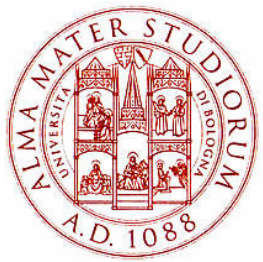
Sicurezza 2006 - 2007

Lezione 3: Concetti di base

Gabriele D'Angelo
<gda@cs.unibo.it>
http://www.cs.unibo.it/~gdangelo/



Master universitario in
Tecnologia del Software Libero
e Open Source
Università di Bologna

05/10/2007, Bologna

Scaletta della lezione

- Protezione e sicurezza
- Obiettivi della sicurezza
- Politiche e meccanismi
- Minacce
- Obiettivi della protezione
- Attacchi

Protezione e sicurezza

- **Comunemente i termini “protezione” e “sicurezza” sono usati come sinonimi, in realtà sono piuttosto differenti**
  - **Sicurezza**:
    - è il problema generale, che coinvolge non solo il sistema informatico, ma anche aspetti amministrativi, legali, politici e finanziari
    - è la misura della fiducia sul mantenimento della integrità dei dati di un sistema informatico
  - **Protezione**:
    - l'insieme dei meccanismi utilizzati in un sistema di calcolo per il controllo di accesso alle risorse

Obiettivi della sicurezza

- **Data confidentiality**: come mantenere la *segretezza* dei dati
- **Data integrity**: come evitare che i dati vengano *alterati*
- **System availability**: come garantire che il sistema continui ad *operare senza interruzioni*
- E inoltre è importante evitare che il sistema diventi un **trampolino di lancio per altri attacchi**. Sia per evitare lo spreco di risorse, sia per gli aspetti legali eventualmente dovuti ad un'intrusione che origina dai nostri sistemi: dimostrare la nostra estraneità potrebbe essere molto difficile e comunque costoso

Sicurezza

- **Un sistema può essere definito sicuro se tutte le sue risorse sono accedute nei modi previsti ed autorizzati**

- Tipiche violazioni di sicurezza:
  - Furti di informazioni (data confidentiality)
  - Alterazione o distruzione dei dati (data integrity)
  - Denial of Service (system availability)

Politiche e meccanismi [di sicurezza]

- È fondamentale che ci sia una netta separazione tra le **politiche** e i **meccanismi**:
  - la *politica* decide **cosa deve essere fatto**
  - i *meccanismi* attuano **la decisione**
- Si tratta di un concetto fondamentale di software engineering:
  - la componente che prende le decisioni "politiche" può (e dovrebbe) essere completamente divisa da quella che implementa i meccanismi
- Questo rende possibile:
  - cambiare la politica senza cambiare i meccanismi
  - implementare nuovi meccanismi senza cambiare la politica

Politiche [di sicurezza]

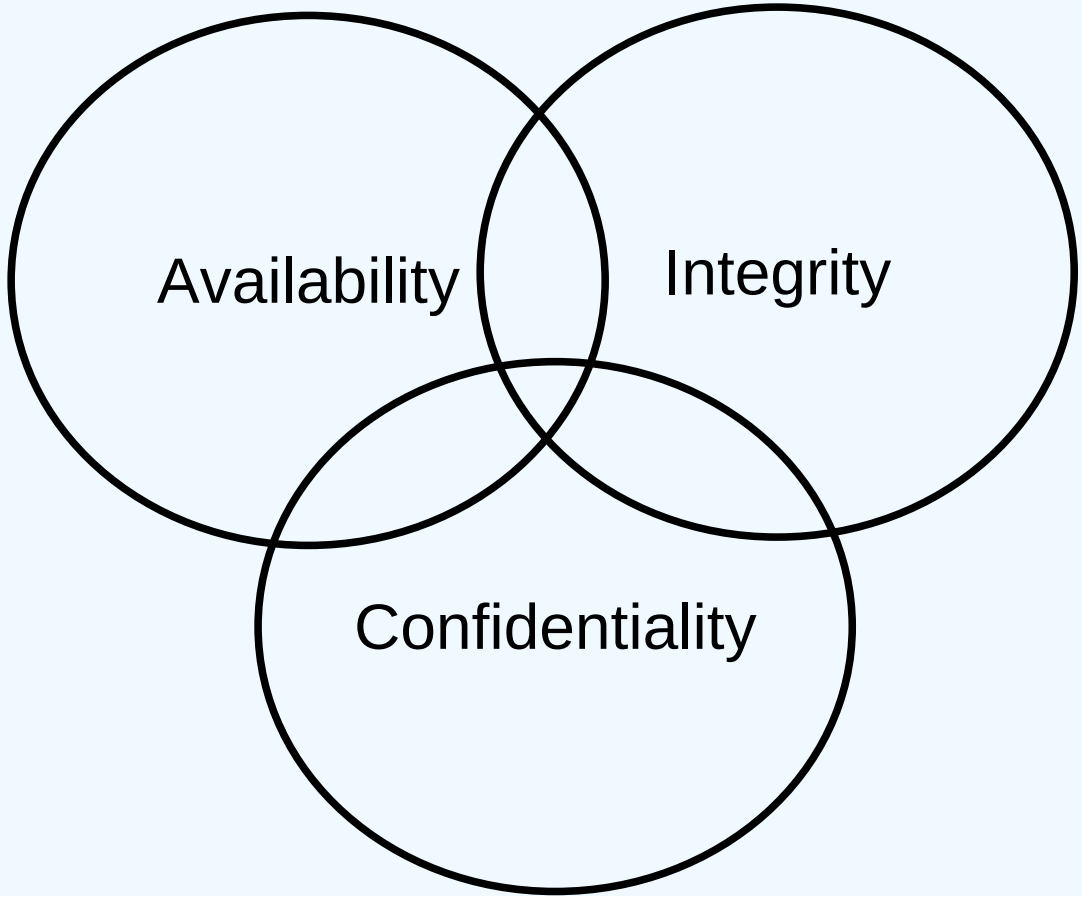
- La scelta di una politica di sicurezza dipende da:
  - il tipo di *attacchi* e *attaccanti* **attesi**
  - il **valore** delle informazioni contenute nel sistema
  - i **costi** dovuti all'utilizzazione di una politica di sicurezza
- Valutare questo tipi di problemi:
  - è ben oltre lo scopo di un corso introduttivo alla sicurezza
  - nel nostro caso ci concentreremo principalmente sui meccanismi

Minacce: tipologie

- Possiamo classificare le minacce di sicurezza all'interno di queste quattro tipologie:
  - **Intercettazione:** un'entità non autorizzata ottiene l'accesso in "lettura" a una risorsa
  - **Modifica:** un'entità non autorizzata ottiene l'accesso in "scrittura" a una risorsa
  - **Interruzione:** la fornitura di un servizio viene interrotta
  - **Falsificazione:** creazione di oggetti contraffatti

Minacce: obiettivi della protezione

- È necessario definire con estrema attenzione gli **obiettivi** della protezione, devono essere definiti **correttamente** e con il **giusto equilibrio**



Minacce: obiettivi della protezione

- **Confidentiality (riservatezza, privacy)**
  - A prima vista: semplice da definire
  - Tuttavia:
    - chi determina chi può accedere a cosa?
    - qual'è la granularità dell'accesso?
    - è possibile accedere ai dati esterni al contesto?
    - un'entità autorizzata può divulgare dati ad altre entità? (eventualmente attraverso un covered/hidden channel)
- **Integrity (integrità)**
  - ancora più difficile da definire
  - ad esempio:

    preciso, accurato, non modificato, modificato in modo accettabile, modificato da processi autorizzati, coerente, etc.

Minacce: obiettivi della protezione

- **Availability (disponibilità)**
  - relativa sia ai *dati* che ai *servizi* (processi che operano sui dati)
  - ancora una volta, è difficile da definire formalmente:
    - il dato/servizio è presente in forma utilizzabile
    - una richiesta viene completata in forma accettabile
    - **graceful degradation**: si tratta di una forma di **fault tolerance**, il sistema è in grado di funzionare anche in presenza di guasti o problemi ad una o più sue componenti hardware o software (molto difficile da implementare)
- **Ma non solo...**
  - come evitare che il sistema sia un trampolino di lancio per altri attacchi

Attacchi: modellazione degli attacchi

- **È necessario comprendere:**
  - come si compone un attacco
  - qual'è l'obiettivo degli attacchi
  - chi sono gli attaccanti
  - quali attacchi sono più facili di altri
  - quali sono le assunzioni di sicurezza di un sistema *(ad esempio spesso si assume [sbagliando] la sicurezza fisica del sistema).* In presenza di un accesso fisico molte tecniche di protezione risultano completamente inutili
  - dove spendere meglio il budget di sicurezza *(che è sicuramente limitato e molto più probabilmente inadeguato)*

Attacchi: composizione di un attacco

- **Un attaccante deve poter disporre di questi tre elementi:**
  - **Metodo**
    - capacità, conoscenze e strumenti necessari per l'attacco
    - attacchi diversi richiedono abilità diverse
  - **Opportunità**
    - di quanto tempo dispone un attaccante?
    - che tipo di accesso è a disposizione dell'attaccante?
    - che tipo di fondi sono a disposizione dell'attaccante?
  - **Movente**
    - crimine di opportunità vs. attacco con obiettivo specifico
    - motivazione finanziaria vs. motivazione politica
    - divertimento, ovvero nessun movente

Attacchi ed attaccanti

- **Le intrusioni possono essere di vario tipo e con conseguenze molto diversificate**
  - **Attaccanti passivi:**
    - attaccano un sistema al fine di leggere i dati, senza modificarli
  - **Attaccanti attivi:**
    - attaccano un sistema al fine di modificare i dati, spesso causando danni
- Non necessariamente un attacco passivo è da preferibile ad uno attivo. Gli attacchi passivi passano molto spesso inosservati per lungo tempo e l'attaccante ha la possibilità di raccogliere molte informazioni preziose senza alcuna forma di reazione da parte della vittima

Attacchi ed attaccanti

- **Quali sono i principali obiettivi degli attaccanti? (dal punto di vista tecnico)**
  - Acquisire una qualche *forma di controllo della macchina*
  - Se possibile, acquisire il *controllo totale della macchina*
- **Nota sui sistemi operativi multi-utente**
  - Permettono a più persone di accedere allo stesso sistema informativo
  - **Vi è una distinzione estremamente importante tra:**
    - **Utenti normali**
      - hanno accesso solo ad un sottoinsieme di risorse personali e ad alcune risorse opportunamente condivise
    - **Superutenti, root, amministratori di sistema, administrator**
      - hanno accesso *all'intero insieme di risorse* della macchina
      - la controllano totalmente (e se l'admin fosse un nemico?)

Attacchi: elementi coinvolti

- **Hardware**
  - L'hardware fornisce i meccanismi base per implementare i meccanismi di protezione più complessi?
  - **Ma innanzitutto: cosa si intende con hardware?**
    - Il processore, la memoria, i dispositivi di input/output
    - Ma anche l'ambiente fisico in cui si trova la macchina (**sicurezza fisica**)

- **Sistema operativo (nucleo)**
  - Il nucleo del sistema operativo fornisce due meccanismi fondamentali per garantire la protezione del sistema:
    - **Autenticazione**
    - **Autorizzazione**

Attacchi: elementi coinvolti

- **Sistema operativo (librerie, tool di sistema)**
  - Spesso e volentieri:
    - contengono grandi quantità di codice
    - vengono eseguiti in *modalità superutente*
  - Quali sono gli attacchi possibili a questi elementi?
    - attacchi *interni* e *esterni*
- **Applicazioni**
  - quasi sempre scritte da *non esperti di sicurezza*. Molto spesso gli argomenti di sicurezza non fanno parte dell'educazione degli informatici o di chi si occupa di informatica. Programmare non è banalmente "scrivere codice"
  - possono fornire una prima "testa di ponte" per attaccare un sistema (es. base per ulteriori attacchi al sistema operativo)
- **Utenti**
  - sono indiscutibilmente l'anello più debole del sistema!
  - tutta la sicurezza ruota intorno a loro

Ringraziamenti

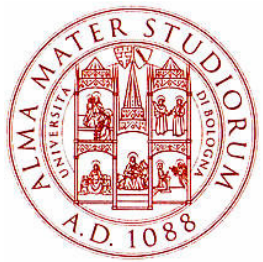
- Gran parte di questi lucidi sono direttamente tratti o “ispirati” da un lavoro precedente del Prof. Renzo Davoli e del Prof. Alberto Montresor, si ringrazia sentitamente

- In ogni caso la responsabilità di qualsiasi eventuale errore rimane integralmente dell’autore di questa lezione

Sicurezza 2006 - 2007

Lezione 3: Concetti di base

Gabriele D'Angelo
<gda@cs.unibo.it>
http://www.cs.unibo.it/~gdangelo/



Master universitario in
Tecnologia del Software Libero
e Open Source
Università di Bologna

07/09/2007, Bologna