Controllo di accesso a risorse condivise

Lezione 15 di Sicurezza dei sistemi informatici 1

Docente: Giuseppe Scollo

Università di Catania, sede di Comiso (RG)
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Studi in Informatica applicata, AA 2006-7

Indice

controllo di accesso e autorizzazione

autorizzazione, controllo di accesso, autenticazione: **non** sono sinonimi

- autorizzazione: **definizione** e **conferimento** di diritti di accesso
- controllo di accesso: meccanismo operativo per l'**esercizio** di diritti di accesso
- autenticazione: accertamento di veridicità dell'**identità** conclamata da un soggetto

più precisamente, nel **controllo di accesso:**

- si accerta che **ogni** richiesta di accesso goda della relativa autorizzazione
- dunque si garantisce l'esercizio di diritti di accesso **solo** a chi li gode
- a tal fine **può** essere necessaria l'autenticazione, però ...
- ... è saggio evitarne la reiterazione, per uno stesso soggetto, ad ogni sua richiesta di accesso durante una sessione di lavoro, per non compromettere le prestazioni del sistema (misurate dal tempo di risposta)

nel seguito ci occupiamo di **autorizzazione**

modelli di autorizzazione

modello di autorizzazione:

- sistema di **concetti** relativi a definizione e conferimento di diritti di accesso

un'autorizzazione di accesso coinvolge tre entità:

- **soggetto** della richiesta
- **oggetto** dell'accesso
- **operazione** sull'oggetto richiesta dal soggetto

rappresentazione elementare della **definizione** di autorizzazioni: **matrice di Lampson**

rappresentazioni ridotte (proiezioni della matrice di Lampson):

- **per soggetto: lista delle capacità**, ingl. capabilities, su ogni oggetto
- **per oggetto: lista di controllo di accesso**, ingl. Access Control List (ACL), da parte di ogni soggetto
  - di uso più frequente, ma in forme più pratiche, che esaminiamo appresso

tipi di diritti di accesso e ruoli

astrazioni insiemistiche connaturate all'autorizzazione:

- **classe** di oggetti: un insieme di oggetti sui quali sono definite le stesse operazioni
- **tipo di diritti di accesso:** un **nome univoco** di un sottoinsieme delle operazioni di una **classe**
- **ruolo:** un **nome univoco** di un sottoinsieme delle operazioni su un **oggetto**

ambito di univocità dei nomi:

- locale a ciascuna **classe** per i **tipi di diritti di accesso**
- locale a ciascun **oggetto** per i **ruoli**

cioè:

- un ruolo può avere definizioni diverse per oggetti distinti, pur se della stessa classe
- un tipo di diritti di accesso può avere definizioni diverse solo per classi diverse di oggetti

queste astrazioni hanno vantaggi pratici:

- definire la ACL di un oggetto in termini di assegnazione di ruoli ai soggetti
- ridefinire i ruoli per un oggetto in termini di tipi di diritti di accesso
- conferire diritti di accesso ai soggetti operando sulle ACL **degli oggetti**, dunque con notevole guadagno in flessibilità rispetto a una più tradizionale definizione di ruolo quale gruppo di utenti (che è implicitamente determinato dall'assegnazione di ruoli in una ACL, ma è dunque **locale all'oggetto**)

autorizzazione e raggruppamento

la doppia stratificazione dei diritti di accesso in **tipi** e **ruoli** semplifica la gestione dell'autorizzazione in presenza di oggetti **contenitori**, quali ad es. le directory in un filesystem o gli spazi di lavoro in un sistema di collaborazione (l'acronimo sta per Computer Supported Collaborative Work), in quanto

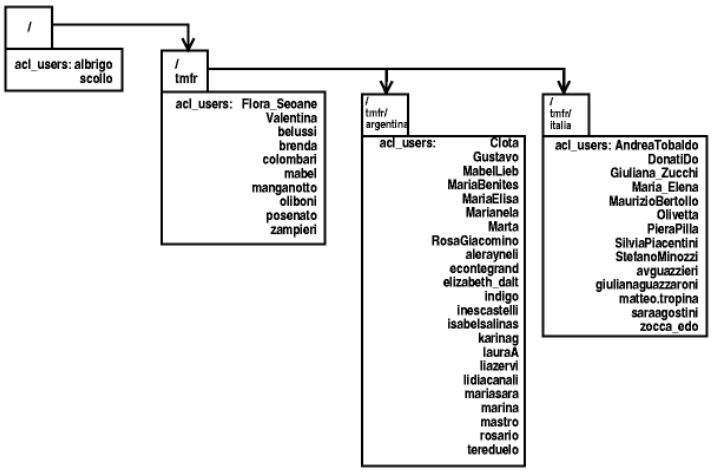
- si possono "mascherare" differenze fra classi (in termini di operazioni definite) ridefinendo opportunamente gli stessi tipi di diritti di accesso
- definire gli stessi tipi anche per le classi di contenitori
- definire i ruoli per gli oggetti in termini di tipi di diritti di accesso
- sfruttare l'**ereditarietà di default** dei ruoli fra oggetti contenitori e quelli in essi contenuti, sì che alla creazione di un nuovo oggetto (in un contenitore) non sia necessario definire la sua ACL esplicitamente, ma solo qualora si vogliano ridefinire i ruoli, o le loro assegnazioni ai soggetti, per quell'oggetto

oltre che soggetti individuali, è comunque utile definire **gruppi di utenti** come soggetti, ad es. per la **condivisione** di contenitori quali spazi di lavoro, di discussione, etc.

vediamo appresso due esempi di sistemi di supporto alla collaborazione in rete, con due diversi modelli di autorizzazione, entrambi basati su ACL e raggruppamento

autorizzazione di gruppi in *Zope*

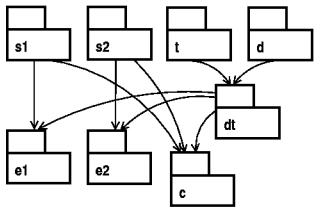
Zope è una piattaforma open source per lo sviluppo di siti e applicazioni Web



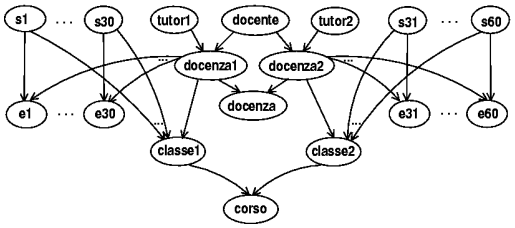
struttura ad albero degli spazi Zope per un corso in rete

autorizzazione nel sistema BSCW

l'acronimo sta per Basic Support for Coooperative Work: è un prodotto commerciale
DAG: Directed Acyclic Graph, radicato negli spazi personali degli utenti



esempio di struttura DAG di spazi BSCW



DAG di gruppi BSCW per un corso in rete con due classi

la negazione in modelli di autorizzazione

se un soggetto accede ad un oggetto con un solo ruolo, la definizione di quest'ultimo per l'oggetto in questione specifica i diritti di accesso del soggetto all'oggetto

ma quando, come accade ad esempio in DAG di oggetti e contenitori con eredità di ruoli, un soggetto può accedere a un oggetto con **più ruoli**, come determinano questi i diritti di accesso del soggetto all'oggetto?

nei modelli di autorizzazione **disgiuntiva**: un diritto di accesso è goduto sse è attribuito da **almeno uno** dei ruoli assegnati al soggetto

nei modelli di autorizzazione **congiuntiva**: un diritto di accesso è goduto sse è attribuito da **tutti** i ruoli assegnati al soggetto

sono di uso più pratico **modelli misti**, in cui una delle due suddette politiche costituisce il default, ma è possibile modificarne l'effetto quando occorre

ad es., il concetto di **diritto di accesso negativo** è un antidoto al potenziale eccesso di liberalità dell'autorizzazione disgiuntiva: si può interpretare l'attribuzione di un diritto di accesso con segno negativo come la **negazione** di tal diritto, quando si assegna il ruolo che lo contiene, indipendentemente dall'attribuzione (positiva) dello stesso diritto in altri ruoli

autorizzazione e delega

definizione di ruoli e ACL sono proprietà di oggetti: se sono considerate (come è ben lecito, in linea di principio) come oggetti esse stesse, avranno una propria ACL e definizione di ruoli... il qual fatto genera una catena infinita (di dubbia utilità) di metalivelli di autorizzazione

si può arrestare la catena al secondo livello semplicemente distinguendo fra:

oggetti **regolari**: dotati di ACL e di definizione di ruoli

oggetti **attributi** di oggetti regolari: non dotati di ACL e definizione di ruoli

e considerando le operazioni sui secondi come operazioni sull'oggetto regolare di cui sono attributi, dunque autorizzate mediante la definizione di ruoli e ACL di quest'ultimo

l'autorizzazione all'autorizzazione è un caso rilevante del concetto di **delega**: diritto, assegnabile a soggetti, di assegnazione di dati (tipi di) diritti ad altri soggetti

la delega può essere **ricorsiva** (delega alla delega): si può realizzarla semplicemente includendo il diritto all'assegnazione di ruoli a soggetti fra i diritti conferiti mediante l'assegnazione di un ruolo

riferimenti

BSCW, Basic Support for Cooperative Work
http://www.bscw.de/english/

Zope.org, The Web Site for the Zope Community
http://zope.org

Zope Italia, Community Italiana dell'application server Zope
http://zope.it

Scollo (2002) :

Modelli di autorizzazione negli ambienti di collaborazione

estratto da: Progettazione di siti Web per la formazione in rete, Cap. 2

Corso Master in Tecnologie e Metodologie per la Formazione in Rete
Università di Verona, Dipartimento di Informatica