Modelli di sicurezza

Lezione 18 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

modelli reticolari per la riservatezza

il modello di **Bell & La Padula** (1973) formalizza la già vista politica di sicurezza militare, basata sulla classificazione delle informazioni e sulla relazione di **dominanza** $\leq$ fra soggetti e oggetti: questa forma un reticolo sull'insieme di rispettivi svincoli e classificazioni, dette **classi di protezione C(s), C(o)**, rispettivamente per il soggetto **s** e per l'oggetto **o**

> obiettivo della protezione di Bell & La Padula è la **riservatezza** dell'informazione

a questo riguardo, il flusso sicuro delle informazioni è caratterizzato da due proprietà:

proprietà della protezione semplice

> un soggetto **s** può avere accesso **in lettura** a un oggetto **o** solo se $C(o) \leq C(s)$

proprietà *

> se un soggetto **s** ha accesso **in lettura** a un oggetto **o**,
> allora **s** può avere accesso **in scrittura** a un oggetto **p** solo se $C(o) \leq C(p)$

la seconda proprietà può lasciare perplessi, perché può permettere a un soggetto l'accesso in scrittura ad un oggetto al quale lo stesso soggetto non abbia accesso in lettura

> il modello di Bell & La Padula protegge **solo** la riservatezza dell'informazione, "scrittura" è intesa come possibilità di **divulgazione**

modelli reticolari per l'integrità

il modello di **Biba** (1977) è la controparte del modello di Bell & La Padula riguardo alla protezione dell'**integrità** dei dati

> alle classi di protezione (della riservatezza) del modello di Bell & La Padula fanno da controparte nel modello di Biba le **classi di integrità I(s), I(o)**

la protezione dell'integrità in questo modello è caratterizzata da due proprietà:

proprietà dell'integrità semplice

> un soggetto **s** può avere accesso **in scrittura** a un oggetto **o** solo se $I(s) \geq I(o)$

proprietà * dell'integrità

> se un soggetto **s** ha accesso **in lettura** a un oggetto **o**,
> allora **s** può avere accesso **in scrittura** a un oggetto **p** solo se $I(o) \geq I(p)$

nel modello di Biba, "scrittura" è intesa come possibilità di **modifica** dell'informazione

> ciascuno dei due modelli reticolari visti protegge uno solo di due aspetti della sicurezza, entrambi fondamentali ... allo stato attuale, nessun modello formale di largo impiego li copre entrambi in misura soddisfacente

modelli di sistemi di protezione

a differenza dei semplici modelli reticolari di sicurezza visti sopra, modelli più complessi sono generalmente basati su un **sistema formale di regole di protezione**, definite in termini di

- **soggetti**
- **oggetti**
- **diritti di accesso**
- **controllo degli accessi**

modelli di sistemi di protezione così concepiti possono esser utilmente impiegati per

- lo studio di **fattibilità** di politiche di sicurezza, prima di intraprenderne l'implementazione
- valutazioni preliminari dell'**efficacia** di politiche di sicurezza
- analisi dell'**impatto** di una politica di sicurezza, o di scelte alternative in proposito, sulle **prestazioni** del sistema

modello di Graham & Denning

il modello di sistema di protezione di **Graham & Denning** (1972) consta di

- un insieme S di **soggetti**
- un insieme O di **oggetti**
- un insieme R di **diritti di accesso**
- una **matrice A di controllo degli accessi** di soggetti a oggetti o ad altri soggetti

il modello prevede inoltre **otto operazioni**, eseguibili da soggetti su oggetti o altri soggetti in base a **condizioni** specifiche, il cui valore dipende dai diritti specificati nella matrice A

- **crea oggetto**, **crea soggetto**
- **elimina oggetto**, **elimina soggetto**
- **leggi diritti di accesso**
- **garantisci diritto di accesso**
- **elimina diritto di accesso**
- **trasferisci diritto di accesso**

l'esecuzione di queste operazioni (eccetto la quinta) modifica la matrice A

si possono garantire o trasferire diritti di accesso **con diritto di trasferimento** o meno

modello di Harrison, Ruzzo & Ullman

una variazione del modello di Graham & Denning visto sopra è costituita dal **modello di Harrison, Ruzzo & Ullman (HRU)** (1976)

motivata dall'obiettivo di migliorare la **decidibilità** di questioni relative al possesso di specificati diritti di accesso da parte di soggetti

come il modello di Graham & Denning, il modello HRU consta di soggetti (ciascuno dei quali è anche un oggetto), oggetti, generici diritti di accesso e di una matrice di controllo degli accessi

la principale differenza sta nel fatto che un modello HRU è definito da **comandi**, della forma

comando nome(o_1, ..., o_k) **se** r_1 in $A[s_1,o_1]$, ..., r_m in $A[s_m,o_m]$ **allora** op_1, ..., op_n

dove: nelle **condizioni**: gli r_i sono diritti di accesso, A è la matrice di controllo degli accessi e op_1, ..., op_n sono **operazioni** del modello

il modello HRU prevede **sei** operazioni:

crea il soggetto **s** / l'oggetto **o**
distruggi il soggetto **s** / l'oggetto **o**
inserisci / **elimina** il diritto di accesso r in / da A[s,o]

riguardo alla decidibilità del conferimento di diritti di accesso a soggetti per oggetti specificati, è stato dimostrato che in un modello HRU tale relazione:

è decidibile se ogni comando è limitato a **una sola operazione**
altrimenti non è, in generale, decidibile

modello Take-Grant

il numero di operazioni primitive si riduce a **quattro** nel **modello Take-Grant**, di cui sono state proposte diverse varianti (1977 - 1981)

ogni operazione è eseguita da un **soggetto s**:

crea(o,r): **s** crea **o** con diritti **r** su **o**
revoca(o,r): **s** revoca i propri diritti **r** su **o**
garantisci(o,p,r): **s** garantisce a **o** i diritti **r** su **p**
prendi(o,p,r): **s** acquisisce da **o** i diritti **r** su **p**

le ultime due operazioni presuppongono la sussistenza di specifici diritti, rispettivamente:

di **garanzia di diritti** di **s** a **o** (e che **s** abbia i diritti **r** su **p**)
di **assunzione di diritti** di **s** da **o** (e che **o** abbia i diritti **r** su **p**)

il modello Take-Grant permette di rappresentare lo stato del conferimento di diritti di accesso con un **grafo**, in cui i diritti etichettano gli archi fra i vertici (soggetti e oggetti)

nei modelli Take-Grant è decidibile la **condivisibilità** fra soggetti di diritti su oggetti e, in dipendenza da questa, la possibilità di "furto" di tali diritti fra soggetti