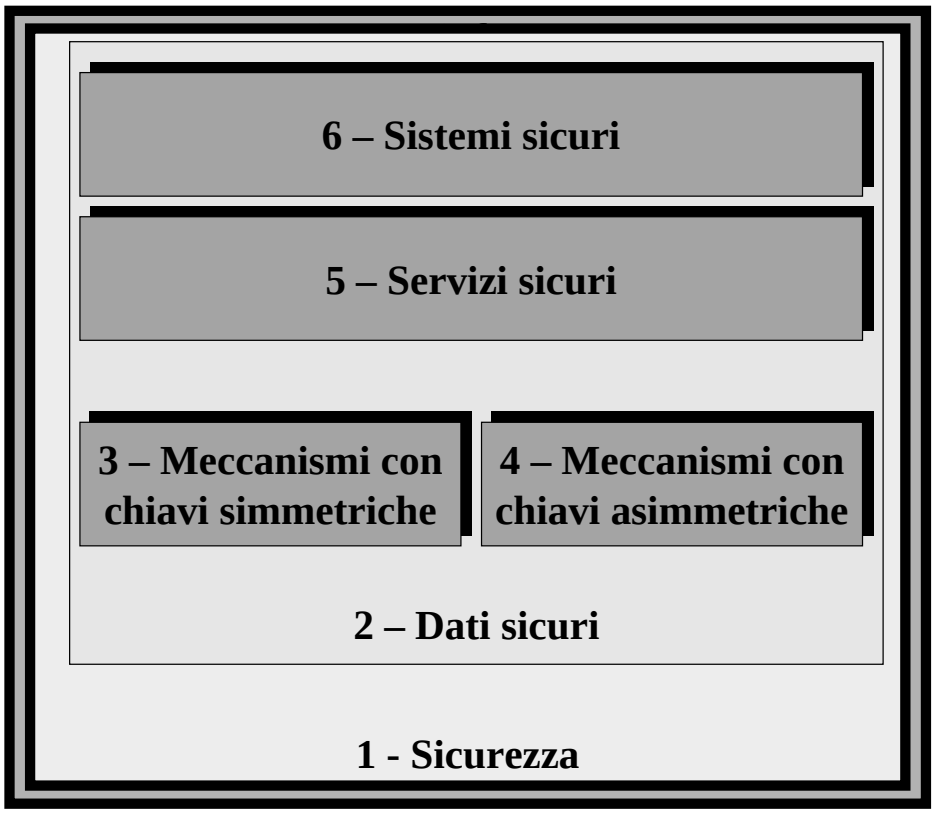
a.a. 2005 – 06

Lauree specialistiche in Ingegneria Informatica, Elettronica e delle Tlc.
Laurea in Ingegneria Informatica (vecchio ordinamento)

Tecnologie per la sicurezza

Rebecca Montanari
Dipartimento di Elettronica, Informatica e Sistemistica
rmontanari@deis.unibo.it

Programma



Riferimenti

Su tematiche di sicurezza:

1. A.J. Menezes, et.al: "*Handbook of Applied Cryptography*" CRC Press 1997 **www.cacr.math.uwaterloo.ca/hac**
2. H.C.A. van Tilborg: "*Fundamentals of Cryptology"* Kluver Academic Publishers 2000 **Lab 1, biblioteca DEIS, biblioteca Dore**
3. William Stalling: "*Crittografia e sicurezza delle reti. Standard, Tecniche, Applicazioni*" McGraw-Hill Italia 2003 **biblioteca DEIS, Dore**
4. R.Laschi, R. Montanari: Appunti di Tecnologie per la sicurezza" IIa edizione, Esculapio, 2006 (presso negozio Pitagora)

Su Java e sulla sua architettura per la sicurezza:

1. Philip Heller, Simon Roberts. "Java 2.0", Jackson Libri, 1999
2. Li Gong, et al. "Inside Java 2 Platform Security: Architecture, Api Design and Implementation". Addison Wesley , 2003

Ausili didattici

Sito del corso:
lia.deis.unibo.it/Courses/TecnologieSicurezzaLZ

- **Informazioni generali**
- **Laboratorio virtuale**

Modalità d'esame

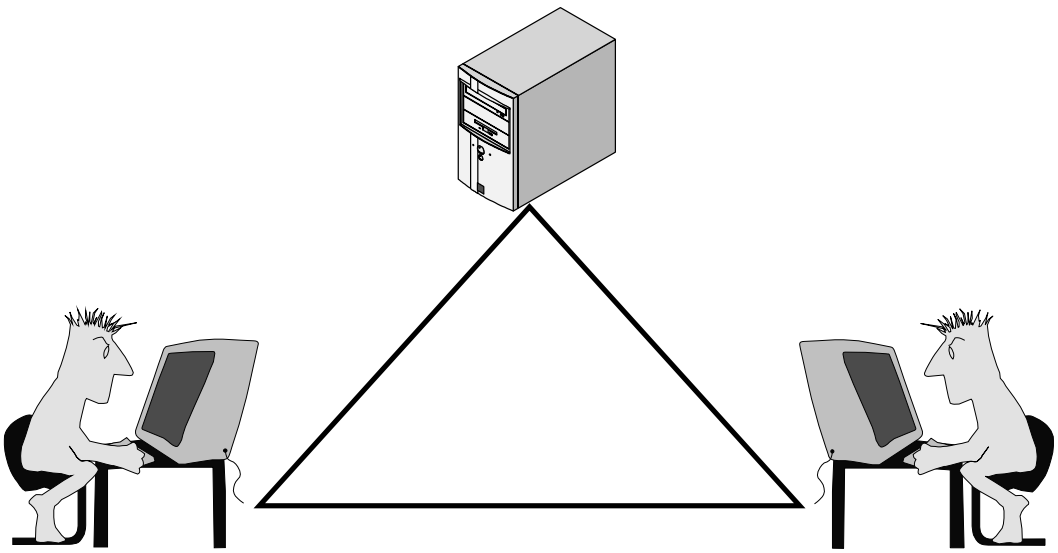
Prove scritte

- E-mail riservata (PGP)
- Sviluppo di un servizio sicuro (Java)

Prova orale

- Domande sul programma (Dispense)
- Approfondimento (Bibliografia, Internet)
- Discussione degli elaborati

Sicurezza

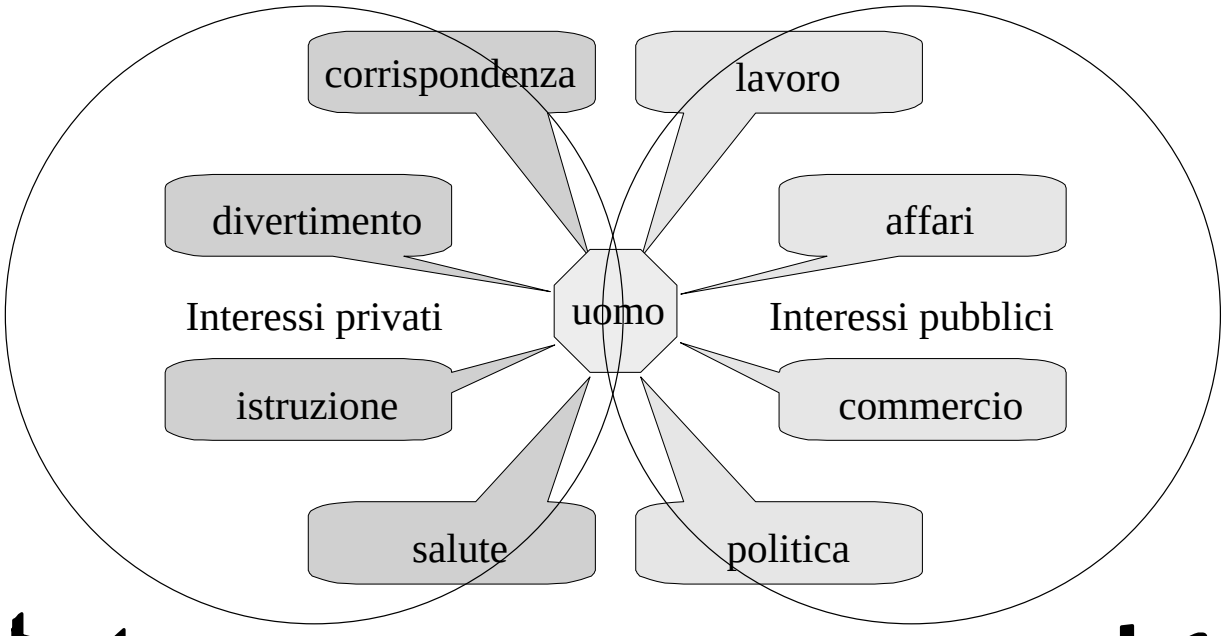


Sicurezza dell'informazione

1.1 Che cosa si intende?

1.2 Come si ottiene?

Finalità e forme di comunicazione

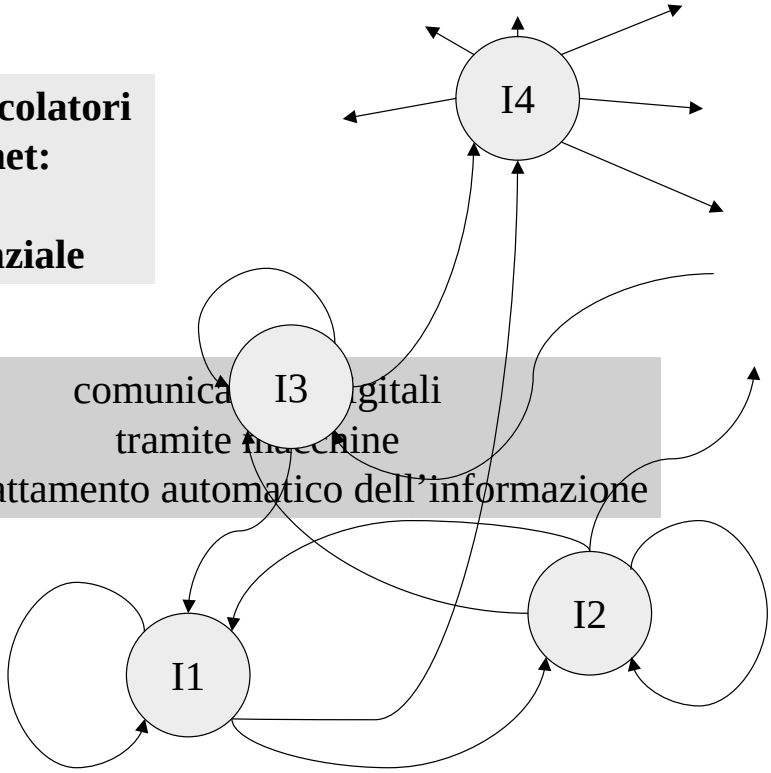


testo, voce, suono, disegno, immagine

Trattamento elettronico dell'informazione

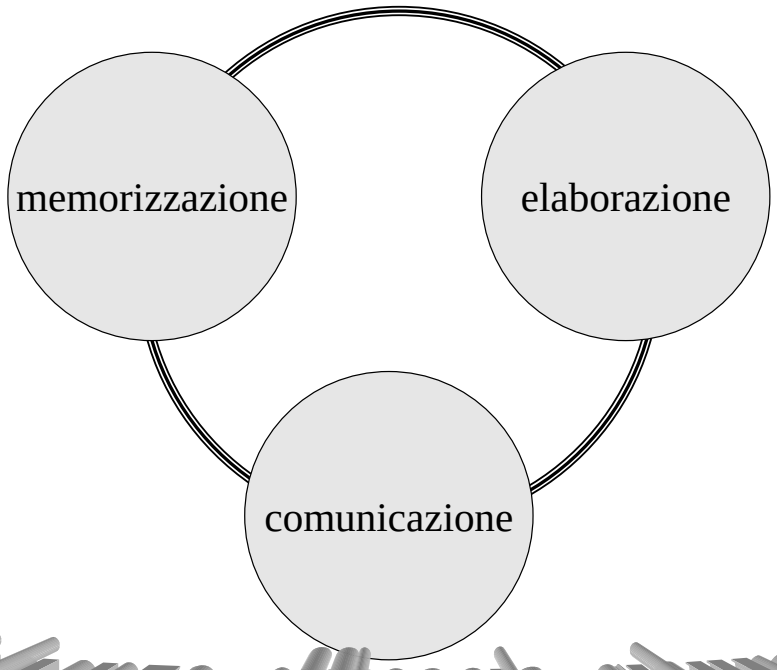
2002: $5 . 10^8$ calcolatori collegati a Internet:

Crescita esponenziale



comunicazione di dati digitali
tramite macchine
per il trattamento automatico dell'informazione

Fasi di vita dell'informazione



efficienza, efficacia, sicurezza

La Società dell'informazione

La **Società dell'informazione**

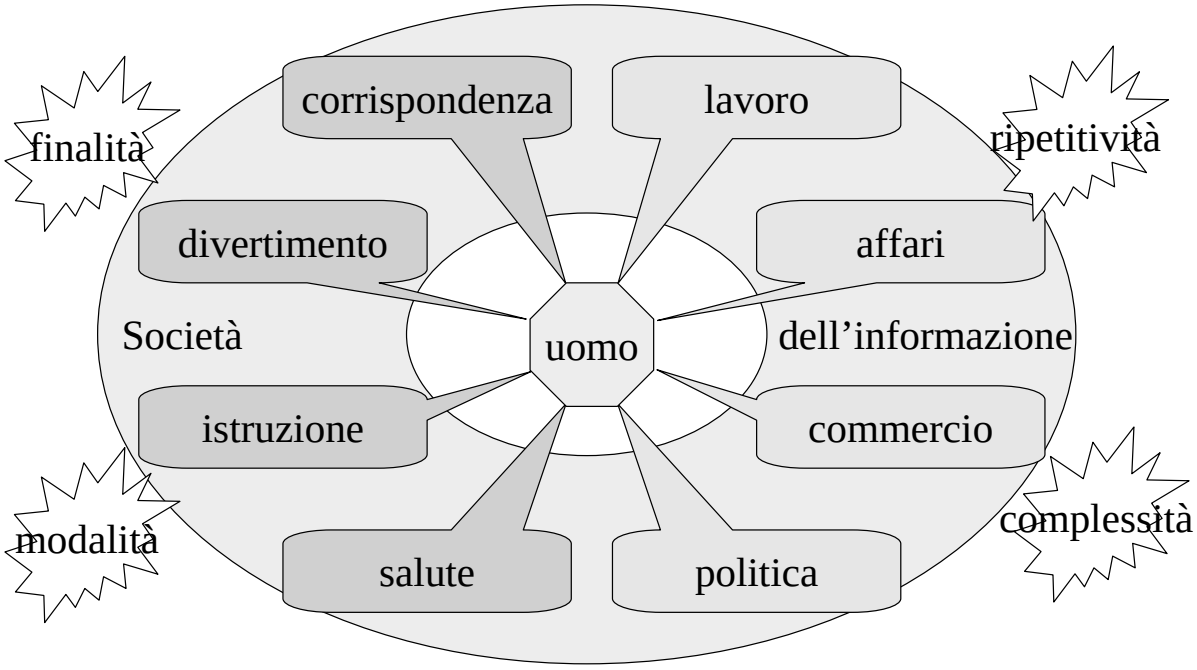
•**paradigma di vita**: nuovo bene

•**contesto sovranazionale**: nuove etiche e nuove leggi

•**struttura mondiale**: nuove macchine e nuovi tecnici

•**e ..**

.. servizi automatizzati



Tecnologie dell'informazione

- **codifica binaria**
- **hardware**
- **software**
- **rete di calcolatori**

La codifica binaria della informazione

n bit

b_1 b_2 b_3 ..... b_n

Rappresentazione dell'informazione

Alfabeto A:{a, b, c, …, p} con $|A| = M$

Stringa S: $\{s_1 s_2 s_3 \ldots s_N \mid s_i \in A\}$ con $|S| = M^N$ se N costante

Alfabeto dei numeri **:{0 1 2 … 9 + - }**
Alfabeto dei testi **:{a b .. z A B .. Z 0 1 .. 9 : ; . ' ? ! + - * / ( ) [ ] .. }**
Alfabeto della musica **:{do re mi fa sol la si}**

Alfabeto binario - B:{0,1}

A_{NUMERI}
A_{TESTI}
$A_{IMMAGINI}$
A_{SUONI}

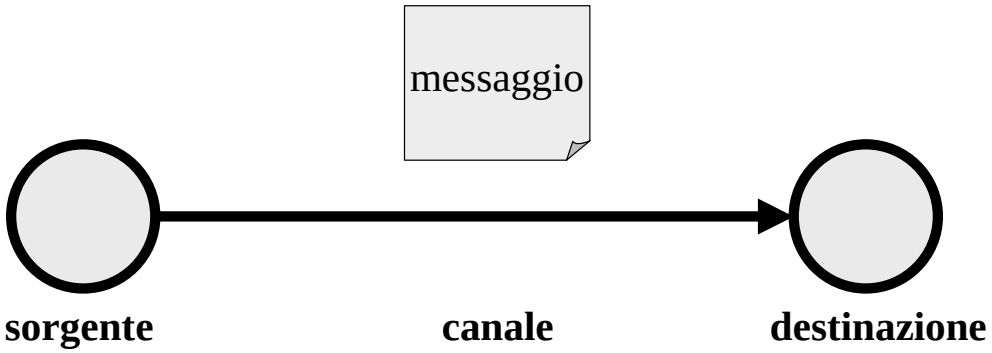
Codifica con n bit di M simboli
$M \leq 2^n$

UNICODE 16 bit — Colore del pixel 8 bit

interoperabilità standard

Stringhe di N×n bit

Comunicazione dell'informazione



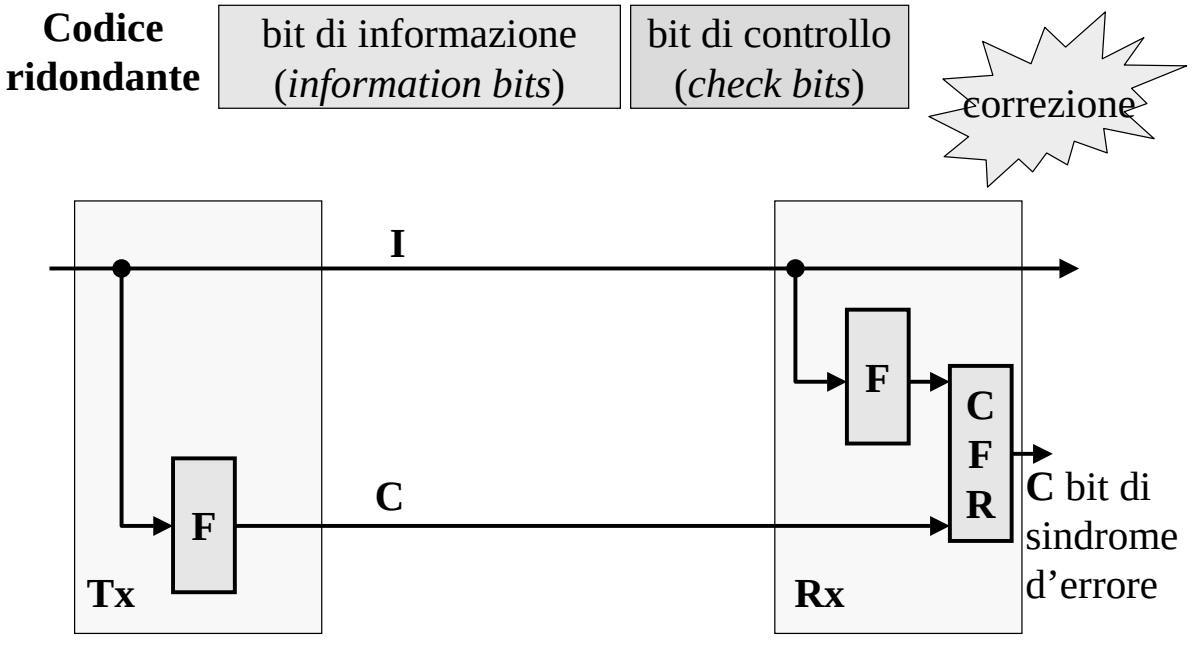
Canale: memoria, doppino, cavo, fibra, aria

Segnali: grandezze fisiche variabili nel tempo
trasmissione di bit in serie, in parallelo, in serie/parallelo

Protocolli: segnali, modalità, ritmo,distanza, mezzo, codice, controllo

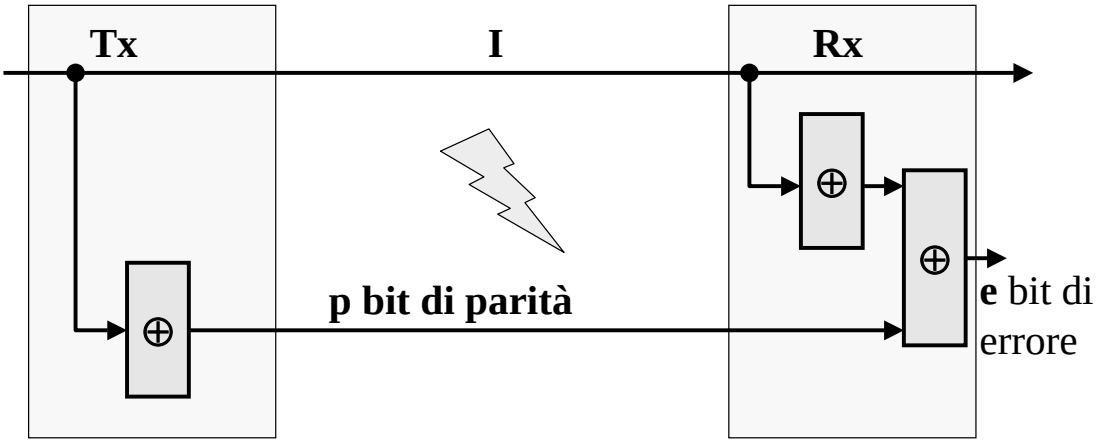
RS232: start+bit d'informazione+stop

Integrità: rilevazione di errori casuali



Bit di parità, Checksum, Cyclic Redundancy Check, ecc.

Bit di parità



p : bit di parità

$\mathbf{p = i_1 \oplus i_2 \oplus .. \oplus i_i}$

e : bit di errore

$\mathbf{e = p \oplus i_1 \oplus i_2 \oplus .. \oplus i_i}$

Checksum: una efficace estensione della parità per stringhe “lunghe”

x_1	x_2	...	x_n
x_{n+1}	x_{n+2}	...	x_{2n}
...			
x_{kn+1}	x_{kn+2}	...	$x_{(k+1)n}$
c_1	c_2	...	c_n

Dato: 7× 8 = **56** bit
Parità **8** bit

c_j : parità dei bit in colonna j

$\mathbf{c_j = x_j \oplus x_{n+j} \oplus ... \oplus x_{kn+j}}$

Internet: addizione senza riporto finale

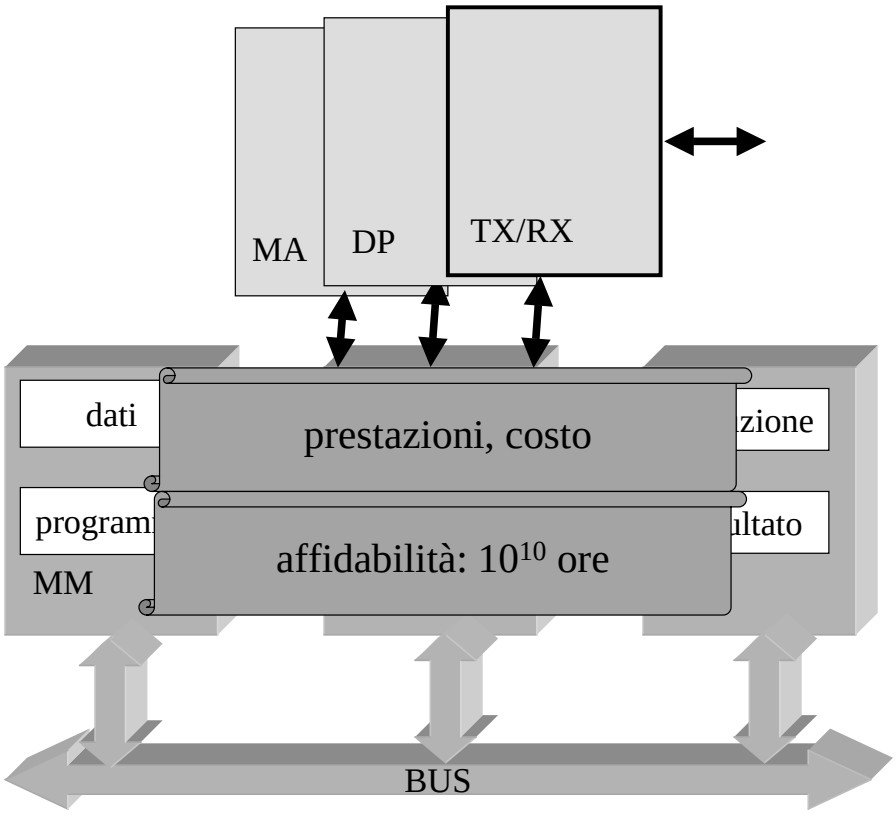
Elaborazione dell'informazione

Macchine digitali:

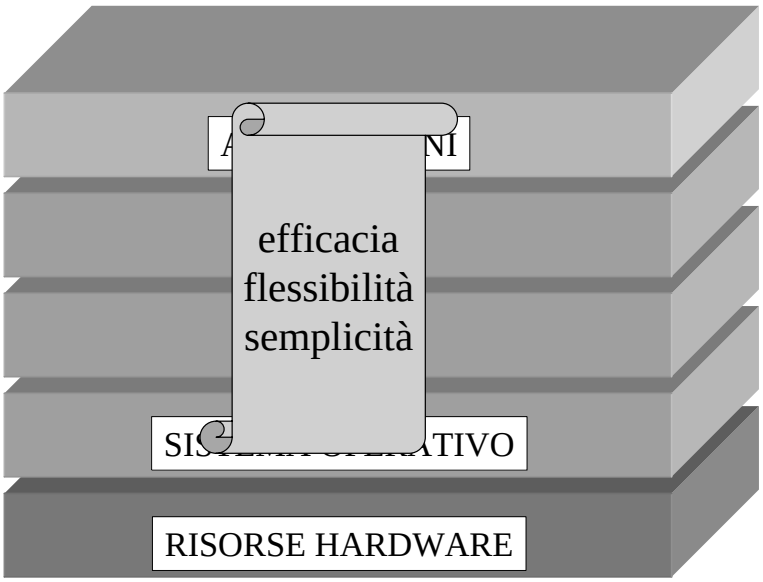
•special purpose (realizzazione di una specifica funzione)

•general purpose (esecuzione di qualsiasi algoritmo)

Il calcolatore: hardware

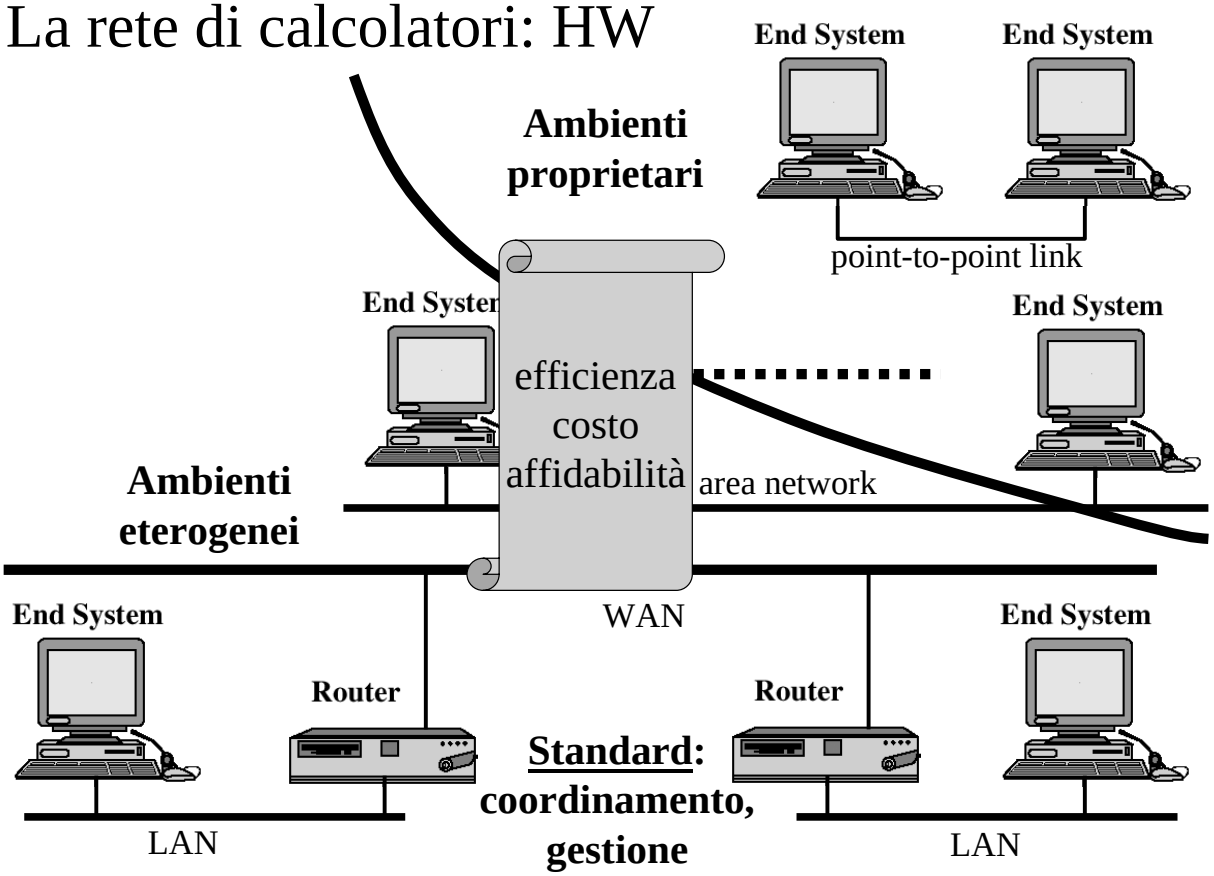


Il calcolatore: software



Personal communicator **Server**

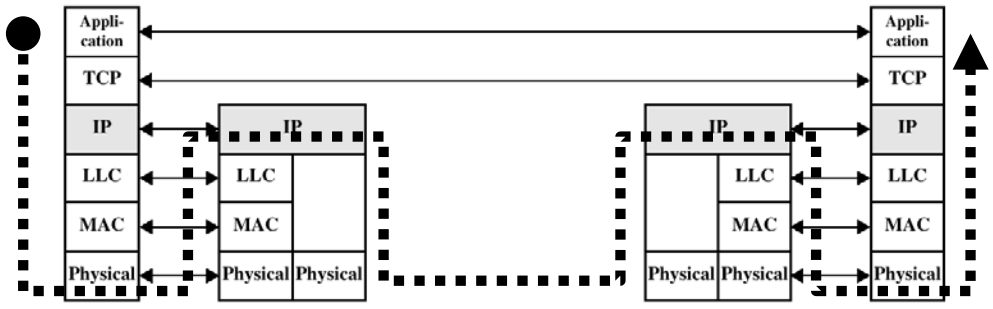
La rete di calcolatori: HW



La rete di calcolatori: la suite di protocolli

ISO/OSI	**Internet**	
Strato “applicazione”	**IETF** Internet Engineering Task Force **RFC** Request For Comments www.rfc-editor.org	SMTP, Telnet FTP, HTTP D…, …
Strato “presentazione”		efficacia flessibilità semplicità
Strato “sessione”		
Strato “trasporto”		
Strato “rete”		
Strato “collegamento”		MAC,PPP,802.11 802.5, FDDI
Strato “fisico”		

La suite di protocolli: apparati e flusso



Tecnologie per la sicurezza

- **minaccia**
- **vulnerabilità**
- **contromisura**

Minacce, vulnerabilità e contromisure

Sistema informatico

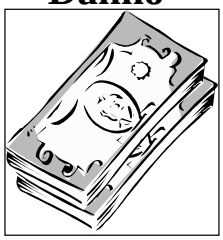
- **organizzazione**
- **utenti**
- **supporti**
- **dati**
- **software**
- **hardware**

Ricavo

Funzionamento corretto

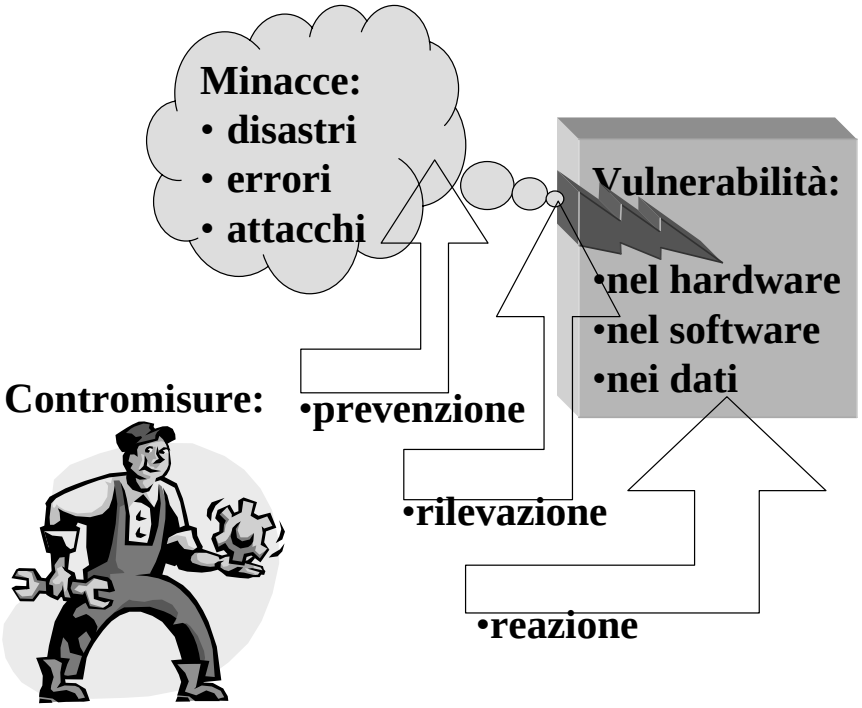
Danno

Funzionamento errato



Minaccia: insieme di circostanze che può potenzialmente creare danni
Vulnerabilità: punto debole che consente il concretizzarsi di una minaccia
Contromisura: azione, dispositivo, procedura o tecnica che consente di rimuovere o di ridurre una vulnerabilità

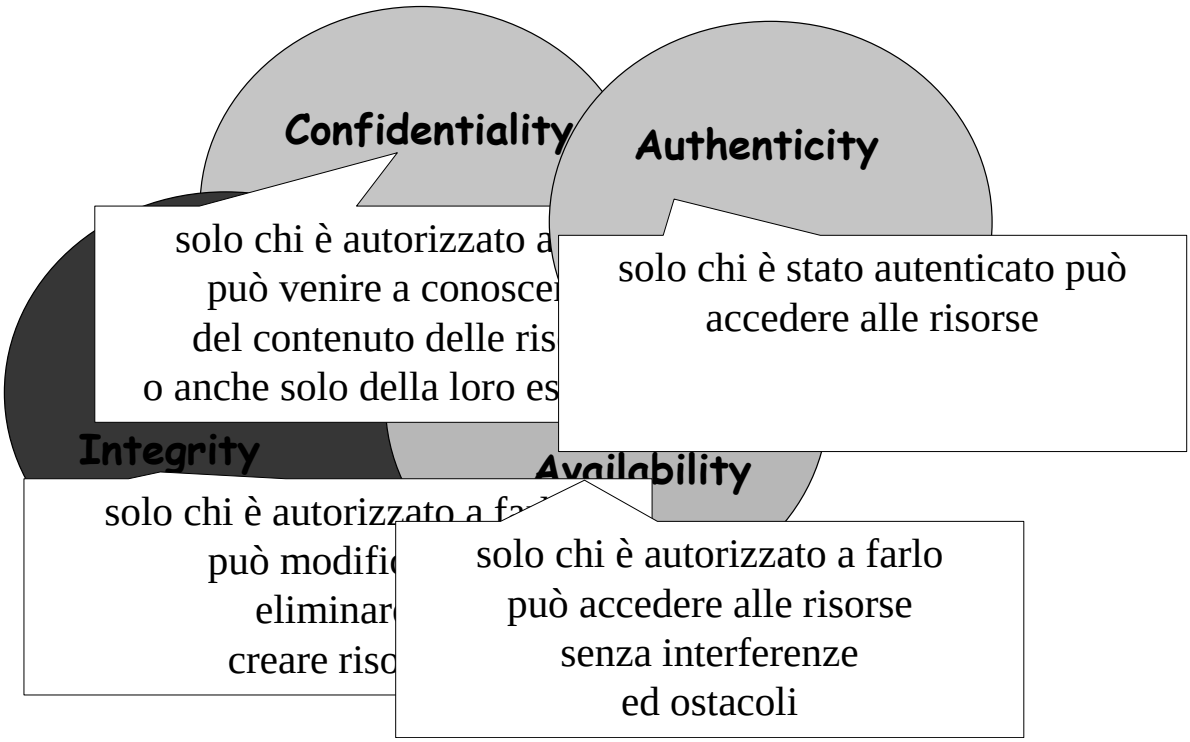
Classificazioni



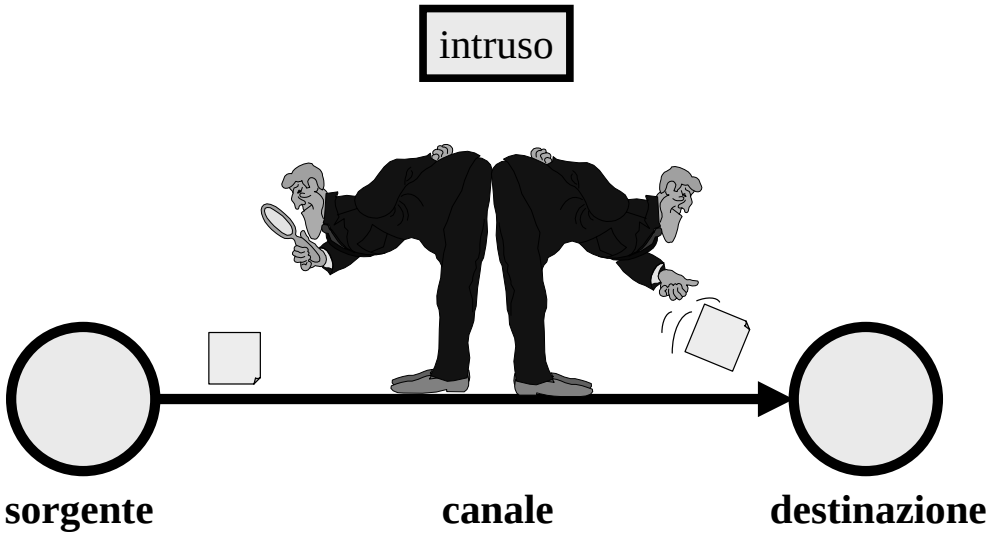
Tecnologie per la sicurezza

- **attacco**
- **proprietà per la sicurezza**
- **meccanismi e servizi**

Proprietà di Base per la Sicurezza dell'Informazione

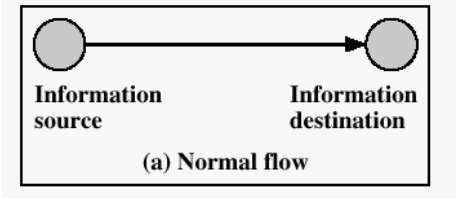


Il modello del Canale Insicuro

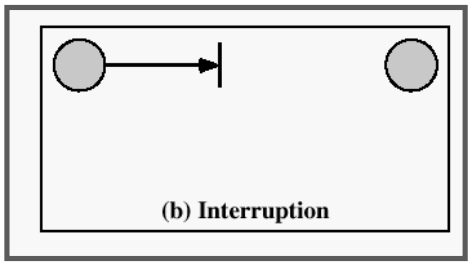


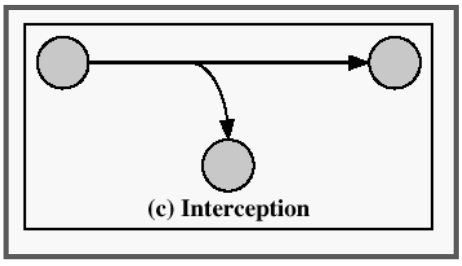
Attacchi di Sicurezza

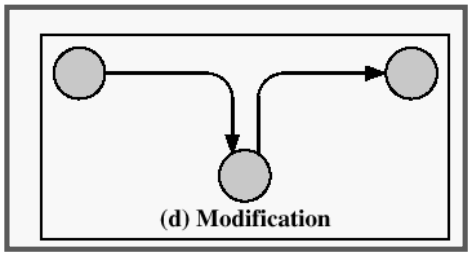
Attacco passivo

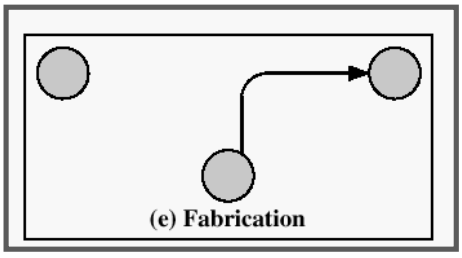


Attacco attivo









Attacco di Sicurezza: azione mirata a compromettere la sicurezza del sistema

Attacchi di Sicurezza

Tipi di attacchi:

- **Intercettazione:** un attacco alla confidenzialità
- **Interruzione:** un attacco alla disponibilità *(availability)*
- **Modifica:** un attacco all' integrità
- **Fabbricazione:** un attacco all' autenticità

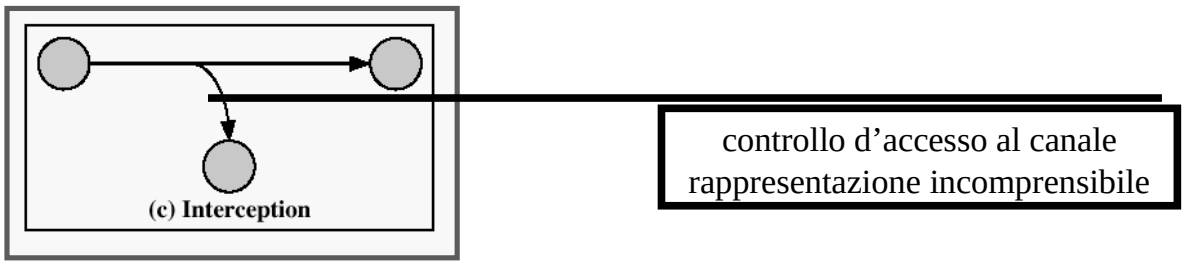
Contromisure

Prevenzione: azioni atte a minimizzare la probabilità di successo dell'attacco

Rilevazione: azioni atte ad individuare che l'attacco è in corso

Reazione: azioni atte ad annullare, o almeno a delimitare, gli effetti dell'attacco

☐ Attacco passivo Proprietà a rischio: **riservatezza**



Contromisure

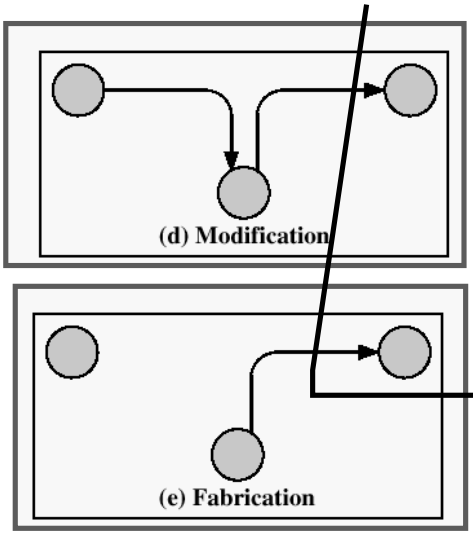
Prevenzione: azioni atte a minimizzare la probabilità di successo dell'attacco

Rilevazione: azioni atte ad individuare che l'attacco è in corso

Reazione: azioni atte ad annullare, o almeno a delimitare, gli effetti dell'attacco

Attacco attivo

Proprietà a rischio: **integrità, autenticità**



controllo d'accesso alla destinazione
attestato d'integrità e d'origine

Valutazione di una Contromisura

1. What problem does the security measure solve?

2. How well does the security measure solve the problem?

3. What other security problem does the measure cause?

4. What are the costs of the security measure?

5. Given the answers to steps two through four, is the security measure worth the costs?

Meccanismi e Servizi

- **Meccanismo:** meccanismo progettato per rilevare, prevenire o porre rimedio ad un attacco
- **Servizio:** un servizio che realizza la sicurezza dei sistemi di elaborazione e trasmissioni dei dati facendo uso di uno o piu' meccanismi.

Classificazione dei Servizi di Base (1.)

Riservatezza: consiste nel proteggere dati trasmessi o archiviati da attacchi passivi

Autenticazione: fornisce garanzia dell'autenticità di una comunicazione: autenticità delle entità comunicanti e autenticità dell'origine dei dati

Classificazione dei Servizi di Base (2.)

Integrità: per flussi di messaggi, per singolo messaggio e o singoli campi di messaggio rileva alterazioni rispetto allo stato originario (inserzioni, cancellazioni, sostituzioni)

Non ripudio: tale servizio impedisce che il mittente o il destinatario neghino che sia stato trasmesso un messaggio

A partire da questi servizi si costruiscono servizi avanzati, quali ad esempio servizi di controllo dell'accesso, di timestamping, di notariato ....

Valutazione e Certificazione

Standard internazionali per la valutazione e la certificazione della sicurezza: Orange book del NCSC, ISO 17799, ITSEC

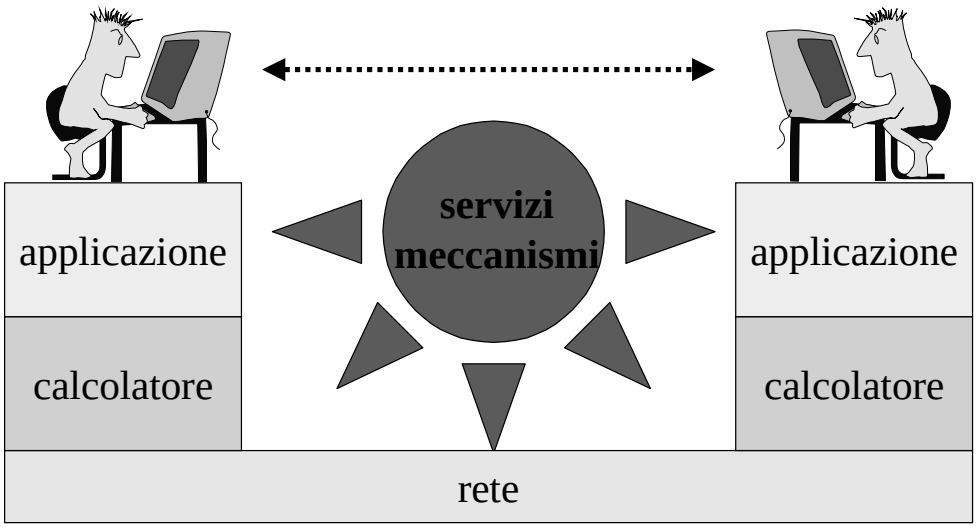
Standard nazionali: legge 196/2003 sulla privacy

1- Analisi dei rischi: probabilità d'occorrenza e impatto

2 - Politiche di sicurezza: regole, principi e procedure per gestire, controllare e proteggere strumenti e informazioni.

3 - Contromisure: efficacia e costo

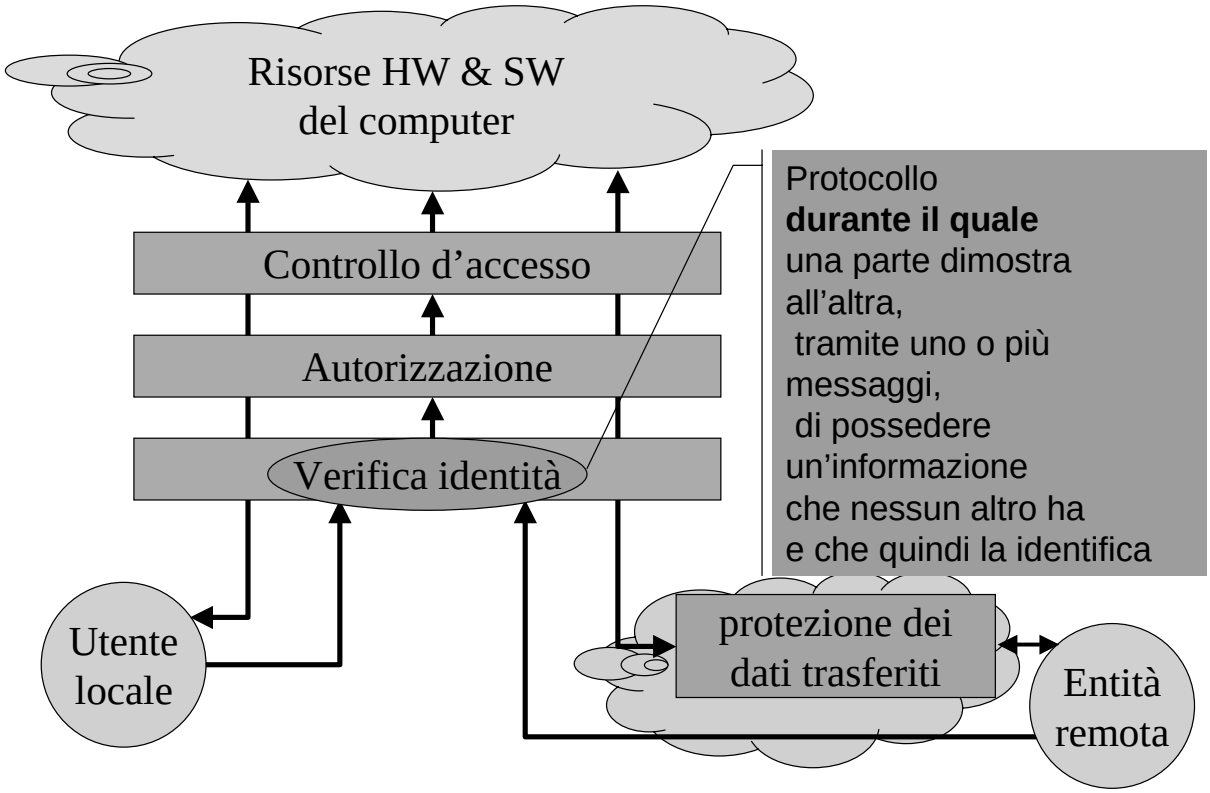
Collocazione dei meccanismi e dei servizi per la sicurezza



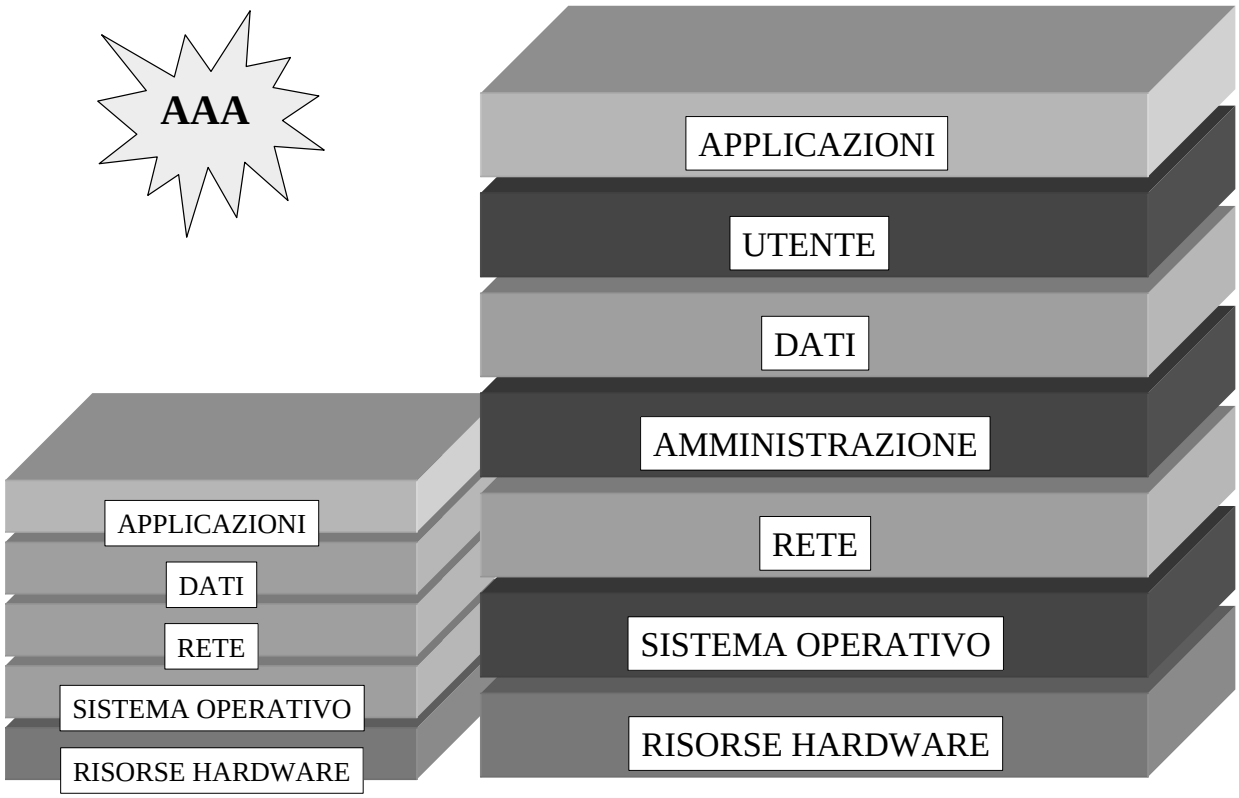
Tecnologie per la sicurezza

- **calcolatore sicuro**

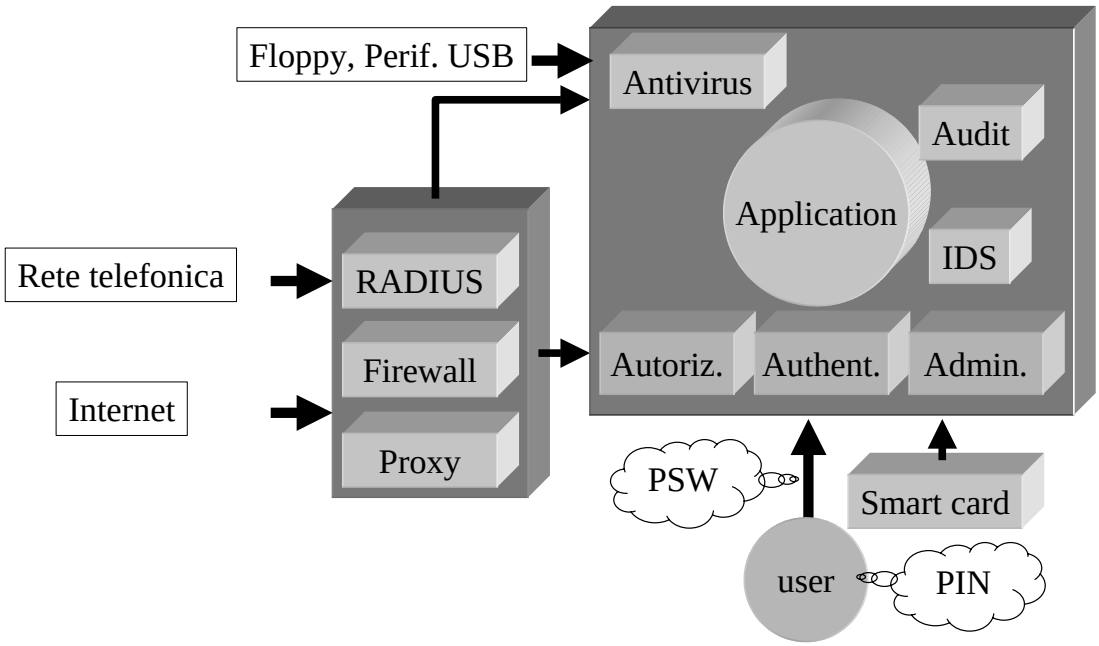
Uso sicuro delle risorse



Computer Security: prevenzione



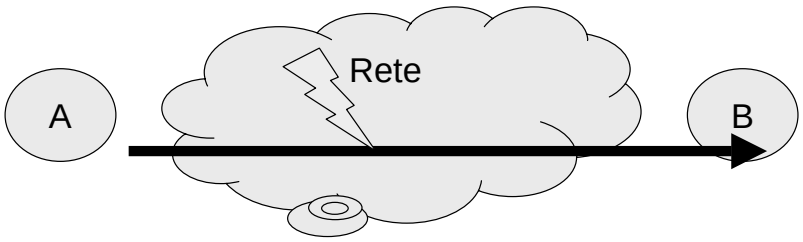
Security services



Tecnologie per la sicurezza

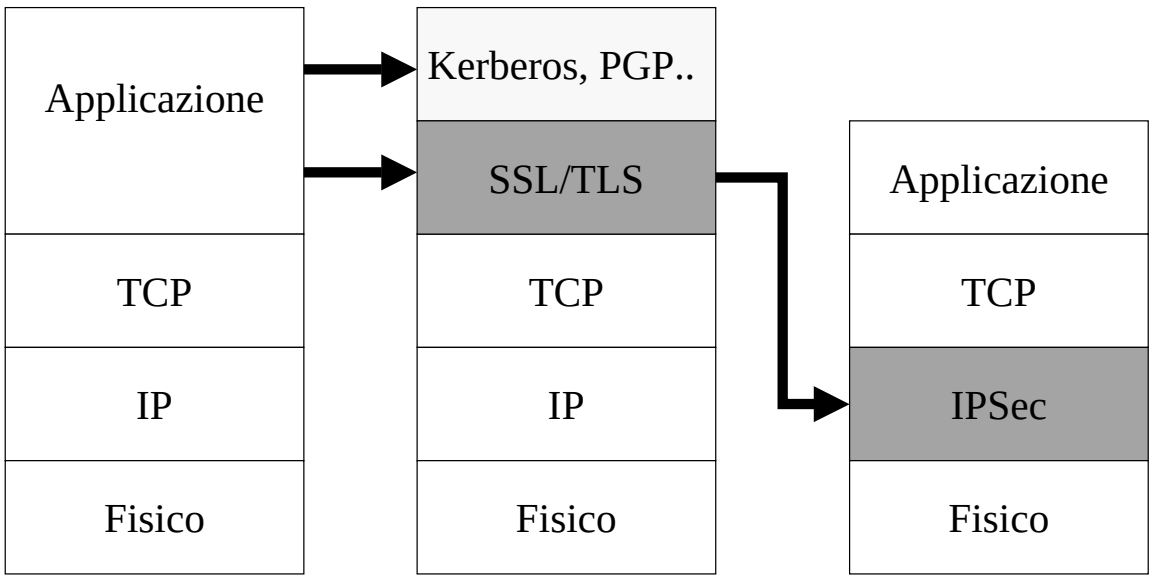
- **rete sicura**

IPv4: DEBOLEZZE



- **Packet sniffing**: lettura dei pacchetti in transito
- **IP spoofing**: falsificazione dell'indirizzo del mittente
- **Connection hijacking**: inserimento di dati nei pacchetti in transito
- **Clogging**: generazione di un carico oneroso di lavoro inutile

Sicurezza in Internet



Netscape
RFC 2246

RFC 2401
RFC 2402
……