directory da 1 milione di entries

Transazioni

- La Directory riesce a gestire solo un semplice modello di transazione che coinvolge solo una singola operazione su un singolo elemento

Per non dimenticare…
Caratteristiche di una Directory

- *Schema*
- *Distribuzione*
- *Repliche*
- *Prestazioni*
- *Transazioni*

Differenze tra Directory e Data Base 1

- In un DataBase la variazione dello schema non è in generale una operazione semplice. Non è sempre possibile aggiungere “al volo” un nuovo campo in un record
- Per un DataBase la distribuibilita’ dei dati è una caratteristica “addizionale”, non sempre disponibile ed in ogni caso con limitazioni sulla scala di distribuibilità (pochi servers).

Differenze tra Directory e Data Base 2

- I DataBase possono avere funzionalità di replica, ma a causa della forte richiesta di consistenza tra le repliche, questo tipicamente porta ad una riduzione delle prestazioni.

- Le prestazioni di un DataBase si misurano in numero di transazioni al secondo. Un Data Base può gestire centinaia di transazioni al secondo.

Differenze tra Directory e Data Base 3

- I DataBase hanno la capacità di gestire transazioni complesse, che coinvolgono molti record, e che richiedono anche molte operazioni. Per garantire che la transazione sia completamente eseguita, sono in grado di “tornare indietro” (rollback) nel caso in cui l’operazione non vada completamente a buon fine.

Perche' usare una Directory

- **Fondamentalmente perche' riduce la necessita' di pensare a directory specifiche per ogni singola applicazione.**

  L'esistenza di un servizio (contenitore) delle informazioni principali permette agli sviluppatori di non doversi preoccupare della fonte delle informazioni

Client/server

- L'accesso al Directory Server utilizza il modello di comunicazione client/server.

- Un'applicazione che vuole leggere informazioni da una Directory non vi accede direttamente, ma invoca una funzione o un'interfaccia che genera l'invio di un messaggio ad un altro processo.
- Questo secondo processo accede alle informazioni della directory per conto dell'applicazione che ne ha fatto richiesta. Il risultato dell'operazione di lettura o di scrittura è restituito quindi all'applicazione.
- Il formato e il contenuto dei messaggi scambiati tra client e server deve rispettare un protocollo concordato, ad esempio LDAP.

LDAP Lightweight Directory Access Protocol

- LDAP definisce il protocollo con cui vengono scambiati i messaggi tra client e Directory Server
- Nel protocollo LDAP sono definiti messaggi di tipo diverso
  - All'inizio di una connessione il client invia un messaggio di tipo bindRequest
  - Un messaggio di tipo searchRequest serve per effettuare una ricerca all'interno della Directory
- LDAP non definisce un Directory Service, ma viene usato comunemente per indicare un Directory Service interrogabile via protocollo LDAP

Chi definisce un Directory Service?

OSI Open Systems Interconnect

- Il Modello di Riferimento OSI (ISO 7498) definisce un modello a sette strati per la comunicazione dei dati. Dal livello fisico (primo livello) al livello applicativo (settimo livello)
- L'implementazione di tale modello, non ha avuto un grande successo
- Tuttavia nel protocollo OSI sono state affrontate un certo numero di problematiche molto importanti nell'ambito di sistemi distribuiti.
- Una di queste è quella dei Directory Services

X.500 Directory Server

- Nel 1988 il CCITT (Comite Consultatif International Telephonique et Telegraphique) definisce lo standard X.500 che diventerà ISO 9594, Data Communications Network Directory, Recommendations X.500-X.521 nel 1990, ma che viene ancora comunemente chiamato semplicemente X.500
- X.500 organizza il contenuto delle Directory in modo gerarchico
- X.500 definisce anche il protocollo di comunicazione tra il client ed il Directory Server.
- DAP Directory Access Protocol

DAP ed ISO-OSI

- Purtroppo gli standard ISO non prevedono meccanismi di comunicazione non standard e quindi per poter usare DAP era necessaria una rete che funzionasse con il protocollo OSI
- Dopo il fallimento delle prime implementazioni di OSI, l'unico modo per poter usare il buono di X.500 e' stato quello di "alleggerire" il protocollo di accesso
- La prima versione di tale protocollo di accesso "alleggerito" è descritta dall' RFC 1487 X.500 Lightweight Access Protocol
- Questo RFC è stato reso obsoleto dall'RFC 1777 Lightweight Directory Access Protocol