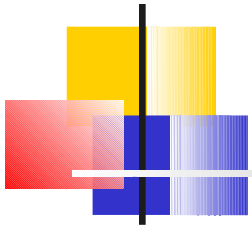
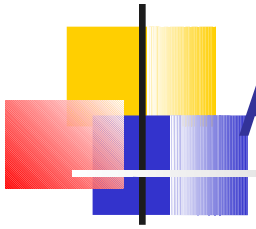


# Analisi delle risorse da proteggere

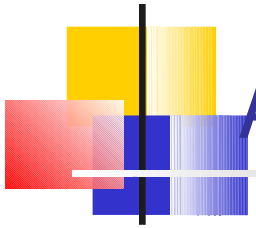
# Analisi delle risorse da proteggere -I

- E' il primo passo della definizione della politica deve individuare
  - le possibili risorse critiche che causano perdite se obiettivo di un attacco
  - l'uso delle risorse da parte dell'ente/ azienda
  - Le attività aziendali (processi) utilizzano le risorse
- Deve inoltre valutare il danno per l'azienda se
  - il processo aziendale viene bloccato (integrità o disponibilità)
  - la risorsa deve essere ricostruita ex novo (database) (integrità)
  - l'attaccante conosce le informazioni contenute nella risorsa (confidenzialità)



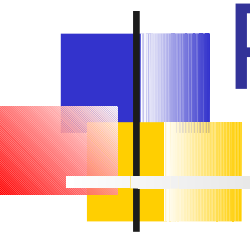
# Analisi delle risorse da proteggere -II

- Risorsa
  - Database con informazioni
  - Applicazioni (talvolta più importanti dei database che utilizzano)
  - Capacità di calcolo
  - Capacità di comunicazione

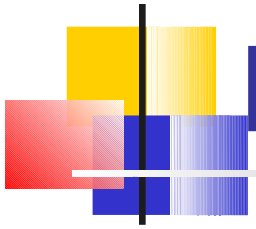


# Analisi delle risorse da proteggere -III

- Spesso è difficile stimare il "valore" di una risorsa
- Strategia alternativa è stimare
  - quanto costerebbe ricreare ex novo la risorsa (database, applicazioni …)
  - Perdita di attività mentre si ricostruisce
- Questa analisi è utile indipendentemente dalla sicurezza perchè produce un inventario delle risorse informative



# Politica di Sicurezza



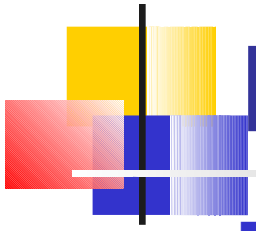
# Politica di sicurezza

Politica di sicurezza = un insieme di regole che riducono il rischio

- Stabilendo gli obiettivi di sicurezza = cosa proteggere
- definendo i comportamenti legali
- vietando l' uso di componenti pericolosi
- richiede la definizione di
  - Architettura Sistema
  - Inventario dei componenti e delle applicazioni
  - Utenti (diritti/doveri)
  - Amministratori (diritti/doveri)
  - Uso legale delle risorse
  - Responsabili della politica
  - Sanzioni

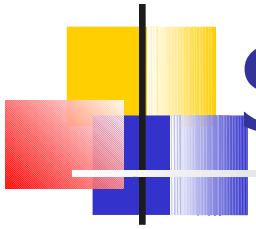
# Politica di sicurezza

- Importante perchè definisce
  - i nostri obiettivi in termini di sicurezza
  - Le operazioni legali
  - Come utilizzare i componenti le cui vulnerabilità non siano state eliminate
  - regole per gestione del personale, risorse
  - Responsabilità e sanzioni
- Relazione tra la politica di sicurezza e legislazione che la politica deve recepire



# Politica di sicurezza

- Inventario delle risorse, logiche e fisiche (oggetti)
- Uso accettabile delle risorse
- Criticità di ogni risorsa
- Regole per il controllo degli accessi (soggetti/oggetti)
- Responsabilità dell' installazione e manutenzione delle applicazioni e dei sistemi operativi
- Strumenti da usare
  - per elaborazione e per protezione delle risorse
  - per controlli interni
- Periodicità
  - del riesame della politica
  - dell'analisi del rischio

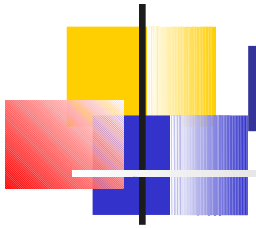


# Soggetti & oggetti

- Una definizione più formale della politica astrae  risorse condivise ed utenti come oggetti e soggetti che su di esse operano
- I soggetti invocano le operazioni definite dagli oggetti
- Se un oggetto invoca le operazioni definite da altri oggetti allora diventa esso stesso un soggetto
- La nozione di soggetto/oggetto dipende dal livello di astrazione

Soggetto = utente, applicazione, programma, processo, thread, istruzione, microistruzione …

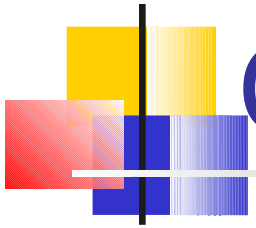
Oggetto = tipo di dato astratto, procedura, parametro, risorsa logica, risorsa fisica



# Diritti

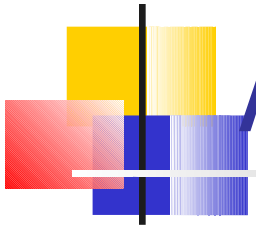
- Il diritto equivale alla possibilità per un soggetto di invocare una certa operazione
- In base al livello di astrazione, il diritto viene stabilito in base alla politica di sicurezza in modo diretto o indiretto
  - Diretto = S può leggere il file F
  - Indiretto= poiché S può leggere F allora il programma eseguito da S può accedere all'area di memoria dove sono memorizzati i dati di F

    = deduzione da un diritto diretto



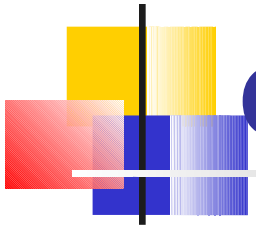
# Oggetti ed operazioni

- La definizione di oggetti ed operazioni equivale alla definizione di tipo di dato
- La correttezza dell'invocazione delle operazioni su un certo oggetto può essere formulata utilizzando i meccanismi per la verifica dei tipi dei dati
- Controlli sui tipi non possono essere solo statici ma occorre prevedere controlli a tempo di esecuzione per scoprire e limitare gli attacchi permessi dalla vulnerabilità = le vulnerabilità rendono necessari controlli a tempo d'esecuzione



# Alcuni tipi di politica

- Default allow = definisce i comportamenti illegali e quindi vietati e permette tutto il resto = enumerating badness
- Default deny = definisce i comportamenti legali e vieta tutto il resto
- "Ci sono più cose in terra ed in mare che nella tua politica"  quindi default allow è troppo pericolosa = enumerating badness dimentica sempre di vietare qualcosa



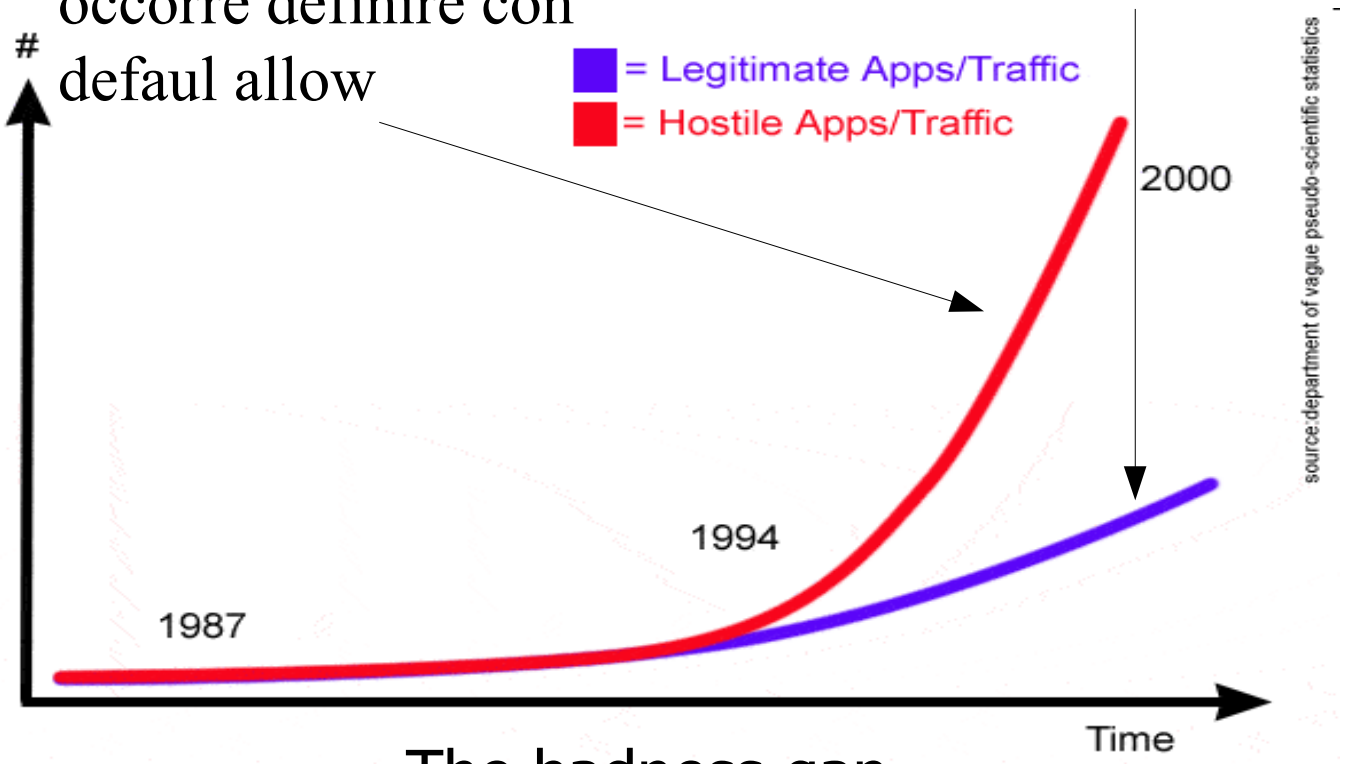
# The Six Dumbest Ideas in Computer Security (M.Ranum)

1. **Default Permit**
2. **Enumerating Badness**
3. **Penetrate and Patch**
4. **Hacking is Cool**
5. **Educating Users**
6. **Action is Better Than Inaction**

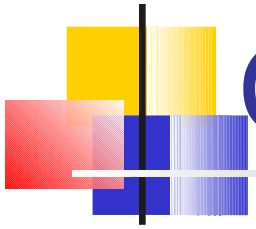
# Enumerating Badness

Questo è quello che occorre definire con defaul deny

Questo è quello che occorre definire con defaul allow

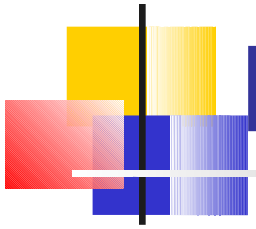



The badness gap



# Classi di politiche di sicurezza

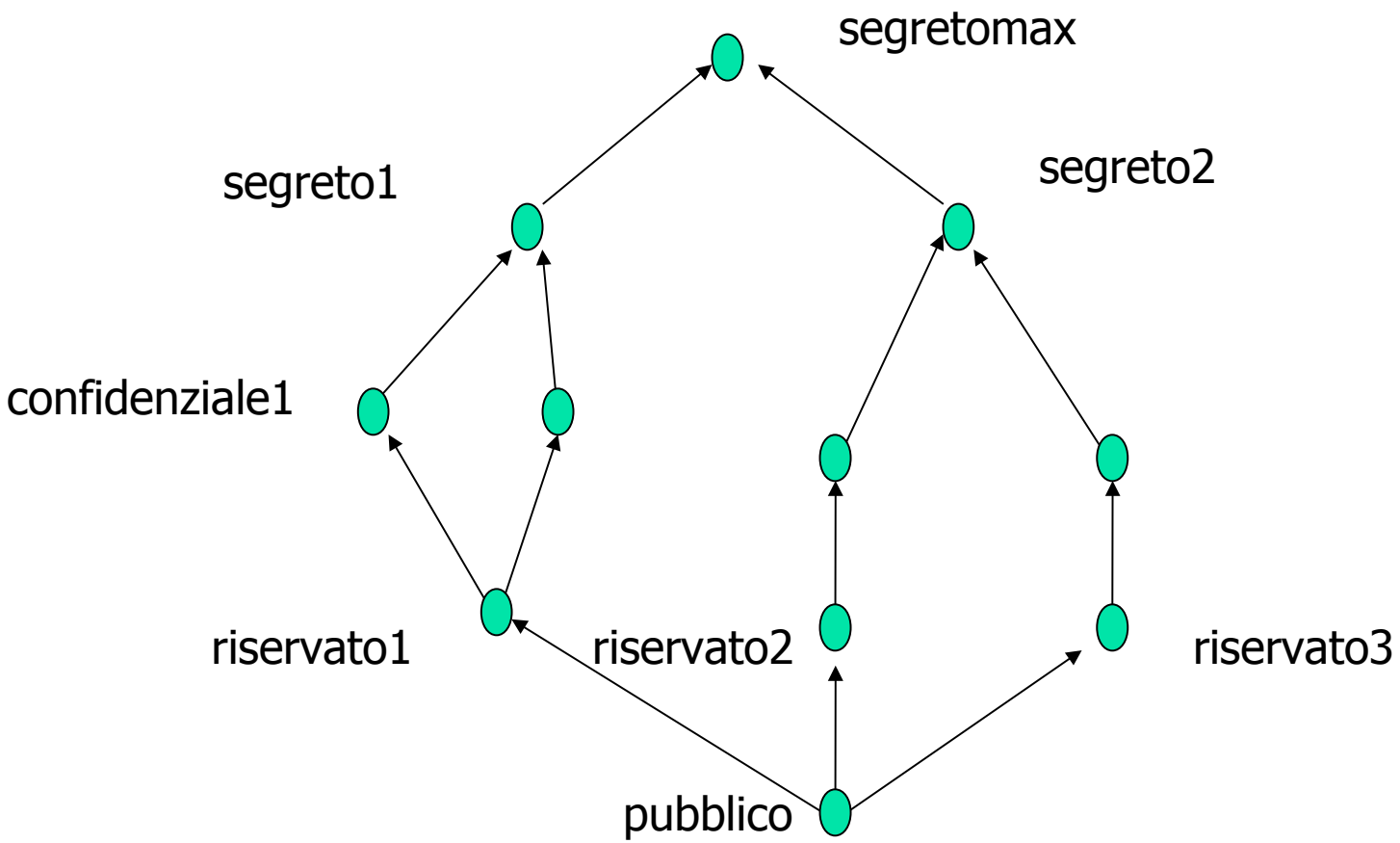
- Discretionary access control
  - Per ogni oggetto esiste un proprietario
  - Il proprietario decide
    - i soggetti che hanno necessità di operare su un oggetto (need to access)
    - i loro diritti
- Mandatory access control
  - Esistono delle regole di sistema che l'owner non può violare

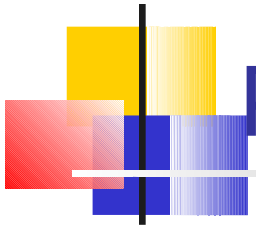


# Mandatory Access Control

- Tutti i soggetti sono divisi in classi
- Tutte gli oggetti divisi nelle stesse classi dei soggetti (non strettamente necessario, solo per semplicità)
- Le classi sono ordinate parzialmente
- La possibilità di eseguire una certa operazione dipende
  - dalla classe del soggetto e da quella dell'oggetto
  - dall'owner

# Ordinamento Parziale

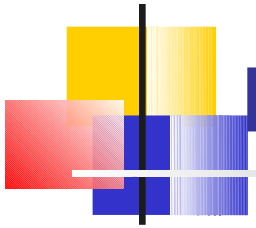




# Politica MAC o information flow - I

- Oggetto = file
- Operazioni = read/write/append
- Un soggetto può
  - leggere tutti i file che hanno classe minore o uguale alla sua
  - modificare i record dei file che hanno classe uguale alla sua
  - appendere un record ad un file che ha classe maggiore della sua
  - è necessario anche il permesso di owner ma all'interno del dominio definito dalle regole

Si privilegia la confidenzialità (No write down)

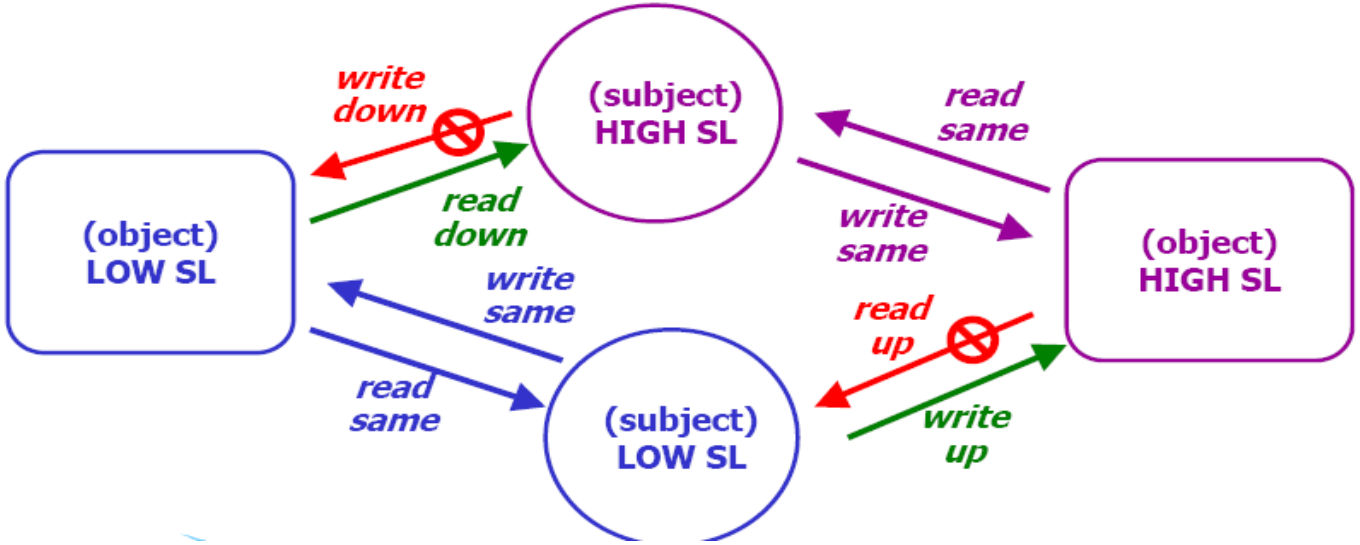


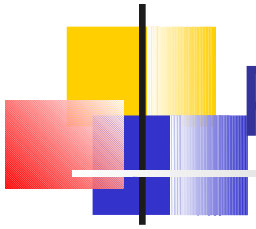
# no write down

- Impedisce di trasferire informazioni da una classe alta ad una bassa con la conseguente perdita di sicurezza
- Provoca un accumulo di informazioni al livello alto poiché un soggetto trasferisce informazioni da livelli bassi a quelli alti
- Periodica desegretazione delle informazioni per trasferire dai livelli alti a quelli bassi

# Mandatory Access Control - I

- Bell-LaPadula Policy (multilevel security)
  - access control attributes:
    - hierarchical security level
    - set of non hierarchical categories
  - fixed rules: "no read up, no write down"

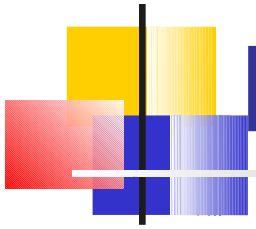




# Politica MAC o information flow - II

- Oggetto = file
- Operazioni = read/write
- Un utente può
  - scrivere tutti i file che hanno classe minore o uguale alla sua
  - Leggere tutti i file che hanno classe maggiore o uguale

Si privilegia l'integrità (No write up)

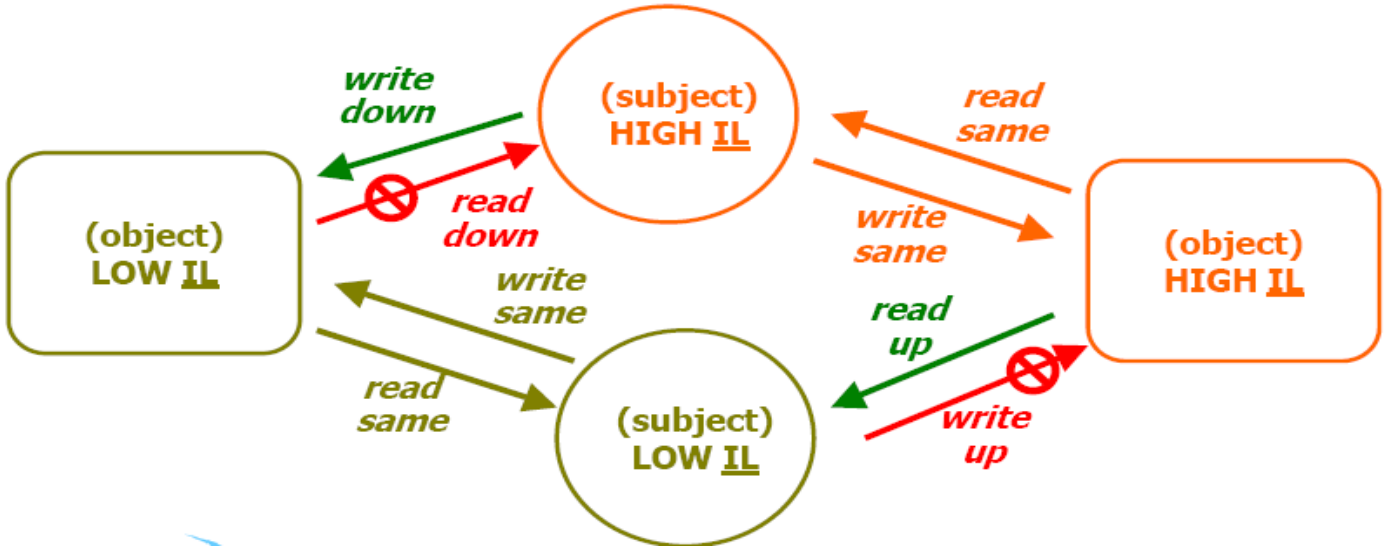


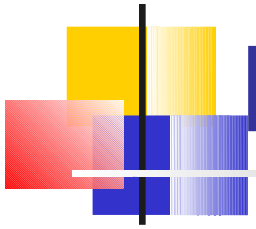
# No write up

- Impedisce ad un soggetto inaffidabile di invalidare una informazione critica
- Si corre il rischio di perdere la confidenzialità pur di garantire integrità

# Mandatory Access Control - II

- Biba Integrity model (multilevel security)
  - access control attributes:
    - hierarchical integrity level
    - set of non hierarchical integrity categories
  - fixed rules: "no write up, no read down"
    - exact opposite of BLP/multilevel security

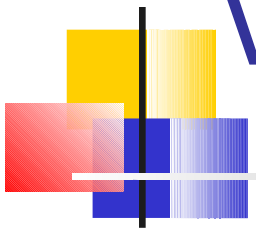




# Non interferenza

- Ad ogni soggetto ed ogni oggetto è associata una etichetta che ne stabilisce il livello
- L'etichetta è funzione delle operazioni eseguite sull'oggetto e delle etichette associate ai soggetti che le eseguono
- Un sistema soddisfa il principio di non interferenza se i suoi output ad un certo livello non cambiano anche se si eliminano soggetti ed oggetti di livello più elevato o meno elevato (Bell-LaPadula o Biba)
- Non si ha travaso di informazioni dai livelli superiori o perdita di integrità dagli inferiori

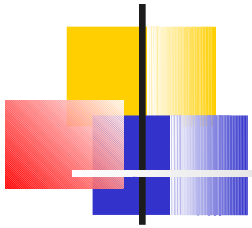
# Vincoli e operazioni



- In questo caso la politica definisce
  - un insieme di vincoli di consistenza sullo stato degli oggetti da proteggere
  - un insieme di operazioni ognuna delle quali è una transizione corretta di stato
- Si passa da uno stato globale che soddisfa i vincoli di consistenza ad un altro che soddisfa ancora i vincoli di consistenza

# Vincoli e operazioni -2

- Ogni transizione è atomica, viene eseguita completamente o non eseguita
- Si può copiare lo stato degli oggetti coinvolti per avere un backup
- Occorre ovviamente provare che ogni transazione provoca una transizione corretta di stato

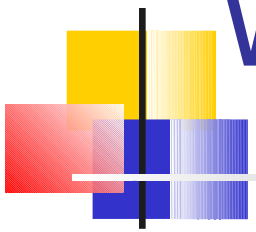


# Esempio

- Ad esempio si possono definire dei vincoli sui conti correnti degli utenti
  - Movimenti a somma zero tra i conti
  - In ogni giorno i soldi ritirati = alla differenza dei conti rispetto al giorno precedente
- La transazione che aggiorna i conti correnti con le operazioni della giornata deve soddisfare i vari vincoli

# Chinese Wall

- Gli oggetti del sistema sono partizionati in sottoinsiemi
- L'utente che ha operato su un oggetto di un insieme non può operare su quelli in un altro insieme
- Permette di gestire conflitti di interesse
- E' dipendente dal tempo
- E' compatibile con MAC



# Watermark

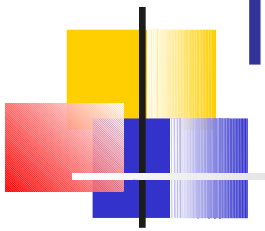
- Il livello di un soggetto non è fissato ma varia in un certo range e dipende da quello degli oggetti su cui ha operato fino all'istante considerato
- Ad esempio il livello di confidenzialità aumenta quando ha letto oggetti di livello elevato
- Ovviamente non diminuisce se dopo legge oggetti di livello minore
- Altra politica che dipende dal tempo

# Politica complessiva – I

- Una politica reale può combinare politiche diverse
- Ad esempio posso fondere
  - No write down
  - Chinese wall
- In questo caso, una volta stabilito mediante i livelli se un certo oggetto può essere letto/scritto, si ha un insieme di altri oggetti che non possono essere acceduti

# Politica complessiva – II

- Fusione di politiche può avvenire anche rispetto agli oggetti
- Un soggetto ha livello per integrità e un altro per confidenzialità
  - Di alcuni oggetti interessa la confidenzialità (no write down)
  - Di altri oggetti interessa l'integrità (no write up)



# Trusted Computing Base

- TCB comprende i componenti del sistema a cui è delegata implementazione della politica di sicurezza
- Se uno di questi componenti è affetto da un errore allora l'implementazione della politica non è corretta e (quasi) sicuramente questo errore è una vulnerabilità
- Quindi dobbiamo poterci “fidare” di questi componenti = garantirne l'affidabilità = assurance

# Dimensioni TCB

- Minore è il numero di componenti di cui dobbiamo fidarci, migliore è la situazione dal punto di vista della sicurezza
- Dimensione ridotta permette anche l'applicazione di tecniche formali per la correttezza
- Questo è un criterio importante per valutare implementazioni alternative di una stessa politica

# Dimensioni TCB

- Ovviamente minore è il numero di componenti di cui dobbiamo fidarci, migliore è la situazione dal punto di vista della sicurezza
- Dimensione ridotta permette anche l'applicazione di tecniche formali per la correttezza del software del TCB

# Possibilità di utilizzare un diritto

Dati

- un assegnamento di diritti agli utenti
- la possibilità per alcuni utenti di concedere (grant) e prelevare (take) diritti a/da altri utenti condizionato al possesso di altri diritti

Esiste una sequenza di azioni che permette ad un utente di utilizzare un certo diritto ?

Nel caso più generale il problema non è decidibile

# Principio di attenuazione

- Un soggetto può concedere solo i diritti che possiede
- Generalizzabile a "solo i diritti che esso controlla"
- Ad esempio il proprietario di una risorsa può concedere diritti sulla risorsa anche se non ha quei diritti = non ha attribuito a se stesso quei diritti