

ELEMENTI DI SICUREZZA INFORMATICA

Ferrara 13 dicembre 2002

Classificazione dei rischi per la
sicurezza

- **Rivelazione di informazioni
confidenziali**
- **Accessi non autorizzati**
- **Interruzioni di servizio**

Motivazioni degli attacchi alla sicurezza

- Spionaggio industriale
- Guadagno economico
- Vendetta
- Scopo ludico
- Pubblicità

Funzioni di un sistema di sicurezza

- Identificazione
- Autenticazione
- Autorizzazione
- Controllo accesso
- Riservatezza
- Integrità dati
- Non ricsuzione

Identificazione

- *In un sistema le applicazioni sono in grado di identificare gli utenti in base ad un identificativo utente o User ID che determina il diritto o meno all'uso del programma o l'accesso alle informazioni*

Autenticazione

- È il procedimento utilizzato per verificare l'identità dell'utente
- Richiede lo scambio di informazioni segrete tra utente e applicazione, generalmente password

- Nell'autenticazione ad una via solo l'utente è autenticato dall'applicazione
- Nell'autenticazione a due vie anche l'applicazione deve autenticarsi all'utente

-
- materiali** alfabettizzazione nuovi Properties
- General | **Sharing** | Security
- ☒ Share this folder
- Share name:
- Agd...
- Remove
- Permissions:
- | | Allow | Deny |
|----------------------|-------------------------------------|--------------------------|
| Full Control | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Modify | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read & Execute | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| List Folder Contents | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Read | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
| Write | <input checked="" type="checkbox"/> | <input type="checkbox"/> |
- Advanced...
- Additional permissions are present but not viewable here. Press Advanced to see them.
- ☒ Allow inheritable permissions from parent to propagate to this object
- OK Cancel Apply

Controllo accesso

- Procedimento che consente all'utente di utilizzare la propria autorizzazione per accedere alle risorse di rete
- Viene usato per consentire o negare l'accesso ad una determinata risorsa
- È impostato dall'amministratore di sistema o dal proprietario della risorsa

Controllo d'accesso (segue)

- Devono essere indicati:
 - ☐ Gli utenti che possono accedere alla risorsa
 - ☐ Le modalità di accesso
 - ☐ I periodi in cui l'accesso è consentito
 - ☐ Le condizioni di accesso

Riservatezza

- È la funzione utilizzata per impedire la rivelazione di informazioni riservate.
- Tale protezione deve operare sia durante le operazioni di memorizzazione sia durante la trasmissione in rete

Integrità dati

- Tale funzione permette di rilevare modifiche non autorizzate apportate ai dati

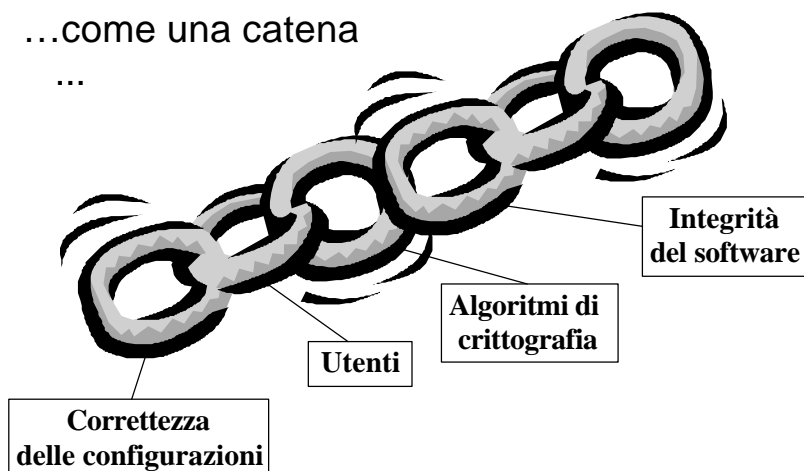
Non riconsuazione

- Tale funzione permette di dimostrare l'origine o la destinazione dei dati
- Impedisce a chi invia dati di negare di averli inviati
- Impedisce a chi riceve i dati di negare di averli ricevuti
- Usata spesso nelle transazioni commerciali via Internet

La “sicurezza” informatica è ...

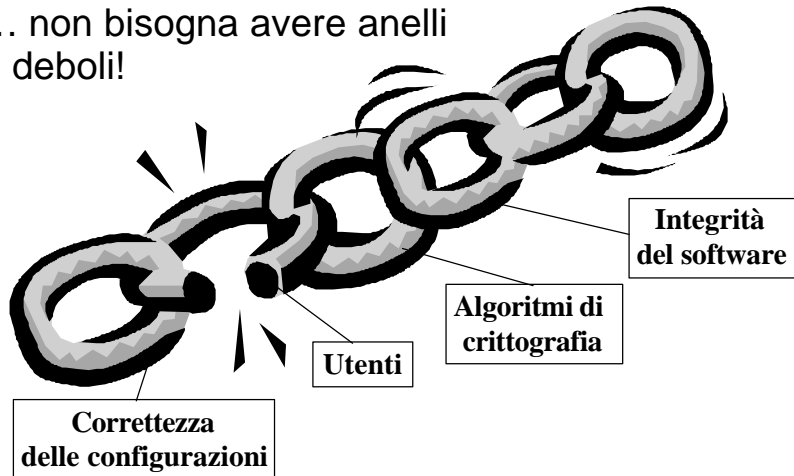
...come una catena

...



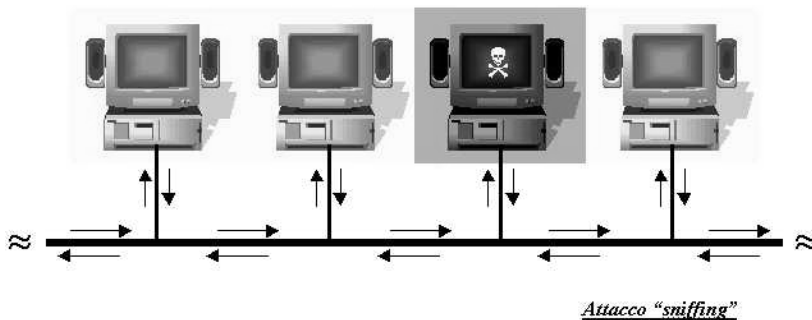
... non importa avere anelli molto forti ...

... non bisogna avere anelli deboli!



Tipologie di attacchi ai protocolli TCP/IP

- Attacchi passivi (es. sniffing)



Tipologie di attacchi ai protocolli TCP/IP

■ Attacchi attivi (es. web-spoofing)



Differenze tra i metodi di attacco

- Gli attacchi passivi sottraggono informazioni senza interferire sul sistema.
- Gli attacchi attivi interferiscono sui sistemi con diversi scopi: DoS, spoofing, bridging ecc.

Soluzioni per utenti finali contro gli attacchi informatici

- Controllo dell'integrità delle applicazioni (bugs free) e verifica della correttezza delle configurazioni
 - ☐ Utilizzare software originale!!!
 - ☐ Verificare che la configurazione standard di installazione del sistema operativo e dei programmi non sia troppo "permissiva"
- "Manutenzione" del software con download periodico (controllo settimanale) di patch e eventuali Service pack per il sistema operativo e le applicazioni
 - ☐ Windows <http://windowsupdate.microsoft.com>
 - ☐ Office <http://office.microsoft.com/ProductUpdates>

Soluzioni per utenti finali contro gli attacchi informatici (segue)

- Utilizzo di software che controllino e limitino il traffico di rete dall'esterno verso l'interno e viceversa (ad es. firewall software gratuiti per uso personale)
 - ☐ ZoneAlarm <http://www.zonealarm.com>
 - ☐ Tiny Personal Firewall <http://www.tinysoftware.com>
 - ☐ Sygate Personal Firewall <http://soho.sygate.com/>
- Utilizzo di antivirus aggiornati **settimanalmente**
 - ☐ Norton Antivirus
 - ☐ McAfee antivirus
 - ☐ E-Trust EZantivirus