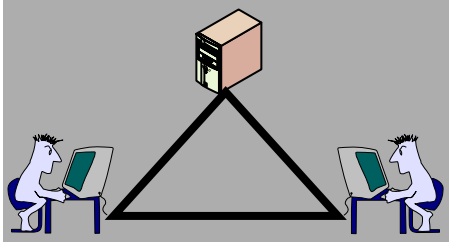
Capitolo 1

Sicurezza



1.1 Il trattamento automatico dell'informazione ……..…..2

- Società dell'informazione
- ICT

1.2 Hardware e Software.....…..…..3

- Rappresentazione dell'informazione
- Comunicazione e memorizzazione dell'informazione
- Elaborazione dell'informazione
- Trasmissione a distanza dell'informazione

1.3 Tecnologie per la sicurezza ……..7

- Minacce, vulnerabilità, attacchi e contromisure
- Disastri
- Errori
- Attacchi intenzionali
- Meccanismi e servizi per la sicurezza
- Calcolatori sicuri
- Reti sicure

1.1 Il trattamento automatico dell'informazione

1.1.1 Società dell'informazione

Il **dare/ricevere** quotidianamente grandi quantità informazioni tramite **testi**, **voci**, **suoni**, **disegni** ed **immagini**, sta diventando un aspetto essenziale della nostra vita.

La comunicazione è sempre più spesso in **forma elettronica** e può riguardare la sfera degli interessi "privati" (*rapporti interpersonali*, *divertimento*, *istruzione*, *salute*) o di quelli "pubblici" (*lavoro*, *affari*, *commercio*, *politica*).

L'interlocutore è, di norma, **remoto**; in alcuni casi è **umano**, in altri è il **server** di un'Impresa di *produzione*/*distribuzione* di beni e servizi, o di un'Organizzazione con specifiche finalità (*sanità, formazione*, *finanze*, *pubblica amministrazione*, ecc.).

Parimenti caratterizzanti del mondo in cui viviamo sono i continui scambi di dati tra Enti diversi e tra parti diverse di uno stesso Ente.

Tutto ciò è reso possibile da una diffusione capillare di **macchine per il trattamento automatico dell'informazione** e dalla disponibilità di **servizi per comunicazioni digitali** su scala mondiale.

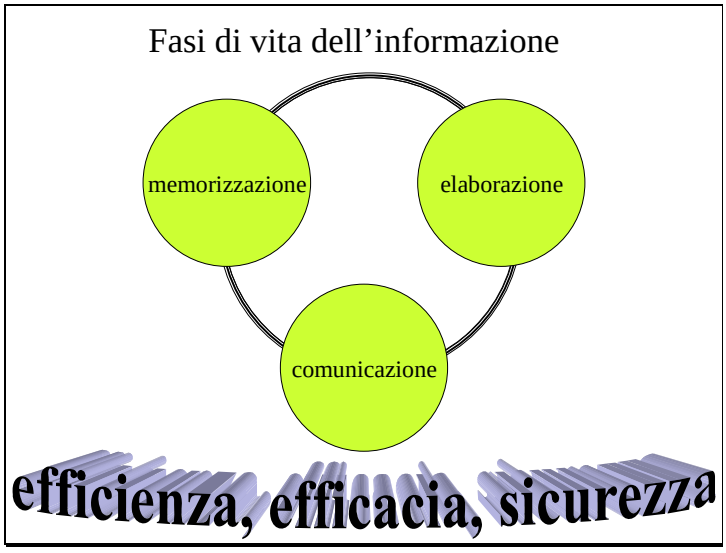
ESEMPIO – Negli ultimi anni il numero di calcolatori collegati ad Internet è cresciuto con legge esponenziale; si prevede che tale tipo di crescita varrà anche nei prossimi anni.

L'informazione deve dunque essere oggi considerata un **bene primario** per tutta l'umanità. L'uso di questo bene deve avvenire in un contesto sopranazionale, la cosiddetta **Società dell'informazione**, e richiede:

- un'idonea tecnologia di supporto,
- persone che la sappiano mettere in servizio ed impiegare,
- nuove leggi e nuove etiche di comportamento.

1.1.2 ICT

Compito della tecnologia impiegata nella Società dell'informazione, genericamente indicata dall'acronimo **ICT** (*Information and Communication Technologies*), è il dare supporto all'uomo nello svolgimento delle attività più ripetitive e/o più tediose e/o più complicate richieste dalle tre **fasi di vita** dell'informazione.



Ogni forma di trattamento dell'informazione può, infatti, essere modellata da un continuo susseguirsi di tre momenti topici:

- la **comunicazione**,
- la **memorizzazione**,
- l'**elaborazione**.

Tre sono le proprietà da garantire in massimo grado quando si vuole affidare a macchine il trattamento dell'informazione:

1. **efficienza** (i tempi di esecuzione devono essere i più bassi possibili),
2. **efficacia** (i dati trattati devono garantire il più possibile il conseguimento della finalità del servizio cui si riferiscono),
3. **sicurezza** (l'attività svolta deve essere quella desiderata, e questo anche alla presenza di eventi che potrebbero indurre comportamenti dannosi e/o pericolosi).

Da cinquant'anni a questa parte il conseguimento di una sempre maggiore efficienza ed efficacia è stato l'obiettivo primario dei Costruttori di prodotti **hardware** e **software** (le due **tecnologie di base**).

L'ottenimento di sicurezza, o meglio di robustezza a fronte del verificarsi di eventi che possono negativamente incidere sullo svolgimento di ciascuna fase di vita dell'informazione, è un obiettivo più recente, coinvolge fortemente anche gli Utenti e richiede il corretto impiego delle **tecnologie per la sicurezza dell'informazione**, un nuovo insieme di accorgimenti e di prodotti Hw/Sw, in continuo divenire.

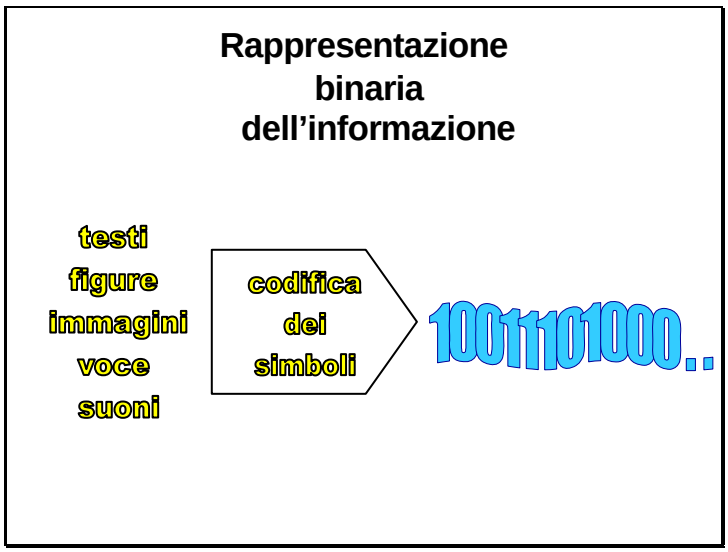
1.2 Hardware e Software

1.2.1 Rappresentazione dell'informazione

L'informazione è sempre rappresentata da una **stringa** di simboli appartenenti ad un certo insieme finito, detto **alfabeto**. Ogni simbolo dell'alfabeto rappresenta un'informazione "elementare". Giustapposizioni in un **certo ordine** di un **certo numero** di simboli rappresentano informazioni più "complesse".

ESEMPI – L'alfabeto dei numeri contiene dieci *cifre*, due simboli di *segno* e la *virgola*. L'alfabeto della lingua scritta affianca ai simboli precedenti i *caratteri* maiuscoli e minuscoli, i *segni di interpunzione*, i *simboli di operazione* e le *parentesi*. L'alfabeto della lingua parlata è formato dai *fonemi*. L'alfabeto della musica è formato dalle sette *note*.

Per dare una rappresentazione unitaria a qualsiasi tipo d'informazione, le tecnologie dell'informazione impiegano l'alfabeto più semplice possibile:



$$\mathbf{B} = \{\mathbf{0},\mathbf{1}\}.$$

La **rappresentazione binaria** di "numeri", "testi", "immagini" e "suoni" richiede di associare a ciascuno degli **M** simboli del loro alfabeto originario una delle $\mathbf{2^N}$ differenti stringhe di **N bit**. Naturalmente deve essere

$$\mathbf{M \leq 2^N}.$$

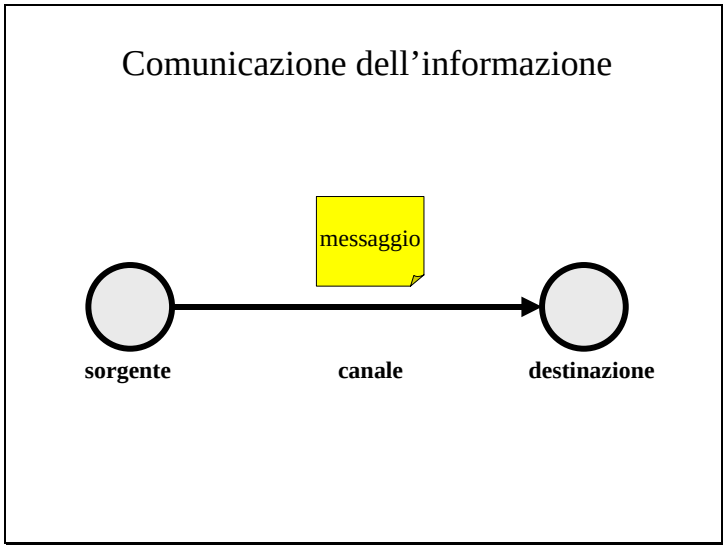
Una volta stabilito il **codice**, una stringa di **K** simboli dell'alfabeto originario è così trasformata in una stringa di **KxN** bit.

La scelta di quale codice impiegare deve essere **condivisa** da chi trasmette l'informazione e da chi la deve ricevere.

L'uso di **codici standard**, definiti da Enti internazionali, consente di eliminare inutili invenzioni e rende **interoperabili** programmi scritti in posti diversi ed in momenti diversi.

ESEMPIO – Con 16 bit lo standard UNICODE definito dalla ISO rappresenta in binario i simboli grafici di tutte le lingue della Terra. UNICODE è compatibile con il precedente standard ASCII a 8 bit.

1.2.2 Comunicazione e memorizzazione dell'informazione



La comunicazione dell'informazione è affidata a **messaggi** formati da una o più stringhe concatenate.

L'entità che invia un messaggio è detta **sorgente**; l'entità che lo riceve è detta **destinazione**. Gli interlocutori possono essere o due uomini, o un uomo una macchina, o due macchine.

Il supporto necessario per lo svolgimento di una comunicazione è detto **canale**; da un punto di vista fisico può essere o un **mezzo trasmissivo** (un doppino di rame, un cavo coassiale, una fibra ottica, l'aria stessa) o un'unità di memoria (elettronica, magnetica, ottica). Un canale impiega **segnali**, cioè grandezze fisiche variabili nel tempo, per trasportare i simboli di informazione dalla sorgente alla destinazione.

I segnali hanno di norma due soli valori, per essere il più possibile insensibili ai disturbi presenti sul canale.

I bit del messaggio possono essere trasportati o dai valori assunti consecutivamente da un solo segnale (trasmissione **in serie**), o dai valori assunti contemporaneamente da un pari numero di segnali (trasmissione **in parallelo**), o dai valori assunti contemporaneamente e consecutivamente da un numero inferiore di segnali (trasmissione **in serie/parallelo**).

Le macchine che svolgono i ruoli di sorgente e di destinazione alle estremità di uno stesso canale devono naturalmente impiegare

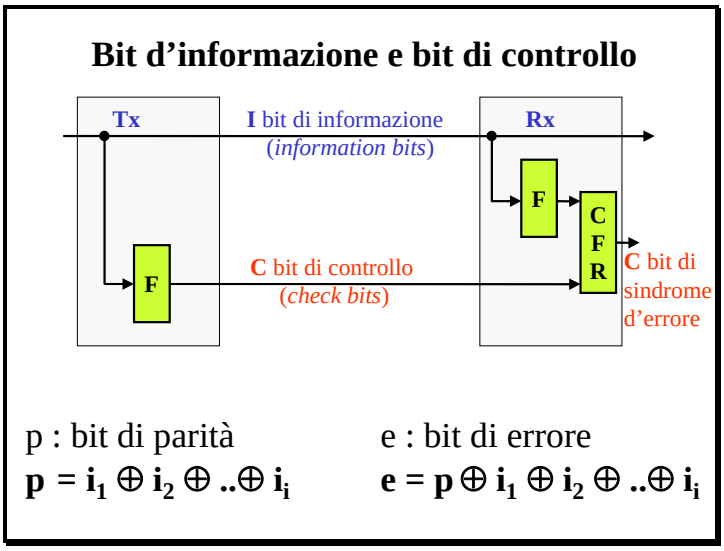
- gli stessi segnali,
- la stessa modalità di trasmissione,
- lo stesso ritmo di invio e di estrazione dei bit,
- la stessa codifica binaria dei simboli d'informazione e dei simboli di controllo del flusso dei dati.

A tal fine sono state stabilite regole precise, i **protocolli di comunicazione**, che mettono anche in conto la desiderata modalità d'impiego del canale (trasmissione continua, a messaggi, a pacchetti), la distanza tra le due macchine (ritardo di propagazione) e la natura del mezzo trasmissivo.

ESEMPIO - Il protocollo asincrono RS232 prevede la trasmissione seriale di singoli messaggi. Inizio e fine della comunicazione sono segnalati da due bit aggiuntivi, lo *start* e lo *stop*, posti alle estremità del messaggio. Sorgente e destinazione devono operare allo stesso ritmo o quasi; il numero di bit del messaggio deve essere prestabilito.

Spesso un protocollo si preoccupa anche di individuare se i messaggi sono stati alterati da disturbi casuali.

L'**individuazione degli errori** richiede l'uso di appropriati **codici ridondanti** (codici cioè che codificano i simboli d'informazione con un numero di bit superiore a quello strettamente necessario).



Nei **codici a riconoscimento d'errore**, la sorgente, tramite una funzione **F**, calcola alcuni bit di controllo (*check bits*) e li aggiunge a quelli del messaggio (*information bits*).

La destinazione, tramite la **F**, calcola i bit di controllo corrispondenti ai bit d'informazione ricevuti e li confronta con i bit di controllo ricevuti. Se ci sono differenze il messaggio è considerato errato: per costruzione, infatti, il risultato fornito dalla F in corrispondenza di una qualsiasi configurazione corretta è diverso da quello che si ottiene, quando la configurazione è stata modificata dai disturbi ritenuti più probabili sul supporto fisico di comunicazione.

La destinazione scarta tutti i messaggi affetti da errore e chiede usualmente alla sorgente di ritrasmetterli.

ESEMPI – Il caso più semplice è il **bit di parità**, che risulta però utile solo se la stringa di informazione è corta (ad es. un byte) e se è trascurabile la probabilità che si modifichi più di un bit alla volta.

Nel caso di stringhe molto lunghe la presenza di errori multipli diventa probabile e l'adozione del bit di parità un accorgimento o inadeguato (se è uno solo) o troppo costoso (se ogni byte della stringa ne ha uno).

In questi casi si è dimostrato efficace l'uso della **somma di controllo** (*checksum*): si scompone il messaggio in blocchi di **n** bit ciascuno (tipicamente uno o due byte), li si somma tra loro e si impiegano n bit del risultato come bit di controllo. Sono in uso o la somma modulo due, o la somma aritmetica, eliminando in questo caso dal risultato il bit di maggior peso (uno standard Internet prevede anche una successiva operazione di complemento a 2).

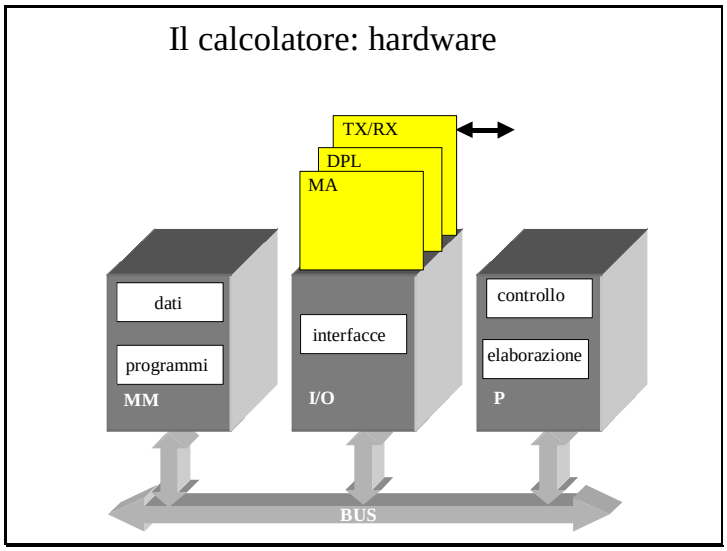
Il calcolo della checksum in ricezione ed il successivo confronto con quella calcolata in trasmissione consente al ricevitore una buona rilevazione di errori multipli a distribuzione casuale.

Per la rilevazione di errori su più bit trasmessi consecutivamente si sono dimostrati particolarmente efficaci i **codici di controllo a ridondanza ciclica** (CRC da *Cyclic Redundancy Check*); usuale è l'impiego di 32 bit.

I **codici a correzione d'errore** sfruttano una ridondanza ancora più alta per individuare la posizione dei bit pervenuti errati. Il ripristino del valore corretto può così essere fatto direttamente dalla destinazione: si noti che per correggere un bit è sufficiente complementarlo.

1.2.3 Elaborazione dell'informazione

Le macchine che generano, elaborano, memorizzano e comunicano informazioni rappresentate da stringhe binarie sono dette **digitali** e possono essere o *special purpose* (cioè singolarmente dedicate a svolgere un compito specifico come la memorizzazione, o la trascodifica, o la visualizzazione, o la rice-trasmissione, ecc.) o *general purpose* (cioè formate da più macchine special purpose che si scambiano informazioni all'interno di un unico sistema in modo da consentire l'esecuzione automatica di qualsivoglia algoritmo).



Il **calcolatore elettronico** appartiene a questa seconda categoria ed è formato da quattro unità.

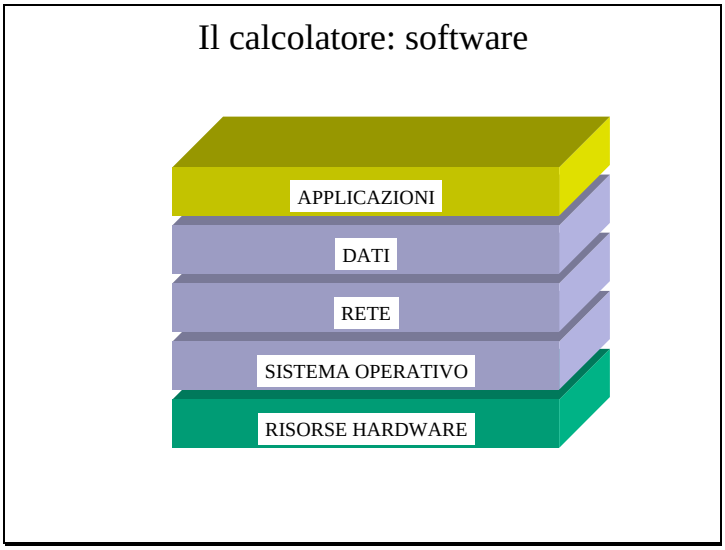
1. **Processor –** *macchina special purpose* in grado di eseguire, una alla volta, le *istruzioni* di un *programma* preventivamente disposto nella unità di memoria.
2. **Main Memory –** *macchina special purpose* contenente i programmi in esecuzione ed i relativi dati.
3. **Input/Output –** insieme di *interfacce* e di *dispositivi* per memorizzare grandi quantità di dati (MA), per interagire con l'utente (DPL) e per comunicare a distanza (TX/RX).
4. **Bus –** efficiente *sistema interno di comunicazione*, condiviso dalle precedenti unità per scambiarsi pacchetti di bit.

L'evoluzione della **tecnologia elettronica** ha reso questo tipo di macchina sempre più **efficiente** e sempre meno **costosa**: l'hardware attualmente acquistabile è caratterizzato da **processori** con diversi MIPS, da **memorie principali** con decine di MB, da **memorie di massa** con decine di GB e da **unità di rice-trasmissione** per flussi di centinaia di KB/s.

L'incremento dell'**affidabilità** è stato il secondo importantissimo contributo di questa tecnologia.

ESEMPI - L'ENIAC aveva in media un guasto ogni quarto d'ora; un attuale processore VLSI lo ha ogni 10^{10} ore. Negli attuali circuiti integrati sono anche presenti strumenti (codici a rilevazione d'errore, delimitazione delle operazioni eseguibili, duplicazioni di unità, ecc) che ne sospendono il funzionamento in presenza di errori.

La **tecnologia informatica** ha esaltato l'**efficacia**, la **flessibilità** e la **semplicità** d'impiego dei calcolatori elettronici. A tal fine si è dimostrata particolarmente importante un'organizzazione del software **a strati di servizio sovrapposti.** A partire dal basso si distinguono quattro livelli base:



1. **sistema operativo -** si occupa della gestione dettagliata delle **risorse** hardware, consentendone un uso condiviso da parte di più programmi;
2. **rete -** esegue ogni azione prevista dai protocolli di comunicazione con dispositivi e macchine remoti, facilitando la definizione e lo svolgimento di **elaborazioni distribuite**;
3. **dati -** gestisce archiviazione, reperimento e salvataggio (*backup*) dei dati impiegati dai programmi, tenendo conto delle relazioni tra essi esistenti (**basi di dati**);
4. **applicazioni –** alloggia sia i programmi che svolgono le attività di calcolo desiderate dall'utente, sia gli strumenti (**compilatori ed interpreti**) che gli consentono di scriverli con un linguaggio di programmazione di alto livello.

Nella Società dell'informazione il calcolatore (l'*host*, nel gergo di Internet) ricopre oggi un duplice ruolo:

- macchina facile da usare per accedere ai servizi (*personal communicator*, *client*, *browser*),
- macchina sufficientemente potente per erogarli (*server*).

1.2.4 Trasmissione a distanza dell'informazione

La **rete di calcolatori** è il secondo strumento di base della Società dell'informazione.

L'evoluzione delle **tecnologie digitali di telecomunicazione** ha dato il supporto fisico di volta in volta più idoneo per mettere in comunicazione macchine digitali sempre più distribuite nel territorio. Dapprima è stato sufficiente *remotizzare* i terminali di un host, poi si è passati alla connessione diretta tra due host, poi ancora alla rete locale, dove più *client* condividono l'uso di uno stesso supporto fisico per accedere a più *server*, ed infine alla rete di reti, che consente di mettere in comunicazione macchine collocate in ogni punto del globo.

Parallelamente le tecnologie informatiche si sono prese in carico la gestione logica delle comunicazioni. Lo *standard di riferimento* ISO/OSI (www. iso.ch) ha introdotto il principio della *suite di protocolli* suddividendo su sette livelli di astrazione (*layers*) la risoluzione dei problemi fisici e logici di una comunicazione tra *sistemi eterogenei*:

STRATO	INCOMBENZE
applicazione (*application)*	protocolli per la gestione di terminali remoti, per il trasferimento di file, per l'amministrazione di rete, per il modello client/server, per la posta elettronica ecc.; procedure per adattare eventuali incompatibilità di hardware.
presentazione (*presentation*)	trascodifiche da dati strutturati a non strutturati e viceversa; compressione e decompressione dei dati.
sessione (*session*)	controllo di sequenze di comunicazioni; gestione della mutua esclusione e della sincronizzazione.
trasporto (*transport*)	raggruppamento dei dati in unità logiche; gestione del trasporto per servizi *end-to-end* e *broadcasting*.
rete (*network*)	ridimensionamento, instradamento e numerazione dei pacchetti; instradamenti alternativi per evitare congestioni.
collegamento (*data link*)	impacchettamento dei bit; regolarizzazione del flusso di invio; ritrasmissione dei frame pervenuti errati.
fisico (*phisical*)	forma del connettore di rete; natura, verso e velocità dei segnali; inizio e fine della trasmissione.

Da un punto di vista logico, ciascun strato della sorgente comunica con lo strato omonimo della destinazione; in realtà ogni comunicazione tra due applicazioni deve da un lato dapprima discendere tutta la pila degli strati di servizio, per poi risalirla tutta dall'altro lato.

Svariate sono state le realizzazioni di apparati HW (*link*, *router*, *gateway*, *local/wide area network*) e SW (*network protocols*) basate su questo modello.

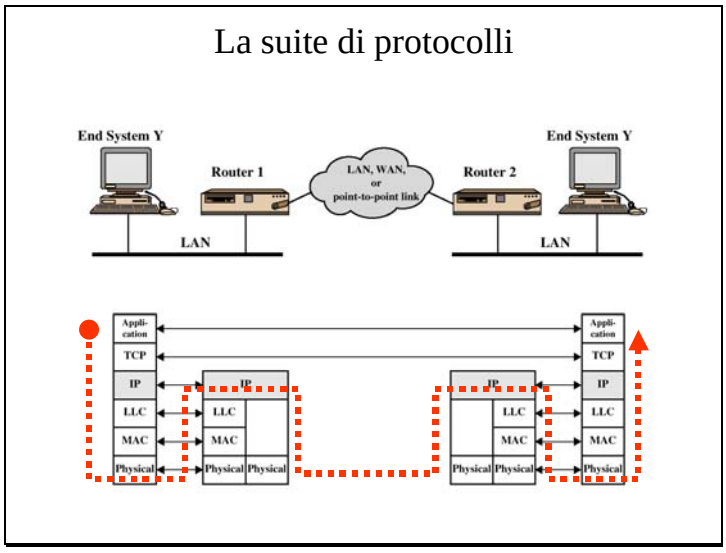
Un differente e più efficace modello è stato successivamente adottato da **Internet**[1] ed è poi diventato uno standard de facto. Nella sottostante tabella i due modelli sono messi a confronto; gli acronimi dei più usati protocolli Internet/Intranet sono indicati nella colonna più a destra.

OSI	Internet	Protocolli
applicazione	**applicazione**	SMTP, Telnet, FTP, HTTP, SOAP DNS, SNMP, ecc.
presentazione		
sessione		
trasporto	**trasporto**	TCP, UDP
rete	**rete**	IPv4, IPv6
collegamento	**collegamento**	MAC, PPP, 802.11
fisico	**fisico**	802.5, FDDI

La suite di protocolli è un importante strumento di flessibilità. Ogni strato può contenere diversi protocolli ed offrire quindi servizi differenziati al livello superiore. Nuove versioni di un protocollo non incidono inoltre minimamente su quello che c'è sopra e su quello che c'è sotto.

ESEMPI – Il protocollo **TCP** dello strato di trasporto è detto **affidabile**, in quanto si prende carico di far arrivare alla destinazione, in ordine e senza errori, tutti i pacchetti che la sorgente ha immesso nella rete. Il protocollo **UDP** (più spartano, ma anche più veloce non prevedendo ritrasmissioni) si preoccupa solo di far arrivare al più presto i pacchetti alla destinazione, senza curarsi che ci siano tutti, che siano in ordine e che siano integri. L'introduzione della nuova versione del protocollo di rete (**IPv6**) non ha indotto modifiche nei protocolli dello strato di trasporto.

[1] Notevole è stato il contributo propositivo dato dal Internet Engineering Task Force (IETF) tramite i documenti di specifica denominati Request For Comments (www.rfc-editor.org/).



La disponibilità di una struttura gerarchica di protocolli di comunicazione ha di fatto reso estremamente semplice il progetto e la realizzazione di applicazioni distribuite su macchine appartenenti a reti diverse.

In figura sono ad esempio prese in considerazione due LAN gestite dai protocolli **Ethernet** e **TCP/ IP.**

Per interconnetterle è sufficiente:

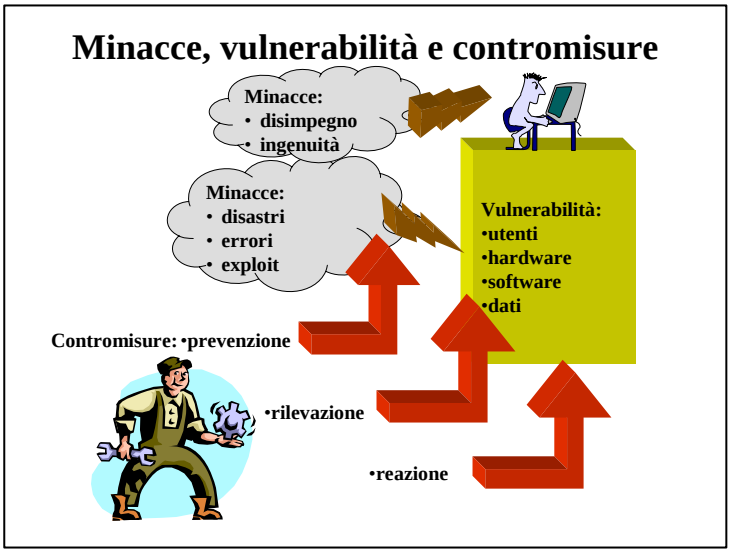
- predisporre o sfruttare un **supporto fisico** di comunicazione *inter-rete* idoneo al traffico da svolgere,
- acquistare sul mercato due **router** ed installarli alle due estremità del supporto,
- caricare il **software** che li abilita a svolgere i servizi del livello fisico, del livello di collegamento e del livello di rete.

1.3 Tecnologie per la sicurezza

1.3.1 Minacce, vulnerabilità, attacchi e contromisure

Ogni macchina della Società dell'informazione ha una sua prestabilita missione da compiere (interfaccia per accedere a servizi, erogazione di servizi, nodo di una rete, ecc.).

Purtroppo ha anche punti deboli, o **vulnerabilità**, che al verificarsi di certe situazioni, o **minacce**, possono indurre comportamenti diversi da quello desiderato e quindi **danni**. Potenziali punti deboli sono il comportamento degli **utenti**, la configurazione del **hardware**, il **software** che viene eseguito ed i **dati** su cui si basa l'elaborazione.



Le minacce che li possono sfruttare appartengono a tre categorie: **i disastri** (o sociali, o ambientali, o impiantistici), **gli errori accidentali** (del hardware, o del software, o dell'uomo), **gli attacchi intenzionali** (portati da qualcuno o per divertimento, o per esibizionismo, o per malizia, o per intento criminale).

Le tecnologie per la sicurezza forniscono le **contromisure**, cioè le azioni, i dispositivi, le procedure, le tecniche che possono rimuovere o ridurre le vulnerabilità.

Esistono tre tipi di contromisura: la **prevenzione** (minimizzare la probabilità che una minaccia possa concretizzarsi), la **rilevazione** (individuare il più presto possibile che il comportamento non è più quello voluto) e la **reazione** (annullare o delimitare gli effetti del comportamento anomalo).

La contromisura è però come un farmaco: ha un suo **costo** (in termini di **soldi**, di **impegno delle risorse** informatiche del sistema, di **impatto** sugli utenti), una sua **efficacia** (a fronte di una certa minaccia) e suoi **negativi effetti collaterali** (la creazione di nuove vulnerabilità). La messa in opera di una certa contromisura deve essere dunque fatta oculatamente, valutando sia la probabilità che si verifichi una certa minaccia in grado di sfruttare una certa vulnerabilità, sia il danno che ne discende. Tale attività è usualmente denominata **analisi del rischio**.

ESEMPIO – Nella sua rivista elettronica CRYPTO-GRAM (aprile 2002), Bruce Schneier ha suggerito di valutare ogni contromisura (passata, presente o futura) dando risposte puntuali alle seguenti domande:
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*?

1.3.2 Disastri

I **disastri** possono determinare parziali o totali **interruzioni del servizio** di elaborazione. Fin dagli anni '50 sono state adottate **contromisure** di tipo logistico ed impiantistico.

ESEMPI – Appropriata scelta dei locali, protezione dei punti di accesso, uso di impianti antincendio e di gruppi di continuità, attuazione periodica di *backup*, assicurazioni, ecc.

La drastica riduzione d'ingombro, di peso e di consumo energetico delle macchine attuali ha comunque contribuito a ridurre moltissimo la pericolosità di questi eventi.

1.3.3 Errori

Disturbi elettromagnetici, bachi del software e **distrazioni** degli utenti possono determinare un più o meno grave **degradamento del servizio** di elaborazione. Il problema è dunque quello di recuperare al più presto un funzionamento "accettabile".

La **difesa**, tradizionalmente predisposta nel Hw e nel Sw, si articola in accorgimenti per la **prevenzione**, la **rilevazione** e la **reazione**; spesso è richiesto il coinvolgimento dell'**utente** finale e/o dell'**amministratore** del sistema.

ESEMPI – Ventilazione delle schede, schermatura dei cavi e filtri sull'alimentazione prevengono gli effetti nocivi sul Hw di molti disturbi. La prevenzione dei bachi Sw è affidata alle metodologie di progetto; la reazione alle *patch*.

La rilevazione e la non propagazione di dati errati è oggi presente all'interno delle unità hardware e dei moduli software. La reazione è di norma affidata al *roll-back*, cioè alla immediata riesecuzione delle elaborazioni affette da errori. La contromisura, una volta di competenza dell'operatore, è oggi chiamata in causa automaticamente (dal sistema operativo, dal gestore della base di dati, dagli strati di *data link*, di *network* e di *transport* dei servizi di rete, ecc.); moltissimo dell'attuale software applicativo (ad es. il pacchetto *Office* della Microsoft) consente il lancio del *roll-back* anche da parte dell'utente che si accorge di aver dato comandi errati.

1.3.4 Attacchi intenzionali

Con l'**attacco intenzionale** (l'*exploit*, nel gergo degli *hacker*) un malintenzionato sfrutta le vulnerabilità di un sistema informatico per tentare di impedirne il corretto funzionamento, o per impiegarlo per propri fini.

Questa minaccia, già avvertita fin dall'installazione dei primi Centri di Calcolo, è stata inizialmente fronteggiata con il **controllo d'accesso** (tramite guardia giurata, o badge, o sensore biometrico) sui punti di ingresso dei locali e con adeguate protezioni apposte sulle porte e sulle finestre.

Successivamente, con l'avvento dell'accesso remoto e della multiprogrammazione, il controllo d'accesso è stato necessariamente posto all'interno delle macchine ed ha riguardato singolarmente l'uso di tutte le loro **risorse**.

L'obiettivo era quello di garantire al hardware, al software ed ai dati del sistema informatico le proprietà di *confidentiality*, di *integrity* e di *availability* (il cosiddetto "*CIA triangle*"):

- la **confidenzialità** assicura che solo chi è autorizzato a farlo possa venire a conoscenza del contenuto delle risorse o anche solo della loro esistenza;
- l'**integrità** assicura che solo chi è autorizzato a farlo possa modificare, eliminare, creare risorse;
- la **disponibilità** assicura, a chi ne ha il diritto, un accesso alle risorse senza interferenze ed ostacoli.

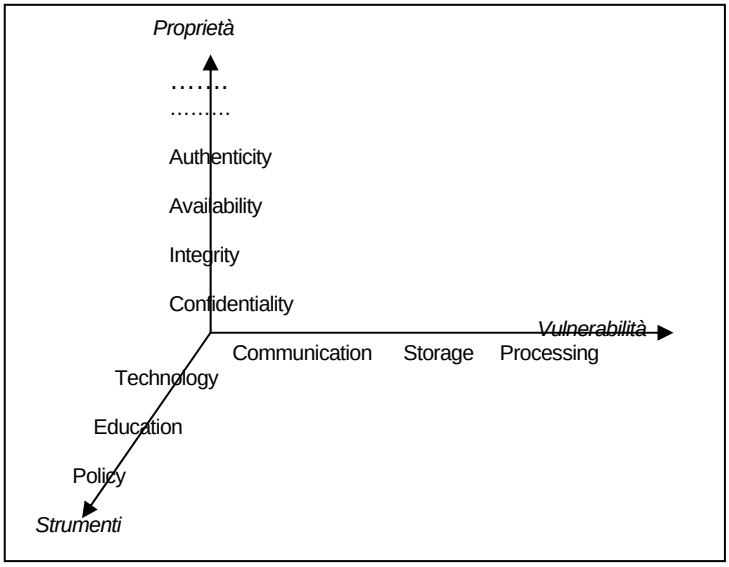
Le tre proprietà, una volta assicurate a tutte le componenti del sistema, sono, infatti, in grado di ridurre od eliminare le vulnerabilità indicate nella seguente tabella[2]:

Vulnerabilità	Assenza di confidenzialità	Assenza di integrità	Assenza di disponibilità
• **del hardware**	Furto	Aggiunta, modifica ed eliminazione di periferiche	Arresto totale ed impedimenti allo svolgimento di servizi
• **del software**	Intercettazione	Modifica Falsificazione	Eliminazione
• **dei dati**	Intercettazione	Modifica Falsificazione	Perdita Cancellazione

Da una ventina di anni si è dovuto prendere atto che la protezione del funzionamento delle singole parti di una macchina è una condizione necessaria, ma non sufficiente, per far fronte ai sempre più numerosi e differenziati

[2] da [5], cap.1

attacchi condotti da malintenzionati. Per essere adeguatamente sicuri è indispensabile proteggere il prodotto finale dell'attività di calcolo, cioè **l'informazione**.



A tal fine è utile fare riferimento ad uno spazio a tre dimensioni[3]

- su un primo asse sono elencate le **vulnerabilità** delle risorse chiamate in causa durante le tre fasi di vita dell'informazione,
- su un secondo asse sono elencate le **proprietà** in mancanza delle quali un'informazione perde, in tutto o in parte, la sua utilità,
- sul terzo asse sono infine indicati gli **strumenti** che consentono di difendere le proprietà più critiche e più a rischio in ciascuna delle fasi di vita.

Ogni punto di questo spazio deve essere oggetto di una puntuale e separata attività di **risk analysis**. Le conclusioni cui si perviene devono essere poi valutate sulla base di standard internazionali e di leggi nazionali

ESEMPI – **Orange book**, **ISO 17799**, **ITSEC** e **Common Criteria** (www.commoncriteriaportal.org) sono in ordine temporale i più noti standard introdotti per valutare e certificare la sicurezza di un sistema informatico.
La **legge 196/2003** impone l'adozione di misure minime di sicurezza a tutte le aziende italiane.

Le proprietà precedentemente elencate in figura hanno bisogno di qualche ulteriore commento. La criticità varia da caso a caso:

- la confidenzialità, o meglio la **riservatezza** dell'informazione alle volte è richiesta ed alle volte no;
- l'**integrità** è invece quasi sempre critica ed indica che l'informazione è completa e non corrotta;
- la **disponibilità** riguarda la possibilità di accedere ad una certa informazione ed è critica solo in certi momenti e per certi servizi; l'attacco intenzionale alla disponibilità è detto **negazione del servizio** (*denial of service*);
- l'**autenticità**, o **genuinità**, di un informazione è critica quando occorre individuare con certezza chi l'ha originata; l'attacco intenzionale all'autenticità è detto **falsificazione** (*fabrication*);

Queste quattro proprietà costituiscono lo "zoccolo duro" per la sicurezza per tutti i servizi della Società dell'informazione. Altre (come la **tempestività**, l'**anonimato**, la **non ripudiabilità**, l'**impredicibilità**, ecc.) sono richieste in casi ben specifici e saranno discusse più avanti.

Qualche ulteriore commento anche all'elenco degli strumenti per la sicurezza.

La difesa deve essere in generale organizzata su tre livelli.

Al livello più alto si colloca la definizione di una **politica di sicurezza**, cioè di un insieme di regole, di principi e di procedure che stabiliscano come un'Organizzazione intende gestire, proteggere e controllare le proprie risorse informatiche e le informazioni in esse contenute. La definizione della politica deve discendere dalla conoscenza degli eventi che possono costituire una minaccia, dalla stima della loro probabilità d'occorrenza e dalla previsione dell'impatto che possono avere sul conseguimento degli obiettivi dell'Organizzazione.

Al secondo livello si deve mettere in conto l'**addestramento** del personale, mirato a fargli sia rigorosamente rispettare le procedure di sicurezza individuate nel livello superiore, sia correttamente impiegare le tecnologie scelte nel livello sottostante.

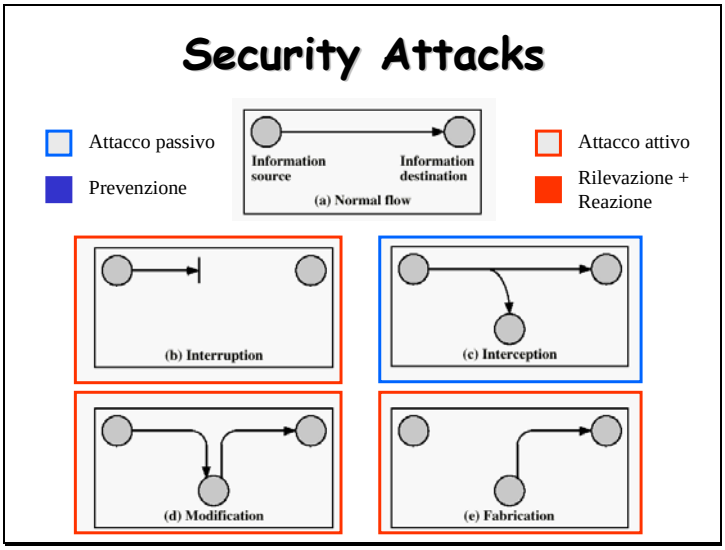
Il terzo passo è la **scelta** e **la messa in opera** di tecnologie per la sicurezza.

1.3.5 Meccanismi e servizi per la sicurezza

Con **attacco intenzionale** si intenderà da ora in poi ogni azione mirante a compromettere una proprietà critica dell'informazione in una qualsiasi delle sue tre fasi di vita. Per classificare le modalità d'attacco, le proprietà minacciate e le contromisure con cui difenderle, è utile introdurre il modello[4] del canale **insicuro**:
"**al canale che connette una sorgente legittima ed una destinazione legittima può accedere illecitamente anche un intruso**".

[3] Il modello è stato proposto da National Security Telecommunications and Information Systems Security Committee.

[4] C. E. Shannon "Communication Theory and Secrecy Systems", B.S.T.J. n.28, aprile 1949. Il lavoro contiene gli studi fatti da S. per conto della U:S: Navy durante la II[a] Guerra Mondiale e getta le fondamenta di quella che sarebbe poi diventata la Teoria dell'Informazione



L'attacco è detto **passivo** se l'intruso può solo intercettare i messaggi in transito sul canale (*interception*). Ciò gli può consentire di ricavare informazioni sul traffico e di minacciare la riservatezza della comunicazione.

L'attacco è detto **attivo** se l'intruso può interrompere il traffico (*interruption*), modificare i messaggi generati dalla sorgente (*modification*), inserire messaggi di sua invenzione attribuendoli alla sorgente (*fabrication*).

L'**interruzione** è una minaccia alla fruibilità dell'informazione.

La **modifica** di messaggi minaccia l'integrità dell'informazione.

La **contraffazione** è una minaccia all'autenticità dell'informazione.

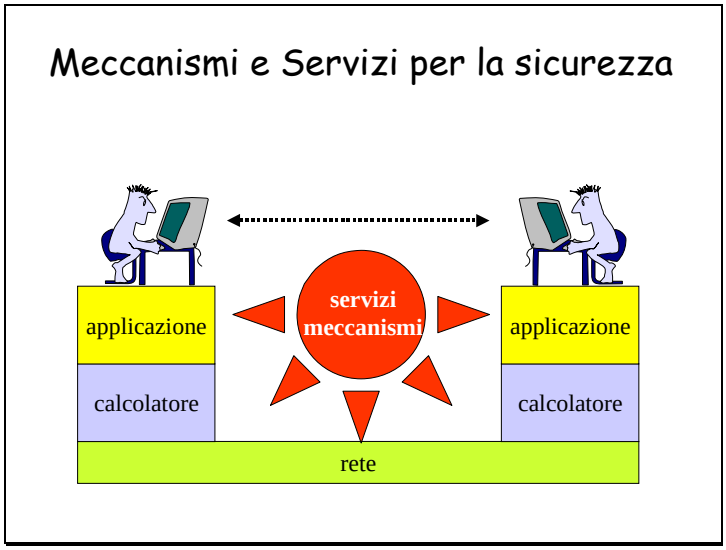
Il tipo di attacco influisce sul tipo di contromisura che occorre adottare:

- l'**attacco passivo** è difficile da rilevare e la difesa deve essere quindi basata sulla **prevenzione**;
- l'**attacco attivo** è difficile da prevenire ed occorre quindi basare la difesa su **rilevazione** e **reazione**.

Le contromisure predisposte dalle tecnologie per la sicurezza si articolano in:

- **meccanismi di sicurezza**, che svolgono azioni protettive per singole e specifiche vulnerabilità,
- **servizi di sicurezza**, che sfruttano in generale più meccanismi per proteggere una o più proprietà critiche dell'informazione.

La **collocazione** di questi strumenti influisce fortemente sulla efficienza, sull'efficacia e sulla sicurezza.



Consideriamo una generica applicazione distribuita, in cui due utenti remoti interagiscono scambiandosi informazioni in tempo reale.

In realtà essi si avvalgono di tre sottostanti livelli di servizio.

Ai fini dello scambio (inizio/fine della comunicazione, formato e ordine temporale dei messaggi, modalità di elaborazione degli stessi, ecc.) entrambi interagiscono con un programma applicativo che li guida e li aiuta a conseguire il loro fine.

I due programmi, a loro volta, sfruttano le risorse Sw e Hw di due calcolatori.

I due calcolatori infine chiamano in causa i servizi di rete ogniqualvolta un'informazione deve fluire da uno all'altro utente.

Ciascuno di questi tre livelli può ospitare meccanismi e servizi per la sicurezza. Per chiarirsi le idee è sicuramente utile dare un'occhiata alle scelte operate nel passato.

Inizialmente gli accorgimenti protettivi sono stati inclusi nelle singole applicazioni (per questo dette **sicure**), non potendosi fare alcun affidamento sulla sicurezza dei supporti sottostanti.

Il passo successivo dell'evoluzione delle tecnologie per la sicurezza è stato quello di conseguire efficienza e semplicità d'uso considerando gli accorgimenti per la sicurezza come ulteriori risorse che un calcolatore mette a disposizione di tutte le applicazioni (si parla allora di **computer security**).

Attualmente molti sono convinti che lo sviluppo e l'affermazione di applicazioni distribuite richieda la presenza di meccanismi e di servizi per la sicurezza anche negli strati più bassi dei protocolli di comunicazione ed all'interno degli apparati di rete (**network security**).

Ciò però richiede che l'applicazione distribuita sia eseguita su "piattaforme" dotate degli stessi servizi, ma questa proprietà di **interoperabilità** delle applicazioni è oggi tutt'altro che garantita nei prodotti messi a punto da Costruttori diversi.

Proprio per superare questo ostacolo ha ripreso vigore anche il principio di inserire i servizi per la sicurezza in appositi **protocolli del livello applicazione**, come ad esempio è previsto dal modello del **Web service**.

1.3.6 Calcolatori sicuri

In un sistema sicuro (*trusted*) devono dunque essere **inclusi** fin dall'inizio, od eventualmente **aggiunti** successivamente, meccanismi e servizi in grado di controllare il corretto funzionamento del Hw, di verificare l'integrità e l'origine del Sw, di rilevare e bloccare ogni uso potenzialmente pericoloso di queste risorse.

ESEMPI – I calcolatori che l'**Orange book** (il nome discende dal colore della copertina del volume Trusted Computer Systems Evaluation Criteria pubblicato dal governo americano) classifica nelle categorie più alte, la **B** e la **A**, sono il risultato di progetti fin dall'inizio indirizzati al conseguimento di un funzionamento sicuro.

Macchine di questo tipo, progettate negli anni '90, sono risultate particolarmente costose ed hanno trovato impiego soltanto in ambiente militare.

Recentemente Microsoft, Intel, IBM, HP e AMD si sono unite in una *Trusted Computing Platform Alliance* per definire le specifiche di macchine a basso costo in grado di impedire, tramite un chip aggiuntivo detto Fritz ed un apposito sistema operativo detto Nexus, che le configurazioni hardware e software subiscano modifiche illecite, che siano utilizzate da chi non ne ha regolarmente acquisito i diritti d'uso e che software malizioso riesca ad aver accesso a dati riservati (v. www.trustedcomputinggroup.org). La piattaforma proposta ha l'indubbio pregio di difendere i diritti d'autore dei Venditori di HW e di SW, ma anche il grave difetto di togliere al proprietario della macchina gran parte del controllo su quello che ha fatto o che vuole fare ed ha di conseguenza creato polemiche di ogni tipo.

Un approccio diverso e più tradizionale è quello di far gestire le risorse di calcolatori originariamente insicuri da **sistemi operativi trusted**: in questa direzione si sono ad esempio mosse diverse estensioni di **Unix** e le più recenti versioni di **Linux**[5].

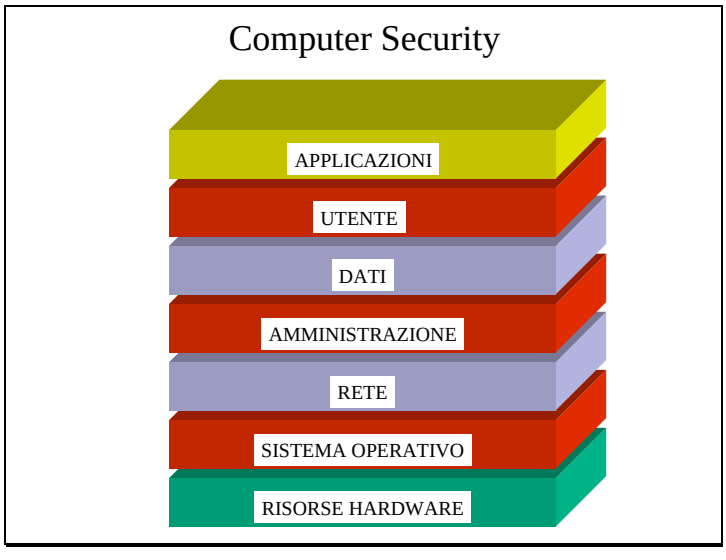
Esistono infine macchine insicure special purpose dedicate a particolari servizi, la cui sicurezza è stata interamente affidata ad un **co-processore** che le affianca e che si prende carico di garantire l'integrità, l'autenticità e la riservatezza dei messaggi che scambiano con l'esterno. In questa categoria ricadono ad esempio gli **apparati mobili** dei sistemi di telecomunicazione di seconda (**GSM**) e di terza generazione (**UMTS**).

La più importante difesa preventiva adottata nei calcolatori sicuri è il **controllo d'accesso**, quale risulta definito dalla seguente politica di sicurezza.

- R1: *"L'accesso ad ogni risorsa HW e SW di un sistema informatico e la sua modalità d'uso devono essere regolamentati; le autorizzazioni concesse ad un utente non devono poter essere usate da altri"*.

L'attuazione del **controllo d'accesso** si basa su tre particolari **servizi**, spesso indicati con la sigla 3A:

- **Autenticazione –** deve esistere una lista degli utenti (o dei gruppi di utenti) potenziali ed un servizio per l'identificazione sicura di chi sta richiedendo l'uso della macchina;
- **Autorizzazione –** deve esistere una lista delle modalità d'uso di ogni risorsa da parte di ogni utente potenziale (ACL da *Access Control List*) ed un meccanismo che impedisce lo svolgimento di azioni non autorizzate;
- **Amministrazione –** deve esistere un *amministratore di sistema*, unico in grado di apportare modifiche alla lista degli utenti, a quella delle risorse ed a quella delle loro modalità d'impiego.



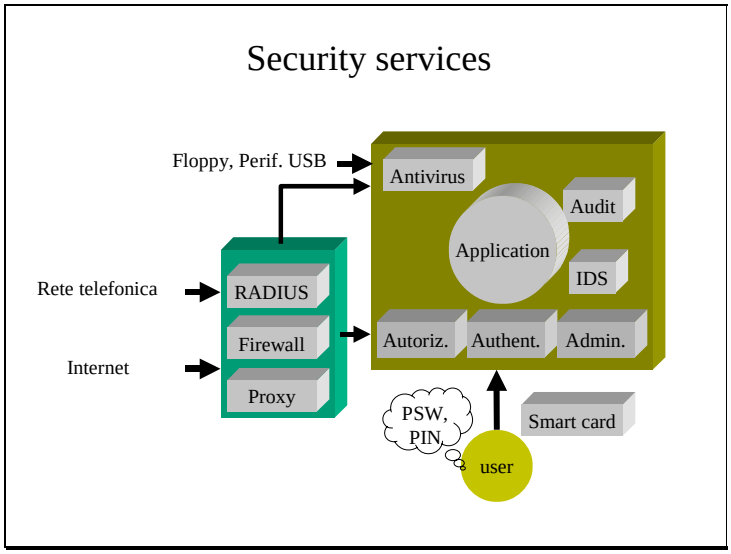
In un calcolatore sicuro il controllo d'accesso è distribuito su tutti gli strati.

L'attività di autenticazione è allocata nel livello *user*, uno strato appositamente interposto tra applicazioni e dati ed adibito a contenere tutte le informazioni relative agli utenti potenziali ed agli utenti attivi.

L'attività di autorizzazione è assegnata al S. O., spesso con l'ausilio di hardware, ed è chiamata in causa dal livello *application*.

L'attività di amministrazione compete al livello *system administration*; uno strato, interposto tra i dati e la rete, adibito a contenere sia le procedure di gestione delle autorizzazioni, sia le procedure di monitoraggio dell'intero sistema (ad es. i codici di *audit*) ed i dati che documentano le situazioni eccezionali che si sono verificate (ad es. registri degli eventi).

[5] **Trusted Linux** è stato proposto da HP (*Communications of the ACM*, Volume 44, Issue 2). **Security-enhanced Linux** è un prototipo messo a punto dalla National Security Agency negli anni '90 e poi rilasciato come prodotto open source alla fine del 2000 (www.nsa.gov/selinux).



A valle del controllo d'accesso deve essere inoltre previsto un **sistema di rilevazione delle intrusioni** (**IDS** da *Intrusion Detection System*) di *hacker* che sono riusciti a spacciarsi per utenti legittimi, o di utenti legittimi che tentano di fare cose per le quali non hanno l'autorizzazione.

Il rilevamento si basa sul fatto che l'uso delle risorse per una finalità legittima è in generale diverso da quello necessario per una finalità illegittima: analizzando in tempo reale i comportamenti di chi sta impiegando la macchina, tramite statistiche o sulla base di regole predefinite, è dunque possibile accorgersi se è in corso un attacco.

In un calcolatore sicuro occorre anche tenere sotto controllo l'ingresso di file, per impedire che nel sistema siano nascostamente immessi **virus** e **worm**. I prodotti **antivirus** evolvono continuamente ed è quindi una buona pratica di sicurezza tenere installata l'ultima versione.

Di norma oggi una macchina è connessa ad una **rete locale**, a sua volta collegata ad altre reti: occorre dunque esercitare un attento controllo anche sui dati e sui comandi che possono arrivare da punti remoti.

Il compito può essere svolto o da programmi installati su tutte le macchine, o da appositi server a disposizione di tutte.

ESEMPI – Il protocollo RADIUS (*Remote Authentication Dial-In User Service*) controlla gli accessi dalla rete telefonica pubblica. Gli accessi tramite Internet sono controllati da **firewall** e da **server proxy**.

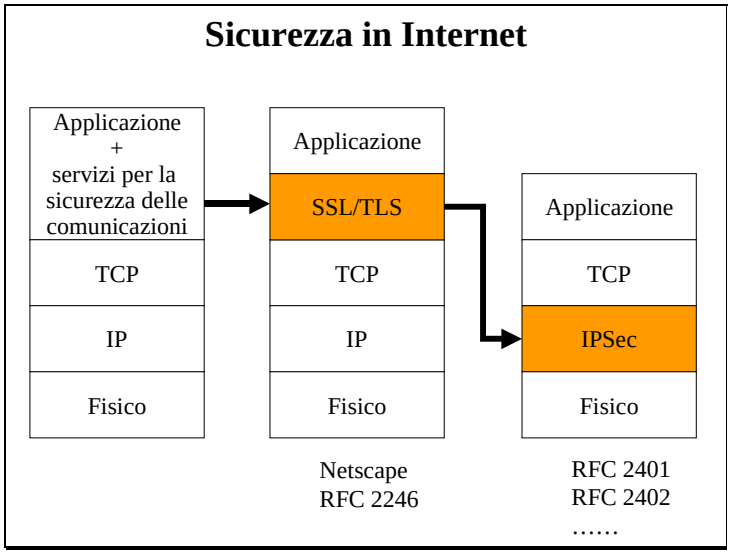
1.3.7 Reti sicure

E' opinione sempre più largamente condivisa che le applicazioni distribuite richieste dai servizi della Società dell'informazione debbano potersi avvalere di una rete in grado di fronteggiare attacchi intenzionali.

Per garantire la sicurezza di un trasferimento di dati, *end-to-end* e/o *link-by-link*, i terminali e gli apparati di rete devono disporre di meccanismi per:

- l'identificazione sicura di chi sta comunicando,
- l'autenticazione dell'integrità e dell'origine di tutti i messaggi scambiati,
- la difesa della loro riservatezza durante il trasporto.

Un problema non facile, sia per la molteplicità delle soluzioni possibili, sia per la necessità di preservare la compatibilità con la preesistente pila dei servizi, è stato quello di decidere dove collocare i meccanismi per la sicurezza inizialmente previsti nelle sole applicazioni.



Dapprima ci si è preoccupati solo di difesa della riservatezza, inserendo i relativi meccanismi sui *data link* più vulnerabili.

Unanimi consensi ha poi trovato la proposta, fatta da Netscape, di collocare uno strato per la sicurezza (**SSL** da *Secure Sockets Layer*) tra i livelli di applicazione e di trasporto.

Le tre successive versioni del protocollo hanno creato uno standard *de facto*, diventato poi uno standard Internet con la denominazione **TLS** (RFC 2246).

IETF ha recentemente proposto e sta sperimentando il *framework* **IPSec** (RFC 2401, 2402, 2406, 2408), un ambiente sicuro a livello di rete che mette a disposizione degli utenti un'ampia gamma di politiche, di servizi e di meccanismi con cui gestire tutto il loro traffico.