Sicurezza in Informatica

Definizione di sicurezza

- Per sicurezza si intende la protezione delle risorse
- Possibili pericoli
  - danneggiamento involontario (*e.g.* inesperienza)
  - danneggiamento fraudolento (*e.g.* virus)
  - furto o alterazione (*e.g. cracker*)

Panoramica

- Singolo utente
  - i calcolatori portatili fanno eccezione!
- Più utenti
  - su un singolo calcolatore
  - in Rete

Sicurezza per il singolo utente

- I dati possono essere danneggiati
  - usura dei supporti o incidenti
  - manomissioni
- Le informazioni più importanti sono i documenti personali
  - cancellazione
  - sovrascrittura

Copie di salvaguardia (backup)

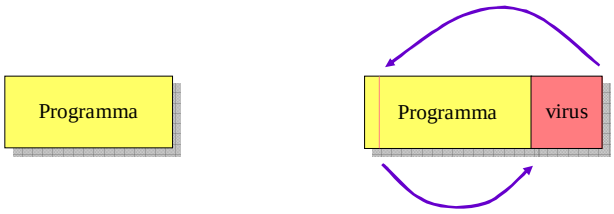
- Completo
- Differenziale
  - le differenze rispetto all'ultima versione
- Incrementale
  - le differenze rispetto all'ultimo *b.* differenziale

I virus

- Un virus è un programma in grado di auto-replicarsi autonomamente
- Possibili danni
  - occupazione di memoria
  - ...
  - danneggiamento dell'*hardware*

I virus propriamente detti

- Modificano i programmi in modo da essere eseguiti
- Si nascondono anche tramite “mutazioni”



Anti-virus

- Esistono programmi per controllare la presenza di virus ed eliminarli
  - in certi casi estremi i programmi infetti non possono essere recuperati
  - è importante tenere aggiornate le definizioni
  - è importante pianificare periodicamente scansioni complete

Sicurezza per più utenti

- Aspetti della sicurezza per più utenti
  - identificazione e autenticazione: *login* e *password*
  - autorizzazione: permessi
  - integrità: codici di controllo, crittografia
  - sorveglianza: *logging* (resoconti)

Identificazione e autenticazione

- Ogni utente viene identificato da un profilo
  - nome
  - *password*
- La *password* non deve essere scoperta
  - deve essere più lunga possibile
  - deve essere difficile da indovinare
  - dovrebbe essere cambiata abbastanza spesso

L'amministratore e i permessi

- Ogni Sistema Operativo multi-utente
  - prevede almeno un (utente) amministratore
  - gestisce le autorizzazioni tramite permessi
- L'amministratore
  - può accedere a tutte le risorse
  - se non è esperto può quindi rovinare il S.O.!

I permessi

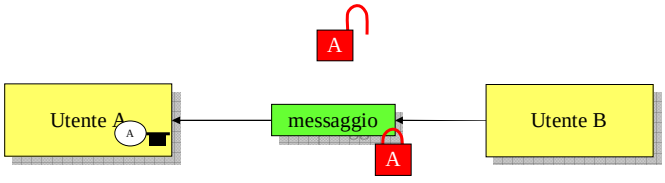
- Ogni risorsa del calcolatore ha un permesso
  - *file*: lettura, scrittura, esecuzione, ...
  - cartelle: lettura, scrittura, consultazione, ...
  - altre risorse: stampanti, modifica di parametri, ...

Crittografia simmetrica

- Quando la stessa *password* è usata sia per criptare sia per decriptare
  - comoda per uso personale
  - non molto sicura
  - problema della distribuzione delle chiavi

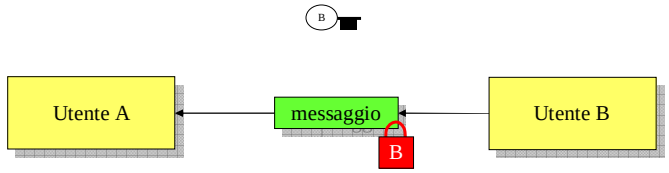
Crittografia asimmetrica

- Ci sono due chiavi, una privata e una pubblica, per ciascun utente
  - il mittente B usa la chiave pubblica di A
  - solo A riuscirà a decifrare il messaggio di B



Integrità: la firma digitale

- Per firmare un documento
  - B usa la propria chiave privata
  - solo usando la chiave pubblica di B si riuscirà a decifrare la firma



Steganografia

- Usa la segretezza per rafforzare la sicurezza
- Può nascondere dati in un documento qualsiasi
  - immagine: 14 KB
  - immagine e testo: 21 KB – nessuna differenza visibile

Sicurezza in Rete

- *worm* e *spyware*
- I *firewall*
- *Social engineering*

Worm e spyware

- I *worm* sfruttano le falle del Sistema Operativo per diffondersi in Rete
  - allegati di posta elettronica (Outlook soprattutto)
  - errori nei programmi (*e.g.*: P2P)
- Gli spyware abbassano le difese del S.O.
  - si fanno passare per programmi innocui

I firewall

- Proteggono un calcolatore dagli attacchi regolandone i servizi di Rete
- Controllano gli accessi da e verso il calcolatore
  - connessioni in entrata (intrusioni)
  - connessioni in uscita (furto di informazioni)

Social Engineering

- Tentativo di carpire informazioni protette
  - *email* contraffatte
  - siti fraudolenti
  - false credenziali
- Precauzioni
  - allegati sicuri
  - protocollo HTTPS