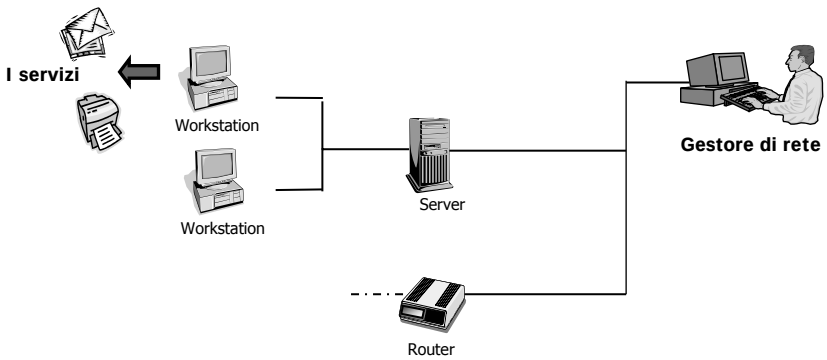
Università di Firenze
Dipartimento di **E**lettronica
e **T**elecomunicazioni

La gestione di rete OSI

pecos,giada@lenst.det.unifi.it

Cosa e come gestire ?

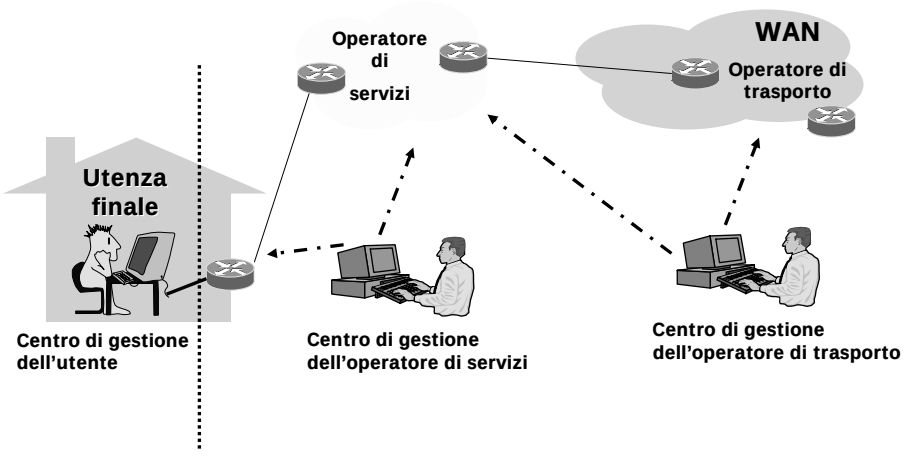


Cosa e come gestire ?

Si possono avere vari livelli di gestione di rete :

- Gestione di rete di backbone (operatore di TLC)
  - **apparati Frame Relay, ATM, SDH, ottici: usano protocolli proprietari x trasporto info e gestione/segnalazione in WAN**
  - **IP e Gbit Ethernet sempre più usati, dunque gestione più "open source", soprattutto agli edge della rete di dorsale (MAN, accesso)**
- Gestione di rete locale (LAN system administrator)
  - **IP, Ethernet, WLAN**
  - **Linux sempre più usato x gestire rete & servizi**

Domini di competenza



Come gestire una rete?

Gestire un insieme complesso di risorse di rete significa:

- Far funzionare correttamente e in modo sicuro la rete
- Configurare opportunamente accessi e apparati
- Fare campagne di monitoraggio della funzionalità e delle prestazioni della rete
- soddisfare le richieste degli utenti (sia in WAN che in LAN)

Gestione di rete OSI e Internet

- **<u>Approccio ISO/OSI</u>:**
  - **definizione di 5 aree funzionali di gestione di rete,**
  - **Gestione distribuita,**
  - **maggiore complessità sugli elementi di rete da gestire.**
- **<u>Approccio IETF</u>:**
  - **protocollo semplice di gestione (SNMP: 1988 primo draft, 1998 SNMPv3)**
  - **gestione centralizzata,**

Aree funzionali del MGMT OSI

1. **Configuration**
2. **Fault**
3. **Accounting**
4. **Performance**
5. **Security**

Configuration Management

- Inizializzazione, monitoraggio e modifica delle informazioni di configurazioni degli apparati
  - In considerazione della topologia della rete
- Nell'accezione comune comprende inoltre problematiche di
  - Network Provisioning

Fault Management

- Coinvolge un processo di 5 passi:
  1. Rilevazione del guasto
     - Polling
     - Trap
  2. Localizzazione e isolamento del guasto
     - Approccio semplice
     - Approccio a correlazione di eventi
     - Trouble Ticket
  3. Riattivazione del servizio
  4. Identificazione della causa del problema
     - Automatica
     - Tramite operatore
  5. Risoluzione del problema
     - Test operativi

Accounting Management

- Determinazione/modifica dei diritti e caratteristiche di accesso al servizio, in base al contratto stipulato
- Billing dei servizi – addebitamento dei costi agli utenti finali
  - Analisi dell'utilizzo della rete

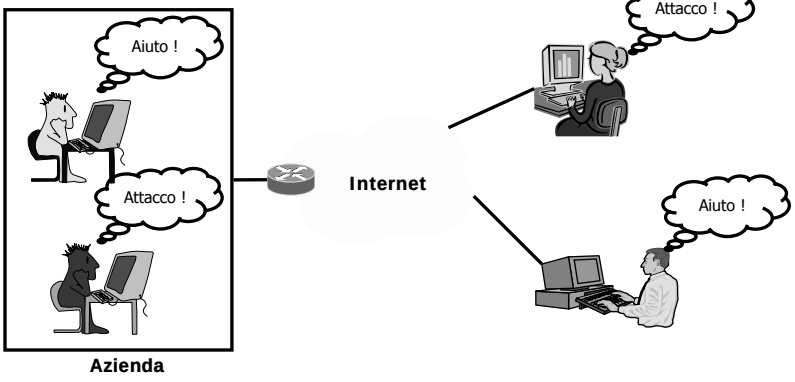
Performance Management

- Monitoraggio delle prestazioni della rete, in base alle specifiche contenute nel Service Level Agreement con il cliente
- Log delle prestazioni monitorate e report agli utenti finali
- Adozione di misure preventive per evitare situazioni di congestione o di disservizio

Security Management

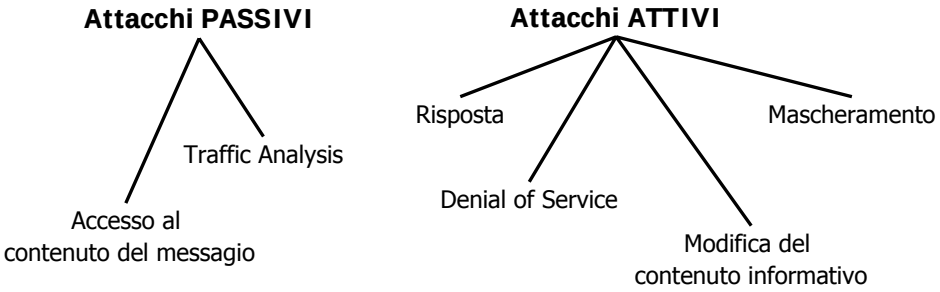
- Definizione di piani per la sicurezza aziendale, sia fisica che di rete.
  - Integrità
  - Reperibilità
  - Riservatezza
- Garantire il rispetto per l'accesso alle risorse della rete
  - Gestione delle autorizzazioni

Sicurezza



Sicurezza

Possibili attacchi:



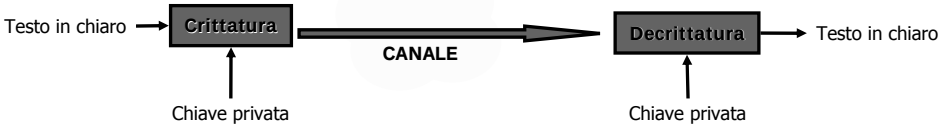
Crittografia

- Cifratura a Trasposizione
  - *Cifratura a permutazione* su un periodo fisso d
    Messaggio in chiaro $M=m_1m_2.....m_d$
    Messaggio cifrato $E_k(M)= m_{f(1)}m_{f(2)}.....m_{f(d)}$
- Cifratura a Sostituzione
    Messaggio in chiaro $M=m_1m_2.....m_d$
    Messaggio cifrato $E_k(M)=f(m1)f(m2).....f(m_d)$
  - *Sostituzione semplice* (uno a uno)
    - Cifratura di Giulio Cesare
      $f(\rho)= (\rho+3) \bmod 26$
  - *Sostituzione omofonica* (uno a molti)
  - *Sostituzione polialfabetica*
  - *Sostituzione a poligramma*

Crittatura a chiave segreta

Cifratura simmerica, convenzionale o a chiave segreta.

- DES Data Encryption Standard
  - Chiave 56 bit
- TDES Triple Data Encryption Standard (1999)
- IDEA International Data Encryption Algorithm
  - Chiave 128 bit



Crittatura a chiave segreta

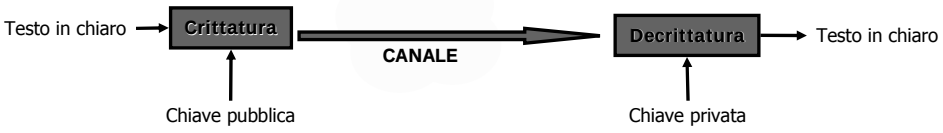
Lunghezza della chiave	Numero di chiavi	Tempo richiesto	Tempo richiesto
32		35.8 minuti	2.15 ms
56		1142 anni	10.01 ore
128		5.4+E24 anni	5.4+E18 anni
256		5.9+E36 anni	5.9+E30 anni

1 decrittatura / µs

1E+6 decrittature / µs

Crittatura a chiave pubblica

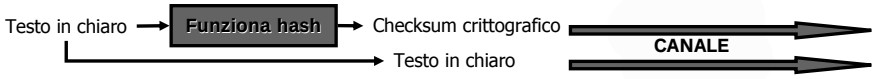
- RSA



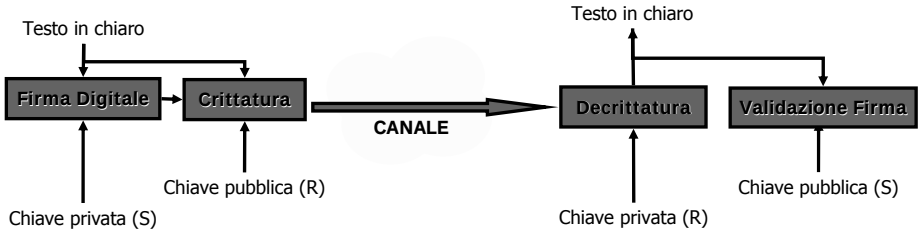
Message Digest

Protegge le informazioni da ogni modifica non autorizzata

- MD5 output 128 bit
- SHA-1 output 160 bit



Firma Digitale



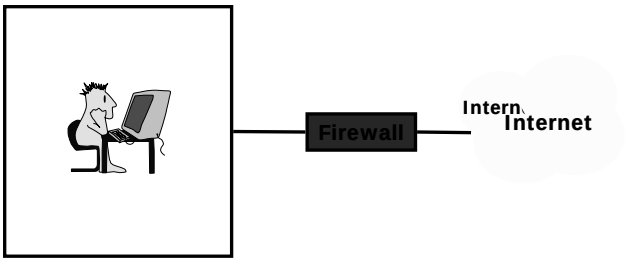
Autenticazione

- Password
- Tecniche biometriche
- Token
  - Smart card

Firewall

Dispositivo per il controllo del traffico in ingresso e uscita

- Firewall a filtraggio dei pacchetti
- Server proxy o gateway a livello applicazione
- Firewall a ispezione di stati



Bibliografia

- *"Network Management Principles and Practice"* Mani Subramanian
  Addison-Wesley

- *"Integrated Management of Networked Systems"* Heinz-Gerd Hegering, Sebastian Abeck, Bernhard Neumair
  Morgan Kaufmann