Introduzione ai problemi di sicurezza nei sistemi informatici

rif.:
C.P. Pfleeger & S.L. Pfleeger, Sicurezza in informatica, Cap.1
D. Gollmann, Computer Security, Capp. 1, 2

Giuseppe Scollo

Corso di Laurea in Informatica applicata
Università di Catania, sede di Comiso (RG)

6 marzo 2008

Sommario

Problemi tradizionali di sicurezza
cosa significa “sicuro”?

- tradizionalmente, il problema della sicurezza riguarda la **protezione** di
  - **persone** da aggressioni fisiche
  - **beni materiali** dall’appropriazione indebita
  - **informazioni** riservate da accessi indesiderati

  per ciascuna delle tre possono richiedersi le altre
- in passato, tipiche **difficoltà** al riguardo, causate da
  - **tecnologie rudimentali**
    di allarme, identificazione, trasporto, comunicazione
  - **inevitabilità del contatto fisico**
    per il trasferimento di beni materiali o informazioni
  - frequente **sottovalutazione** del problema. . .

    . . . fenomeno ancora attuale!

Problemi di sicurezza dei sistemi informatici
cosa significa “sicuro” per un sistema informatico?

- **sottovalutazione** del problema spesso dovuta a
  - **sottostima del danno** provocabile da intrusioni
  - **timore del danno all’immagine**
    associato alla denuncia di un crimine informatico subìto
  - **carenze legislative** in materia di
    protezione del *diritto di proprietà dell’informazione*
- nel seguito si prendono in esame
  - i **rischi** di sicurezza nei sistemi informatici
  - le **contromisure e controlli** disponibili
  - le **vulnerabilità** dei sistemi informatici
  - le **aree di ricerca** tuttora aperte in proposito
- **intrusione nei sistemi informatici**:
  grande varietà di: bersagli, tipi di attacchi, vulnerabilità

  principio della penetrazione più facile

Attacco e difesa: concetti di base
vulnerabilità, minaccia, controllo

- **attacco**: sfruttamento di una vulnerabilità del sistema per ottenere senza autorizzazione
  - **accesso a**, o
  - **modifica di**, o
  - **blocco di**

  componenti HW/SW del sistema o **dati** contenuti in essi
- una **vulnerabilità** del sistema è una sua *lacuna rispetto a requisiti di sicurezza*
- le vulnerabilità di un sistema informatico sono fonti di **minacce** alla sicurezza, cioè di *circostanze che possono causare perdita, danno o blocco di componenti e/o dati*

si fronteggiano le minacce alla sicurezza attraverso il **controllo** delle vulnerabilità da cui esse hanno origine

Vulnerabilità, minaccia, controllo
un esempio illustrativo

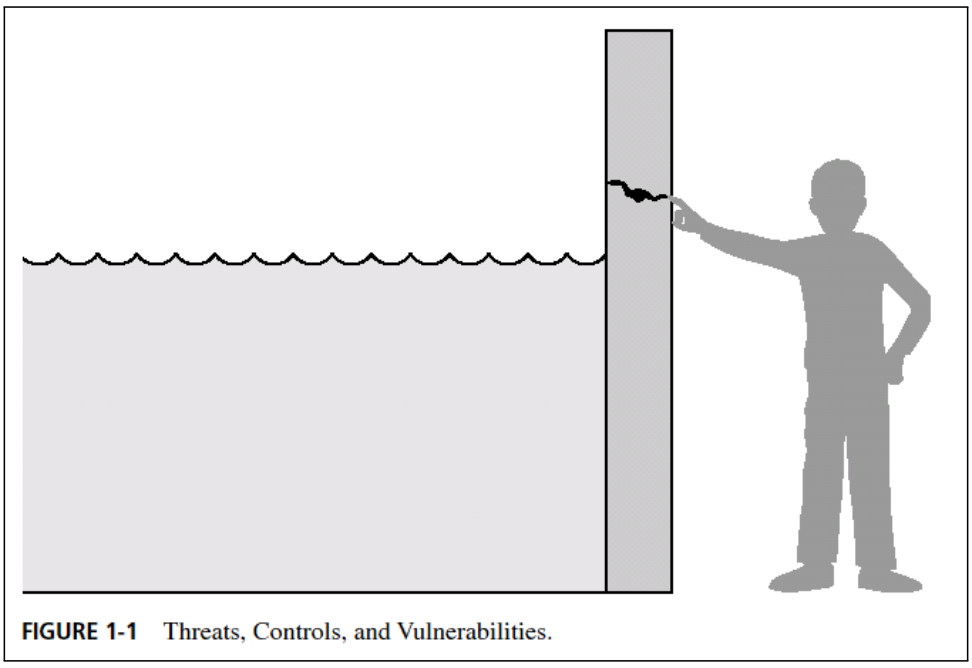

FIGURE 1-1 Threats, Controls, and Vulnerabilities.

Minacce alla sicurezza di sistema
intercettazione, interruzione, modifica, contraffazione

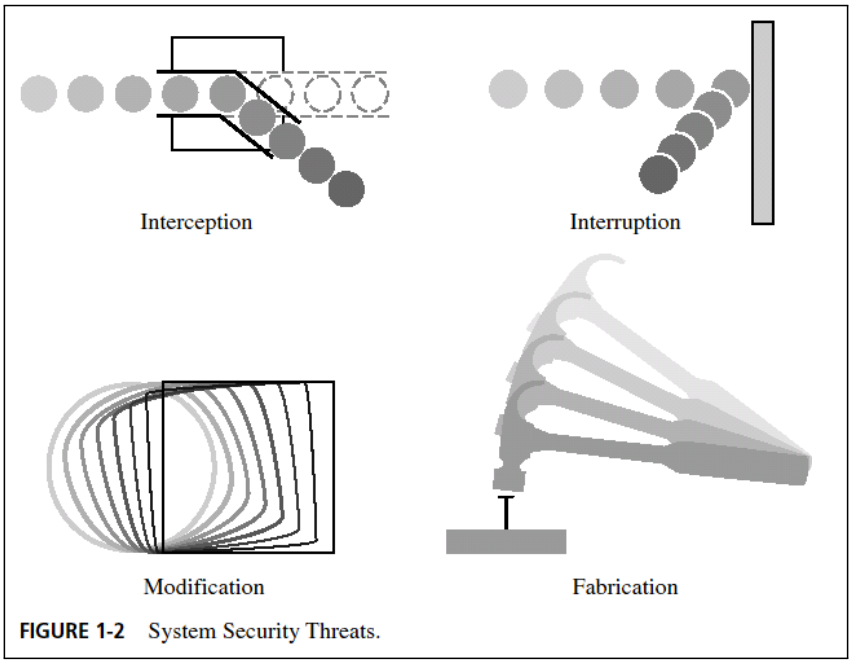

FIGURE 1-2 System Security Threats.

Condizioni necessarie all'attacco
metodo, opportunità, motivo (MOM)

un attaccante deve disporre di

- **metodo**:
  abilità, conoscenze e strumenti necessari all'attacco
- **opportunità** di accesso al sistema
- **motivo** per condurre l'attacco

condizioni **tutte necessarie**
alla messa in opera dell'attacco, *però*. . .
tutte *inerentemente* **difficili da contrastare!**

Proprietà caratteristiche della sicurezza
riservatezza, integrità, disponibilità

riservatezza: **accesso riservato** solo a parti autorizzate

- *sinonimi* frequenti: **segretezza, privacy**
- significato dipendente da quella di *accesso*:
  - visibilità
  - lettura
  - conoscenza dell'esistenza

integrità: **modifica riservata** solo a parti autorizzate

molteplici significati, dipendenti dall'*oggetto* e dal *contesto*

disponibilità: **garanzia di servizio** alle parti autorizzate

- molteplici aspetti, anche *prestazionali*
- area di *ricerca* nello studio della sicurezza

Relazione tra caratteristiche di sicurezza
minacce e contromisure specifiche

attacchi alla

riservatezza:

indebito accesso

integrità:

indebita modifica

disponibilità:

diniego di servizio

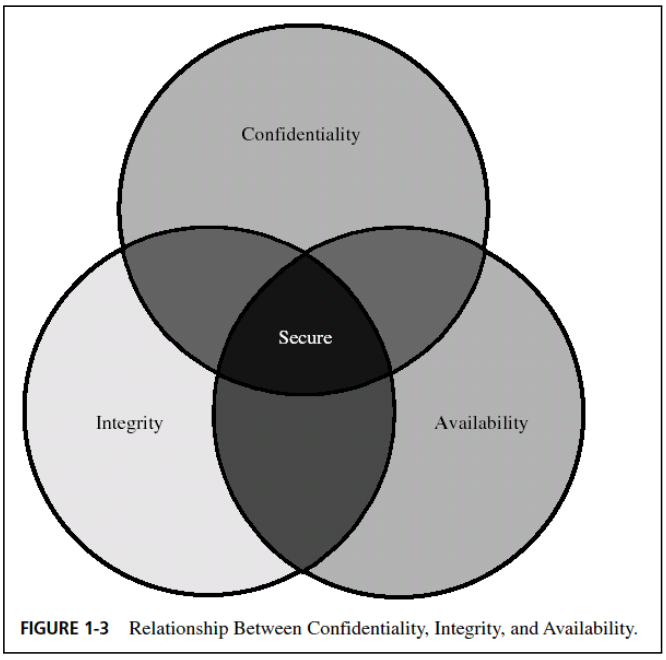

FIGURE 1-3 Relationship Between Confidentiality, Integrity, and Availability.

Vulnerabilità dei sistemi informatici
un quadro generale

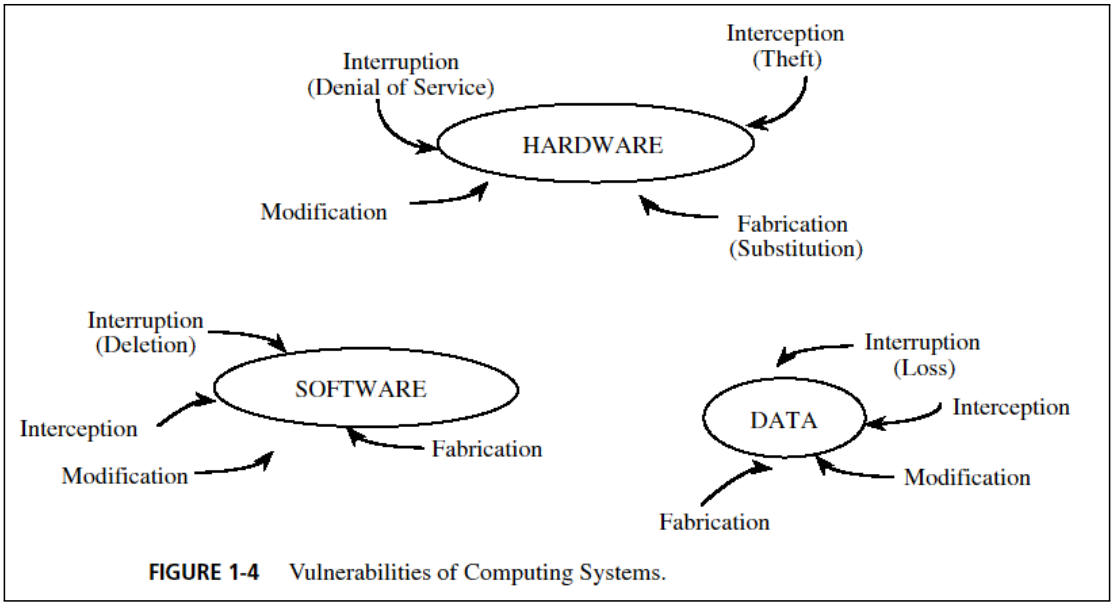

FIGURE 1-4 Vulnerabilities of Computing Systems.

Vulnerabilità hardware
esposizione a...

- **minacce intenzionali**, *e.g.*:
  - **furto** di componenti, dispositivi, sistemi
  - **sabotaggio** del funzionamento, fino alla *distruzione*
  - **sostituzione o aggiunta** di componenti o dispositivi
  - **intercettazione** del flusso di informazione
  - **sovraccarico** di traffico $\Rightarrow$ *diniego di servizio*
- **minacce non intenzionali**, *e.g.*:
  - alterazione di condizioni operative **ambientali** (temperatura, umidità, alimentazione elettrica, etc.)
  - commistione con **materiali dannosi** (polvere, fumi, bevande, olio, etc.)
  - **usura** dei materiali
  - intrusione di **roditori**
  - **errori** tecnici, uso di **strumenti impropri**

Vulnerabilità software
facilità di...

- **cancellazione**: lacune nel (o assenza di)
  - sistema di **backup** periodico
  - **controllo di versione**,
    parte della più generale **gestione delle configurazioni**
- **modifica** $\Rightarrow$ arresto o (mal)funzionamento [improprio]
  - **bomba logica**
  - **cavallo di Troia**, **virus**
  - **trapdoor**
  - **falla informativa**
  - **modifica di sistema** $\Leftarrow$ carenza di controllo
    su installazione e/o esecuzione di programmi
- **furto**
  - più precisamente: **copia** non autorizzata,
    violazione del *diritto di proprietà intellettuale*
  - si discute di: *copyright*, brevetti, *copyleft*...

Vulnerabilità dei dati
... $\Rightarrow$ le minacce più serie

valore dei dati?

- intrinseco: *nullo*
- in contesto:
  di *difficile misura!*
  - **costo** di ricostruzione,
    in caso di perdita
  - **danno** per intercettazione,
    modifica, indisponibilità

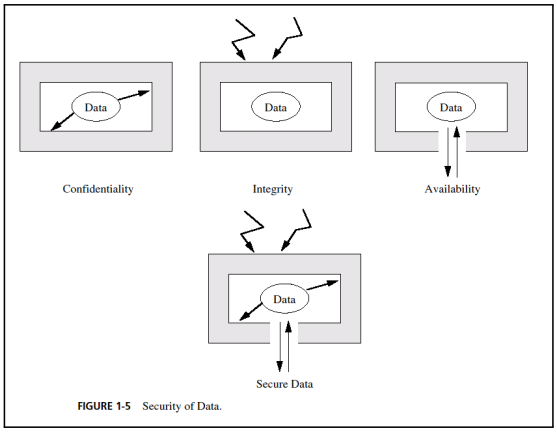

FIGURE 1-5 Security of Data.

di *durata limitata*: $\Rightarrow$ **principio di adeguata protezione**

altre fonti di vulnerabilità: *reti, accessi, persone-chiave*

Crimine informatico
una definizione molto ampia...

crimine che riguarda un sistema informatico o messo in opera con l'ausilio di uno

- definizioni migliori richiedono la precisazione del concetto di *norma sui sistemi informatici*, ad es:

  violazione di norma penale sui sistemi informatici
- inesistenza di **statistiche** sul crimine informatico
- tuttavia, fenomeno di crescente **rilevanza sociale**, per la rapida diffusione dell'informatica nella vita quotidiana
- chi sono i *"criminali informatici"*?

Criminali informatici
tipologie e caratteristiche

- **dilettanti**
  - *maggioranza* degli autori di crimini informatici noti
  - "criminali per caso"
  - *motivazioni*: vantaggio personale, ripicca, ...
- **crackers** (non "*hackers*"!)
  - perpetrano *accesso non autorizzato*
  - *motivazioni* come sopra, inoltre:
    gusto della trasgressione, delirio di onnipotenza, ...
- **criminali professionisti...**
  - ...in altri "settori" del crimine
    scoprono opportunità e prospettive nel crimine informatico
  - problema sociale: *timore del danno all'immagine*
    associato alla denuncia di un crimine informatico subìto

Obiettivi della difesa
disposti in cascata...

- fronteggiare i **rischi di attacchi** alla sicurezza con misure:
  - **di prevenzione** dell'attacco
    e.g. rimozione di vulnerabilità
  - **deterrenti**, rendendo l'attacco più *arduo*
  - **devianti**, spostando il bersaglio
  - **di rivelazione** dell'attacco, non appena avviene o dopo
  - **di ricupero** dagli effetti dell'attacco (avvenuto)
- mettere in opera e coordinare **controlli multipli** di sicurezza, scelti in base a
  - valore del **bersaglio**
  - rapporto **costi/benefici** dei controlli
  - maggior onere causato dai controlli all'**attaccante**

Controlli di sicurezza
Controlli multipli

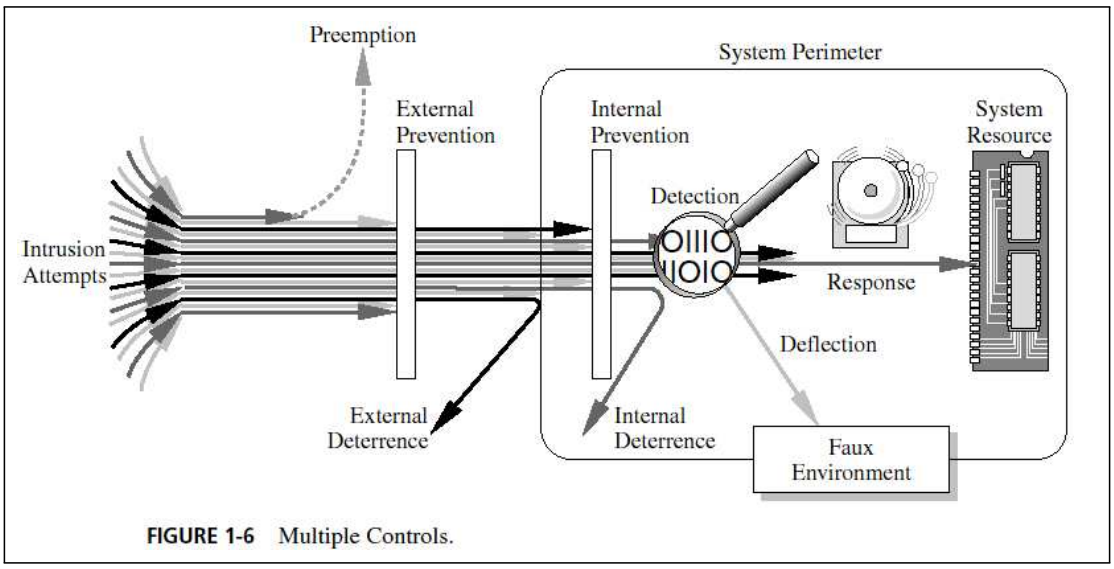

FIGURE 1-6 Multiple Controls.

Tipi di controllo
controlli crittografici, ma non solo...

- **codifica crittografica**
  - *trasformazione* dei dati che li rende intellegibili solo attraverso una trasformazione inversa, di **decodifica**, controllata da informazione disponibile solo agli autorizzati

    $$\texttt{in chiaro} \xrightarrow{e_k} \texttt{cifrato} \xrightarrow{d_k} \texttt{decifrato}$$

  - protegge non solo i *dati* ma anche il *software*
  - spesso realizzata in *hardware* per efficienza prestazionale
  - protegge *riservatezza, integrità* e *disponibilità*, dunque
  - **fondamentale** per la sicurezza dei sistemi informatici
- **software**: *interni* ai programmi, di *sistema* o di *rete*, *autonomi*, di *sviluppo* (controlli di qualità)
- **hardware**: crittografici, rivelatori, biometrici, ...
- **procedurali**: basati su *politiche* e *consenso sociale*
- **fisici**: meccanici, repliche, *site planning*, ...

Efficacia dei controlli di sicurezza
la sola predisposizione di controlli non basta...

- occorre **consapevolezza del problema** di sicurezza prerequisito perché i controlli siano *effettivamente in uso*

  principio di efficacia dei controlli

- **sovrapposizione** di controlli:
  - può compensare eventuali inefficacie di singoli controlli
  - altrimenti detta **difesa stratificata**
  - OK, però...

  principio dell'anello più debole

- **revisione periodica** dell'efficacia dei controlli

Esercizi
controllo della comprensione e dell'apprendimento

1. Distinguere fra vulnerabilità, minaccia, controllo.
2. Si considerano vari tipi di danni, ad es. a seguito di un furto: perdita economica, disagio pratico, sconvolgimento emotivo. Identificare almeno tre tipi di danni che un'azienda può soffrire a seguito del furto di apparecchiature informatiche.
3. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia alla riservatezza di suoi dati.
4. Identificare almeno tre tipi di danni potenziali per un'azienda che derivano da una minaccia all'integrità di programmi o dati.
5. Fornire due esempi di vulnerabilità in automobili per le quali i costruttori hanno installato controlli; esprimere un giudizio sull'efficacia di tali controlli: buona, parziale, nulla.

Problemi
applicazioni dei concetti proposti

8. **Ipotesi**: un programma di stampa degli assegni stipendiali erogati da un'azienda rende ogni mese segretamente accessibile a non autorizzati una lista degli addetti che ricevono più di un ammontare prefissato.
   Problema: escogitare controlli per limitare tale vulnerabilità.

17–20, **Ipotesi**: considerare un programma che

17. visualizza sul proprio sito web personale l'ora e la temperatura nella propria città;
18. permette a consumatori di ordinare prodotti via web;
19. accetta e tabula voti elettorali;
20. permette a un chirurgo di operare da postazione remota su un paziente attraverso una connessione Internet.

17–20, **Problema**: in ciascuna delle ipotesi proposte sopra

- Chi potrebbe voler attaccare il programma?
- Che tipi di danni potrebbe voler causare?
- Che genere di vulnerabilità potrebbe sfruttare a tale scopo?