# Requisiti di sistemi operativi sicuri

Lezione 17 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**

## progettazione di sistemi operativi sicuri

abbiamo fin qui considerato la sicurezza di un sistema operativo nella prospettiva del suo **uso**, ci mettiamo ora in quella del **progettista** di un sistema operativo che si vuole "sicuro"

> in questa e nelle successive lezioni intenderemo questo aggettivo nel senso di **degno di fiducia** (ingl. **trusted**), come si precisa più avanti

la progettazione di sistemi operativi sicuri si basa su quattro **concetti essenziali:**

**politica di sicurezza** (ingl. **policy**):
> concetti e regole generali per la specifica dei **requisiti di sicurezza** del sistema

**modello:**
> rappresentazione dell'applicazione di una politica di sicurezza a un'**astrazione del sistema**, utile ad es. per l'analisi del suo impatto sulle funzionalità e sulle prestazioni del sistema

**progetto:**
> **serie di raffinamenti** successivi del modello di sicurezza, che guidano lo sviluppo attraverso **decisioni** di progetto e **scelte** implementative, volte a soddisfare i requisiti di sicurezza

**fiducia:**
> la qualifica di sistema operativo "sicuro" poggia sull'accertamento che esso
>> abbia le **funzionalità** necessarie alla messa in opera della politica di sicurezza
>> offra **garanzia** di corretta ed efficace implementazione di tali funzionalità

## qualità di sicurezza e di fiducia

letteralmente intesa, la qualità di sicurezza è una proprietà che un sistema operativo **ha o non ha**

> così strettamente intesa, tuttavia, è una proprietà forse facile da asserire, ma ben **difficile da dimostrare** o da sottoporre a **collaudo esaustivo**

l'identificazione del significato di "sicuro" con **degno di fiducia** corrisponde alla sostituzione di una proprietà assoluta, indipendente dal contesto, e non verificabile, con una **relativa** al contesto d'uso e **verificabile** mediante analisi e collaudo

> inoltre, al carattere "manicheo" della sicurezza assoluta si contrappone il più utile carattere **graduale** del conferimento di fiducia, basato su ampiezza dei requisiti e profondità di analisi e collaudi

più che **la** qualità (assoluta) di sicurezza è utile considerare **le** qualità di sicurezza, specificate in generale dalle **politiche** e in dettaglio dai **requisiti** di sicurezza, che permettono il conferimento di determinati gradi di fiducia

> quando corredate da corrispondenti garanzie, fornite da analisi e collaudi

## politiche di sicurezza

nella progettazione di un sistema operativo sicuro, la definizione di una politica di sicurezza costituisce un **quadro concettuale di riferimento** per la specifica dettagliata dei requisiti di sicurezza

> questi ultimi devono essere **oggettivi** e formulati in modo da essere **collaudabili**, perché si possa ottenere garanzia di fiducia nella sicurezza del sistema

una politica di sicurezza fornisce **concetti e regole** che orientano la stesura dei requisiti di sicurezza

> ad es., permettono di analizzarne proprietà quali **consistenza** e **completezza** rispetto alle regole della politica stessa

consideriamo dapprima le politiche di sicurezza **militari**, base storica dello sviluppo di sistemi operativi sicuri, per passare poi a politiche più adatte a sistemi operativi in ambienti **commerciali**

## politiche di sicurezza militari

base delle politiche di sicurezza militari è la **classificazione** delle informazioni secondo una gerarchia di **livelli di autorizzazione**, ad es.:

> non classificato < limitato < riservato < segreto < top secret

inoltre, l'accesso alle informazioni sottosta alla regola **deve-conoscere:**

> l'accesso ai dati sensibili è permesso solo ai soggetti che devono conoscere quei dati per eseguire il loro lavoro

per rendere applicabile la regola, ad ogni informazione classificata si associa un insieme di **scomparti**, relativi all'argomento dell'informazione

> gli scomparti sono anche associati ai progetti in cui è organizzato il lavoro dei soggetti che hanno necessità di accesso all'informazione

la coppia <livello, scomparti> è detta **classe** o **classificazione** di un'informazione

> della stessa forma è lo **svincolo** di un soggetto, che formalizza il livello di autorizzazione fino al quale ha accesso e le categorie di informazione che deve conoscere per il proprio lavoro

l'accesso dei soggetti alle informazioni, o **oggetti** (della protezione) è quindi regolato dalla relazione di **dominanza** fra soggetti e oggetti: un soggetto **s domina** un oggetto **o**

> **s ≥ o** sse $\text{livello}_s \geq \text{livello}_o$ & $\text{scomparti}_s \supseteq \text{scomparti}_o$

## politiche di sicurezza commerciali

in una politica di sicurezza militare, classificazioni e svincoli sono gestiti da un'autorità centrale

le politiche di sicurezza commerciali sono tipicamente di natura **meno rigida**

ad es., di solito non esiste un'autorità centrale per la gestione delle autorizzazioni

permane tuttavia la necessità di classificare i dati in una gerarchia di **livelli di sensibilità**, e di regolare l'accesso dei soggetti ad essi in base alle **necessità del lavoro** che svolgono

**reparti** in cui operano, **progetti** di pertinenza, etc.

le politiche di sicurezza militari sono prevalentemente orientate alla protezione della **riservatezza**

nelle politiche di sicurezza commerciali la protezione dell'**integrità** ha non minore importanza

a questo scopo, ad es., la politica di sicurezza di **Clark & Wilson** (1987) propone il concetto di **transazione ben formata:** una sequenza di triple $<id_u, TP_i, <CD_1, ..., CD_n>>$ dove:

$id_u$ identifica l'utente **u**

$TP_i$ è una **procedura di trasformazione**, che l'utente **u** è autorizzato ad eseguire sui dati:

$<CD_1, ..., CD_n>$, detti **dati vincolati** perché accessibili solo da utenti autorizzati e solo mediante determinate procedure di trasformazione specificate dalla politica di sicurezza

le triple di Clark & Wilson realizzano un approccio **procedurale** alla protezione dell'integrità

## separazione dei doveri

le transazioni ben formate di Clark & Wilson permettono di specificare molti aspetti della **dinamica** di requisiti di sicurezza, poiché descrivono **sequenze** di trasformazioni dei dati, che corrispondono ad appropriate **composizioni** delle relative procedure di trasformazione

tuttavia, ciascuna tripla in una sequenza di Clark & Wilson può solo specificare **vincoli locali** ad una trasformazione

non è cioè possibile far riferimento ad altre triple nella sequenza che formalizza una transazione ben formata

questo limite impedisce di rappresentare aspetti di una politica di sicurezza che possono essere di rilevante importanza

ad es., il principio di **separazione dei doveri** porterebbe a richiedere che gli utenti autorizzati ad eseguire le trasformazioni che compongono una transazione siano tutti diversi (per limitare la possibilità di abusi di potere)

quando ciò occorra, è ben possibile estendere il formalismo di Clark & Wilson per rappresentare anche requisiti non locali di una politica di sicurezza, quale quello indicato

## muraglia cinese

un altro esempio di politica di sicurezza di rilevanza commerciale è quella nota come **Muraglia Cinese**, proposta da **Brewer & Nash** (1989)

protegge la **riservatezza** delle informazioni di una società commerciale, che ha relazioni con altre società, mediante prevenzione di **conflitti di interesse**

tali si definiscono le situazioni in cui uno stesso soggetto abbia accesso a informazioni su **società in concorrenza** fra loro

la politica di sicurezza si basa su **tre livelli di astrazione:**

**oggetti:** dati elementari, ciascun oggetto è relativo a una sola società

**gruppi aziendali:** ciascun gruppo è l'insieme degli oggetti relativi a una data società

**classi di conflitto:** ciascuna classe è la collezione dei gruppi relativi a società in concorrenza fra loro

ogni oggetto appartiene a un solo gruppo, e ogni gruppo a una sola classe di conflitto

**politica di sicurezza:** un soggetto ha accesso a un oggetto **sse** non ha (avuto) accesso a un oggetto di un diverso gruppo aziendale nella stessa classe di conflitto

## reticoli

è facile verificare dalla definizione che la relazione di dominanza, introdotta a proposito delle politiche di sicurezza militari, è un **ordinamento parziale:**

tale è una relazione binaria $\leq$ su un insieme la quale soddisfi le tre proprietà di:

**riflessività:** $x \leq x$

**antisimmetria:** $x \leq y,\ y \leq x \rightarrow x = y$

**transitività:** $x \leq y,\ y \leq z \rightarrow x \leq z$

più specificamente, l'ordinamento parziale di dominanza costituisce un **reticolo**; poiché questo concetto sta alla base di modelli di sicurezza considerati nella prossima lezione, ne precisiamo una definizione

non è l'unica possibile, ma è la più appropriata all'uso del concetto in questo contesto

**terminologia:** se $\leq$ è un ordinamento parziale:

se $a \leq b$, allora $a$ è un **minorante** di $b$, e $b$ è un **maggiorante** di $a$

$a$ è un **minorante** (risp. **maggiorante**) dell'insieme $S$ se è un minorante (risp. maggiorante) di ogni elemento in $S$

**definizione:** un **reticolo** è un ordinamento parziale in cui ogni **coppia** di elementi abbia:

un **minimo maggiorante** (ingl. **join**, o **l.u.b.**: least upper bound ) e

un **massimo minorante** (ingl. **meet**, o **g.l.b.**: greatest lower bound )