Sicurezza dei sistemi e delle reti
Introduzione

Damiano Carra

Università degli Studi di Verona
Dipartimento di Informatica

Riferimenti

- Cap. 8 di “Reti di calcolatori e Internet. Un approccio top-down”, J. Kurose, K. Ross

- Dispense su Internet

  http://infomsearchdata.wikispaces.com/file/view/myiOS.pdf/300514424/myiOS.pdf

  http://www.provincia.foggia.it/upload_delibere/9/2007000002.pdf

  - capitoli 1-4 e 20

Domande fondamentali

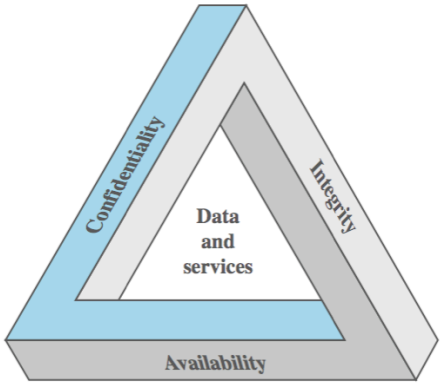
1. Quali risorse (o asset) vogliamo proteggere?
2. In che modo tali risorse sono minacciate?
3. Cosa bisogna fare per contrastare tali minacce?

1- Quali risorse (o asset) vogliamo proteggere?

- Hardware
  - Sistemi, componenti, dischi
    - Sicurezza “fisica”
- Software
  - Sistema Operativo e Applicativi
- Dati
  - File, database
- Rete
  - Collegamenti e apparati

Cosa vuol dire "*proteggere*"?

- Garantire le proprietà di
  - Confidenzialità
  - Integrità
  - Disponibilità



- In aggiunta
  - Autenticità
  - Tracciabilità (Accountability)

Confidenzialità

- Nessun utente deve poter ottenere o dedurre dal sistema informazioni che non è autorizzato a conoscere

- Riservatezza dei dati
  - Le informazioni confidenziali non devono essere rivelate o rilevabili da utenti non autorizzati
- Privacy
  - L'utente controlla o influenza quali informazioni possono essere collezionate e memorizzate

Integrità

- Impedire l' alterazione diretta o indiretta delle informazioni, sia da parte di utenti e processi non autorizzati, che a seguito di eventi accidentali
  - Se i dati vengono alterati è necessario fornire strumenti per poterlo verificare facilmente
- Integrità dei dati
  - Le informazioni e i programmi possono essere modificati solo se autorizzati
- Integrità del sistema
  - Il sistema funziona e non è compromesso

Disponibilità

- Rendere disponibili a ciascun utente abilitato le informazioni alle quali ha diritto di accedere, nei tempi e nei modi previsti
  - in determinate condizioni, in un preciso istante, in un intervallo di tempo
- Nei sistemi informatici, i requisiti di disponibilità includono prestazioni e robustezza

Autenticità

- Ciascun utente deve poter verificare l'autenticità delle informazioni
  - messaggi, mittenti, destinatari
- Si richiede di poter verificare se una informazione è stata manipolata
  - vale anche per informazioni non riservate

Tracciabilità

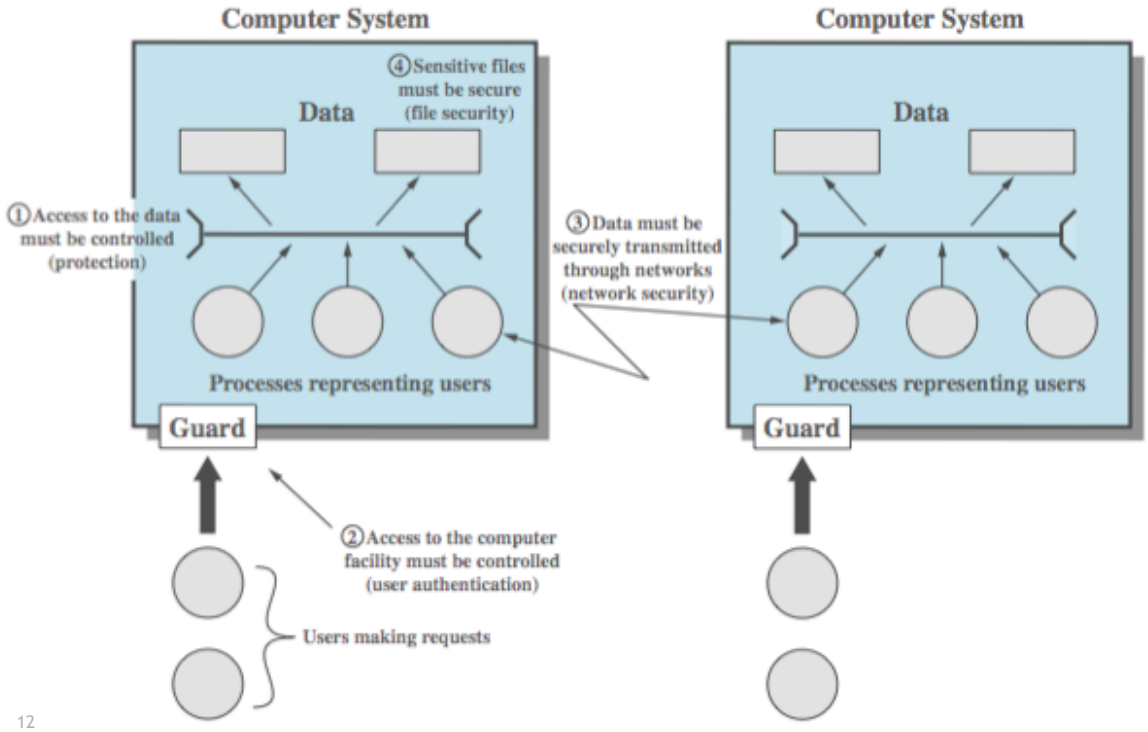
- Le azioni di un'entità devono essere tracciate in modo univoco in modo tale da supportare la non-ripudiabilità e l'isolamento delle responsabilità
  - Ad es., nessun utente deve poter ripudiare o negare in tempi successivi messaggi da lui spediti o firmati

2- In che modo le risorse sono minacciate?

- Le minacce compromettono le proprietà di
  - Confidenzialità
  - Integrità
  - Disponibilità
- Esempi

	Confidenzialità	Integrità	Disponibilità
HW			Calcolatore rubato
SW	Copia non autorizzata	Eseguibile modificato	Eseguibili cancellati
Dati	Lettura non autorizzata	File modificati	File cancellati
Rete	Lettura messaggi inviati	Messaggi modificati / ritardati / duplicati	Messaggi distrutti Rete fuori uso

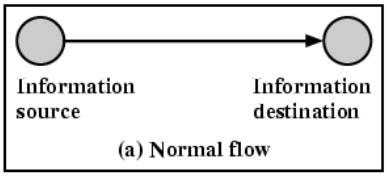
Minacce e attacchi

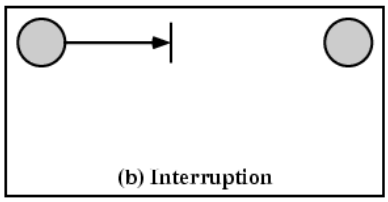


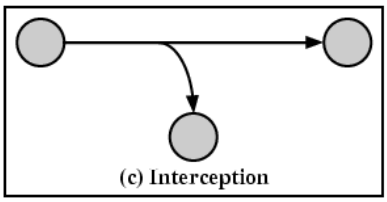
Minacce e attacchi

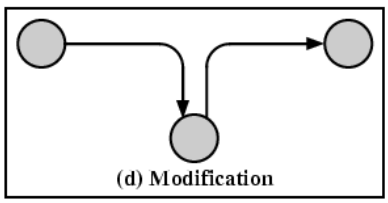
- Una minaccia è una *possibile* violazione della sicurezza
- La violazione *effettiva* è chiamata attacco
- Gli attacchi possono essere
  - Attivi
    - Tentativi di alterare le risorse o modificare il funzionamento dei sistemi
  - Passivi
    - Tentativi di carpire informazioni e utilizzarle senza intaccare le risorse
  - Interni
    - Iniziati da un'entità interna al sistema
  - Esterni
    - Iniziati da un'entità esterna, tipicamente attraverso la rete

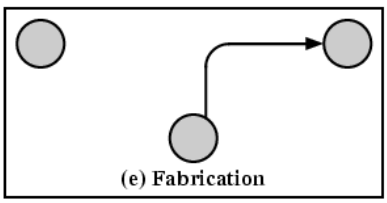
Attacchi: esempi











Classi di minacce / attacchi

- Disclosure
  - Accesso non autorizzato alle informazioni
- Deception
  - Accettazione di dati falsi
- Disruption
  - Interruzione o prevenzione di operazioni corrette
- Usurpation
  - Controllo non autorizzato di alcune parti del sistema

3- Cosa bisogna fare per contrastare le minacce?

- Questa è la domanda più difficile
  - La complessità della sicurezza sta proprio qui
  - Non esiste una risposta unica
  - Le risposte cambiano nel tempo
- Sistemi complessi
  - Le risorse da proteggere sono sistemi composti da sotto-sistemi
  - Sicurezza di un sistema *vs* sicurezza dei suoi componenti
  - Teoria *vs* pratica
    - Condizioni ideali e prevedibili / reali e imprevedibili

Sfide poste dalla sicurezza

- Attacchi potenziali
  - Nella progettazione dei sistemi serve considerare i possibili attacchi
- Soluzioni contro-intuitive
  - Nello sviluppo dei meccanismi di sicurezza, dovuto alla complessita' del sistema e alle possibili minacce
- Dove usare i meccanismi di sicurezza?
  - Sia a livello fisico che logico (protocollare)
- La sicurezza dipende non solo algoritmi o protocolli, ma anche dagli utenti
  - informazioni possedute (ad es., password)
  - creazione, distribuzione e protezione di tali informazioni

Sfide poste dalla sicurezza (cont'd)

- Continua battaglia tra amministratori e attaccanti
  - Per l'attaccante è sufficiente sfruttare una singola vulnerabilità, mentre gli amministratori si devono prevederle ed eliminarle tutte
- La sicurezza non viene percepita come un beneficio
  - Fino a quando non avviene un incidente di sicurezza
- La sicurezza richiede un controllo continuo delle risorse
- Meccanismi di sicurezza come elementi aggiuntivi
  - Invece che parte integrante della progettazione
- La sicurezza è vista come un impedimento / rallentamento del normale funzionamento dei sistemi

Principi fondamentali di progettazione della sicurezza

- Nonostante anni di ricerca, è difficile progettare sistemi che prevengono completamente le falle nella sicurezza

- Tuttavia, insiemi di pratiche e regole sono state codificate
  - Analogamente a quanto succede per ingegneria del software
  - Aspetti economici dei meccanismi, fail-safe default, progettazione aperta, tracciabilità delle operazioni, separazione dei privilegi, separazione delle funzionalità, isolamento dei sottosistemi, modularità

Principi fondamentali di progettazione della sicurezza

- Aspetti economici dei meccanismi
  - La progettazione delle misure di sicurezza deve essere il piu' semplice possibile
    - Da implementare e verificare
- Fail-safe default
  - Comportamenti non specificati devono prevedere un default sicuro
    - Ad es. permessi di accesso
- Progettazione aperta
  - Preferibile rispetto a codice segreto
- Tracciabilità delle operazioni
  - Qualsiasi operazione può essere ricostruita e il sistema ripristinato

Principi fondamentali di progettazione della sicurezza

- Separazione dei privilegi
  - Differenziazione degli accessi
    - Alle risorse create da ciascun utente (file)
    - Alle risorse critiche
- Separazione delle funzionalità
  - Distinzione dei ruoli nei diversi punti del sistema fisico e logico
- Isolamento dei sottosistemi
  - Un sistema compromesso non dovrebbe compromettere gli altri
- Modularità
  - Meccanismi di sicurezza indipendenti, sostituibili, riusabili

Politiche di sicurezza

- Una politica di sicurezza è un'indicazione di cosa è e cosa non è permesso
- Le regole possono riguardare:
  - I dati
    - Protezione
  - Le operazioni possibili
    - Controllo
  - Gli utenti singoli e i profili
    - Controllo

Politiche e meccanismi

- Un meccanismo di sicurezza è un metodo (strumento/ procedura) per garantire una politica di sicurezza
- Data una politica, che distingue le azioni "sicure" da quelle "non sicure", i meccanismi di sicurezza devono prevenire, scoprire o recuperare da un attacco
- Prevenzione: il meccanismo deve rendere impossibile l'attacco
  - Spesso sono pesanti ed interferiscono con il sistema al punto da renderlo scomodo da usare
  - Esempio: richiesta di password come modo di autenticazione

Politiche e meccanismi

- Scoperta: il meccanismo è in grado di scoprire che un attacco è in corso
  - E' utile quando non è possibile prevenire l'attacco, ma può servire anche a valutare le misure preventive
  - Si usa solitamente un monitoraggio delle risorse del sistema, cercando eventuali tracce di attacchi
- Recupero da un attacco: si può fare in due modi
  - Fermare l'attacco e recuperare/ricostruire la situazione pre-attacco, ad esempio attraverso copie di backup
  - Continuare a far funzionare il sistema correttamente durante l'attacco (fault-tolerant)

Meccanismi e livelli

- In quale livello del computer conviene inserire un determinato meccanismo?
- Livelli bassi
  - Meccanismi generali, semplici, grossolani, ma dimostrabili corretti
- Livelli alti
  - Meccanismi ad hoc per gli utenti, sofisticati, difficili da dimostrare corretti

Meccanismi di sicurezza – Esempi

- Meccanismi specifici – Legati ad uno specifico livello OSI
  - Crittografia
    - Trasformazione dei dati in un formato non intellegibile
  - Firma digitale e Integrità dei dati
    - Usata per provare la sorgente e l'integrità di dati o messaggi
  - Autenticazione e Controllo degli accessi
    - Gestione dei diritti degli utenti rispetto le risorse
- Meccanismi generali
  - Rilevamento degli eventi
  - Gestione degli Audit
  - Recovery

Come ottenere un sistema sicuro

- Fasi
  - Specifica: descrizione del funzionamento desiderato del sistema
  - Progetto: traduzione delle specifiche in componenti che le implementeranno
  - Implementazione: creazione del sistema che soddisfa le specifiche

- E' indispensabile verificare continuamente la correttezza dell'implementazione

Considerazioni implementative

- Analisi costi-benefici della sicurezza
- Analisi dei rischi (valutare le probabilità di subire attacchi e i danni che possono causare)
- Aspetti legali (ad esempio uso della crittografia negli USA) e morali
- Problemi organizzativi (ad esempio la sicurezza non "produce" nuova ricchezza, riduce solo le perdite)
- Aspetti comportamentali delle persone coinvolte

Cosa vedremo nelle prossime lezioni

- Panoramica di alcuni dei principali *meccanismi*
  - Crittografia, firma digitale, controllo degli accessi, autenticazione, …
- Qualche esempio di possibile *attacco*
  - Oggetto dell'esercitazione di laboratorio
- Cosa NON vedremo
  - Come i meccanismi possono essere usati per creare una politica di sicurezza