Un computer è formato da:

- **Hardware:** struttura fisica del calcolatore formata da parti meccaniche, elettriche ed elettroniche;
- **Software:** componente del calcolatore costituita dai programmi di base e dai programmi applicativi per la gestione e l'uso del sistema;
- **Firmware:** software cablato direttamente in chip hardware non facilmente modificabile. È un programma, ovvero una sequenza di istruzioni, integrato direttamente in un componente elettronico nel senso più vasto del termine. Il suo scopo è quello di avviare il componente stesso e consentirgli di interagire con altri componenti hardware tramite l'implementazione di protocolli.

INFORMATICA: UNA PANORAMICA GENERALE

CAPITOLO 1 – MEMORIZZAZIONE DEI DATI

1.1 BIT E LA LORO MEMORIZZAZIONE

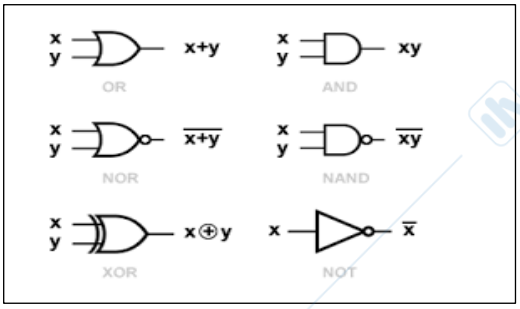
Nei computer le informazioni sono codificate come pattern di 0 e 1, queste cifre sono chiamate **bit**. Sono utilizzati per rappresentare valori numerici, suoni, immagini, lettere ecc…

Il bit 0 rappresenta il valore falso mentre il bit 1 il valore vero. Le operazioni che trattano questi valori sono dette operazione **booleane**. Le operazioni di base sono:

- **AND**: è definita in modo da riflettere la verità o la falsità di un'asserzione.
  0 and 0 → 0
  1 and 1 → 1
  0 and 1 → 0
  1 and 0 → 0
- **OR**: le asserzioni di questo tipo sono vere quando almeno una delle due lo è:
  0 or 0 → 0
  1 or 1 → 1
  1 or 0 → 1
  0 or 1 → 1
- **XOR**: da un output uguale a 1 quando uno dei suoi input è uguale a 1 e l'altro è 0.
  0 xor 0 → 0
  1 xor 1 → 0
  1 xor 0 → 1
  0 xor 1 → 1
- **NOT**: ha solo un input, il suo output è l'opposto di input

PORTE LOGICHE E CIRCUITI FLIP-FLOP

Un dispositivo che produce un output è chiamato **porta logica**. Le porte AND, OR, XOR e NOT sono rappresentate da un simbolo diverso →



Un circuito **flip-flop** è un'unità fondamentale della memoria del computer. Produce un valore di output 0 o 1, che rimane costante finché un impulso su una delle linee di input non lo trasforma nell'altro valore. È possibile impostare l'output di un flip-flop in modo che ricordi uno 0 o un 1 sotto il controllo de stimoli esterni. Il flip-flop costituisce un set di elementi base per la creazione di una circuiteria più complessa. Anche la circuiteria interna dei computer ha una struttura gerarchica. È possibile utilizzare molti flip-flop, costruiti come piccolissimi circuiti elettrici.

1.2 MEMORIA PRINCIPALE

I circuiti della memoria principale sono organizzati in unità gestibili chiamate **celle,** con dimensione di **8bit→ byte** (stringa di 8 bit).

L'estremità sinistra di ciascuna riga è detta **ordine alto** e il bit a questa estremità è detto **bit più significativo**, l'estremità destra di ciascuna riga è detto **ordine basso** e il bit a questa estremità è detto **bit meno significativo**.

Le celle vengono identificate con un **indirizzo** interamente numerico. Se la memoria è divisa in celle di un byte si può archiviare una stringa di 16 byte in solo 2 celle di memoria consecutive. Questi circuiti esterni posso richiedere i contenuti di un certo indirizzo → **lettura**, oppure possono registrare informazioni nella memoria richiedendo che un certo pattern di bit sia posto nella cella che ha un determinato indirizzo → **scrittura.**

La memoria è spesso chiamata **RAM** per indicare la capacità di accedere alle celle in qualsiasi ordine.

I circuiti però alle volte necessitano di una circuiteria supplementare, circuito di aggiornamento, chiamata **DRAM**, **memoria dinamica**.

MISURAZIONE DELLA CAPACITÀ DI MEMORIA

La dimensione delle memorie era di 1024 celle. Molti informatici hanno adottato per questo numero il prefisso kilo. 1 kilobyte è stato usato per indicare 1024 byte di memoria. Se la memoria aveva 4096 byte→ 4KB. Sono stati utilizzati man mano anche i Megabyte, Gigabyte e Terabyte.

1.3 MEMORIA DI MASSA

La maggior parte dei computer è fornita di dispositivi aggiuntivi chiamati **sistemi di memoria di massa**. Ne esistono di vari tipi:

- **Sistemi magnetici** → es: disco magnetico o hard-disk. Le testine di scrittura/lettura sono poste sopra e sotto il disco, in modo che durante la rotazione ciascuna testina percorra un cerchio, chiamato **traccia.** I sistemi disco consistono spesso in più dischi montati su un perno comune, in questi casi le testine si muovono simultaneamente; ogni volta che sono riposizionate diventa accessibile un nuovo insieme di tracce, dette **cilindro.** Ogni traccia è divisa in archi, detti **settori.** Ogni traccia contiene lo stesso numero di settori e ogni settore contiene lo stesso numero di bit (512byte-512Kbyte).
  Nei sistemi a memorizzazione ad alta capacità le tracce vicine al bordo esterno possono contenere molti più settori di quelle vicino al centro, applicando una tecnica chiamata **registrazione dei bit a zona.** Numerose tracce adiacenti vengono raggruppate in zone: un disco tipicamente ne contiene 10. Per valutare le prestazioni di un sistema a disco si tiene conto di:
  1. Tempo di posizionamento
  2. Ritardo di rotazione o tempo di latenza
  3. Tempo di accesso
  4. Velocità di trasferimento

- **Sistemi ottici** → CD. Le informazioni vengono registrate su di essi creando minuscoli fori sulle superfici riflettenti, e possono essere recuperate tramite un raggio laser che rivela le irregolarità del CD mentre questo gira. I CD hanno capacità comprese tra 600 e 700 MB. I DVD forniscono capacità di molti GB.

- **Unità flash** → in un sistema di memoria flash i bit vengono memorizzati inviando segnali elettrici direttamente al dispositivo di memorizzazione, dove gli elettroni vengono intrappolati in piccole celle di biossido di silicio. Le celle possono trattenere gli elettroni per molti anni anche senza alimentazione esterna.
  Dispositivi di memorizzazione flash di grandi capacità, detti **unità flash**, sono esplicitamente progettati per sostituire le unità disco magnetiche.
  Un'altra applicazione delle unità flash è costituita dalle schede di memoria SD che offrono fino a 2 GB di memoria.

1.4 RAPPRESENTAZIONE DELLE INFORMAZIONI COME PATTERN DI BIT

- **Rappresentazione di testo** → l'ANSI ha adottato il codice ASCII. Questo codice usa pattern di 7 bit, oggi viene spesso utilizzato un pattern a 8 bit per simbolo che permettono la riproduzione di 128 pattern non compresi nel linguaggio ASCII.

UNICODE utilizza un pattern univoco fino a 12 bit per rappresentare ogni simbolo. Quando il set di caratteri Unicode è combinato con UTF-8 (pattern di 24 o 32 bit), i caratteri ASCII possono essere rappresentati con 8 bit.

- **Rappresentazione di valori numerici** → viene utilizzata la notazione binaria

- **Rappresentazione di immagini → Pixel.** L'aspetto di ciascun pixel viene codificato e l'intera immagine è rappresentata come **bitmap**. Nel caso di immagini semplici in bianco e nero ogni pixel può essere rappresentato da un singolo bit. Per immagini in bianco e nero più elaborate avremo una collezione di bit. Per immagini a colori abbiamo due approcci:
  1. **RGB:** ogni pixel è rappresentato come combinazione dei 3 colori primari
  2. **Un competente di luminosità+2 componenti di colore:** luminanza del pixel è la somma dei componenti di rosso, blu e verde. Gli altri due componenti (crominanza di rosso e di blu) sono determinati calcolando la differenza tra luminanza del pixel e quantità di luce rossa e blu.

  Quando però si ingrandisce l'immagine questa apparirà sgranata. Un modo per evitare ciò consiste nel descrivere l'immagine come un insieme di strutture geometriche.

- **Rappresentazione di suoni** → un primo metodo consiste nel campionare l'ampiezza dell'onda sonora a intervalli regolari e nel registrare le serie di valori numerici ottenuti. Questa tecnica usa una frequenza di campionamento di 8000 campioni al secondo.
  Per una riproduzione sonora di qualità viene usata una frequenza di 44100 campioni al secondo.
  Un sistema di codifica alternativo **MIDI** codifica le istruzioni necessarie a produrre la musica su un sintetizzatore anziché codificare il suono stesso.

1.5 SISTEMA BINARIO

Nella notazione binaria la posizione di ciascuna cifra è associata a una quantità, ma questa è il doppio della quantità associata alla posizione alla sua destra.

101101 → (1x1=1; 0x2=0; 1x4= 4; 0x8= 0; 0x16=0; 1x32=32) → (1 + 4 + 32) = 37

13 → 13÷2= 6 resto 1; 6÷2= 3 resto 0; 3÷2= 1 resto 1; 1÷2= 0 resto 1 (poiché il quoziente è 0 non si procede oltre. = 1101

1.9 COMPRESSIONE DEI DATI

Gli schemi di compressione rientrano in due categorie: **con perdita dati (lossy)** e **senza perdita dati (lossless)**.

Le tecniche con perdita forniscono maggiore compressione, sono molto diffuse nei casi in cui possono essere tollerati alcuni piccoli errori.

- **Compressione dati→** Quando i dati da comprimere sono costituiti da lunghe sequenze dello stesso valore si usa la **codifica run-lenght**: tecnica lossless che consiste nel sostituire la sequenza con un codice che indica il valore ripetuto e quante volte si ripresenta nella sequenza.

  Un altro approccio è la **codifica dipendente della frequenza**: la lunghezza del pattern di bit usato per rappresentare un elemento è inversamente proporzionale alla frequenza di utilizzo dell'elemento stesso → **codici a lunghezza variabile** (al contrario degli Unicode) → **codici di Huffman.**

  In alcuni casi le informazioni sono costituite da blocchi, ognuno dei quali differisce leggermente dal precedente. In queste circostanze sono utili le tecniche che impiegano la **codifica relativa** o **codifica differenziale**: vengono registrate le differenze tra blocchi di dati consecutivi anziché i blocchi stessi. Questa può essere implementata sia nei sistemi con perdita che in quelli senza perdita.

  Altri sistemi di compressione si basano sulle tecniche di **codifica basata sul dizionario** (dizionario= insieme di blocchi sui quali è costruito il messaggio da comprimere). Sono considerati in genere senza perdita.

  Un'altra variante è la **codifica adattiva basata sul dizionario** in cui il dizionario può variare durante la codifica. Ad esempio la codifica **LZW:** si parte da un dizionario che contiene gli elementi di base del messaggio; qualora si dovessero incontrare blocchi più grandi nel messaggio, questi verranno aggiunti al dizionario in modo da poter codificare come riferimenti singoli occorrenze future di tali blocchi.

- **Compressione immagini→ GIF** è un sistema di codifica basato su dizionario sviluppato da CompuServe. Riduce a 256 il numero di colori che possono essere assegnati a un pixel. È con perdita quando viene applicato a un'immagine arbitraria, perché i colori nella tavolozza possono non essere identici a quelli dell'immagine originale.

  JPEG comprende diversi metodi di compressione delle immagini. È disponibile un metodo senza perdita che non produce livelli di compressione elevati. Standard JPEG di base richiede una sequenza di passi: effettuare una media dei valori di crominanza su quadratini di 2x2 pixel; dividere l'immagine in blocchi di 8x8 pixel. Comprime le immagini a colori di un fattore minimo di 10 a un massimo di 30, senza perdita.

- **Compressione audio e video→ MPEG** prevede una gamma di standard per le diverse applicazioni. La compressione si basa sul fatto che il video è costituito da una sequenza di immagini. Solo alcuni fotogrammi, **fotogrammi-I,** sono codificati interamente.

  MP3: mascheramento temporale fa si che per un breve periodo dopo un suono molto forte, l'orecchio non riesca a individuare suoni più lievi. **Mascheramento di frequenza** fa si che un suono a una determinata frequenza tenda a mascherare suoni più deboli.

CAPITOLO 2 – ELABORAZIONE DEI DATI

2.1 ARCHITETTURA DEI COMPUTER

La circuiteria del computer è denominata **CPU** o precessore. È composta da 3 parti: **unità aritmetico/logica** che racchiude i circuiti che eseguono l'elaborazione dei dati**, unità di controllo e unità dei registri** che contiene celle di memorizzazione dati. Alcuni registri sono considerati **generici** altri invece **specifici**. I registri generici servono per la memorizzazione temporanea dei dati. Per traferire i dati, l'unità centrale e la memoria principale sono collegate da un insieme di fili detti **bus.**

Tramite i bus la CPU è in grado di estrarre i dati dalla memoria principale specificando l'indirizzo della relativa cella di memoria e un segnale di scrittura.

CONCETTO DI PROGRAMMA MEMORIZZATO

Se l'unità di controllo è progettata per estrarre il programma dalla memoria, decodificare le istruzioni ed eseguirle, il programma può essere modificato semplicemente cambiando il contenuto della memoria del computer.

2.2 LINGUAGGIO MACCHINA

L'insieme di istruzioni della CPU è detto **linguaggio macchina**. Diverse filosofie nelle progettazioni della CPU:

- La prima prevede che l'unità centrale debba essere progettata per eseguire solo un insieme minimo di istruzioni macchina e concretizza nella CPU di tipo **RISC**. Un computer di questo tipo è efficiente, veloce e costa poco costruirlo.
- CPU in grado di eseguire molte istruzioni complesse, anche se molte sono tecnicamente ridondanti → CPU di tipo **CISC**. Consente ai programmi di sfruttare un ricco e potente set di istruzioni

Le istruzioni macchina sono classificate in 3 gruppi:

1. **Trasferimento dei dati** → eseguono lo spostamento dei dati da una posizione all'altra. La richiesta di riempire un registro generico con i contenuti di una cella di memoria è comunemente chiamata LOAD. La richiesta di trasferimento dei contenuti di un registro a una cella di memoria è chiamata STORE.
2. **Istruzioni aritmetico/logiche** → è costituito da istruzioni che comunicano all'unità di controllo la richiesta di eseguire un'attività all'interno dell'unità aritmetico/logica. Questa è in grado di portare a termine operazioni anche diverse da quelle aritmetiche di base. Alcune di queste operazioni sono AND, NOT, XOR e OR.
3. **Istruzioni di controllo** → il gruppo di controllo è costituito dalle istruzioni che regolano l'esecuzione del programma anziché l'elaborazione dei dati. Questo gruppo contiene molte delle istruzioni più interessanti del repertorio di una macchina. Esempio l'istruzione Jump che dice alla CPU di eseguire un'istruzione diversa dalla successiva.

Abbiamo **salti condizionati** (se il valore ottenuto è 0 salta al passo 5) e **salti incondizionati** (salta al passo 5)**.**

La versione codificata di un'istruzione macchina è formata da due parti: **il campo codice operativo** (indicano quale operazione elementare è richiesta) **e il campo operando** (i pattern in questo campo forniscono informazioni più dettagliate sull'operazione specificata dal codice operativo)**.**
L'intero linguaggio macchina è costituito da sole 12 istruzioni base, ognuna delle quali è codificata con 16 bit. Il codice operativo è composto dai primi 4 bit o dalla prima cifra esadecimale. Il campo operando di ogni istruzione di tre cifre esadecimali (12 bit). Nelle istruzioni 8 bit sono riservati per specificare la cella di memoria usata dall'istruzione.

2.3 ESECUZIONE DEI PROGRAMMI

Due registri presenti nella CPU per il processo di esecuzione:

- **Contatore di programmi** → contiene l'indirizzo dell'istruzione successiva da eseguire.
- **Registro delle istruzioni** → è usato come contenitore delle istruzioni da eseguire.

La CPU svolge il suo compito ripetendo un algoritmo che la guida attraverso un processo a tre fasi → **ciclo macchina.** Le tre fasi sono: reperimento, decodifica ed esecuzione. Durante il reperimento la CPU richiede che la memoria principale fornisca l'istruzione memorizzata all'indirizzo indicato dal contatore di programma della CPU. La CPU decodifica, quindi scompone il campo operando nei suoi componenti sulla base del codice operativo

PROGRAMMI E DATI

Nella memoria principale possono essere archiviati simultaneamente più programmi. Si può stabile quale programma sarà eseguito all'attivazione della memoria solo impostando in modo adeguato il registro contatore di programma. Questo perché nella memoria sono contenuti anche in forma binaria i dati codificati, il computer non è quindi in grado di distinguerli quali sono i dati e quale invece è il programma.

2.5 COMUNICAZIONE CON ALTRI DISPOSITIVI

RUOLO DEI CONTROLLER

La comunicazione tra un computer e altri dispositivi è gestita dai **controller.** Un controller effettua le conversioni di messaggi e dati tra il formato compatibile con le caratteristiche interne del computer e quello richiesto dalla periferica cui è collegato.
Vengono usati spesso USB e FireWire.
Ciascuno controller comunica con il computer tramite le sue connessioni allo stesso bus che connette la CPU e la memoria principale. Il computer è in grado di controllare i segnali che passano tra la CPU e la memoria principale, e anche di immetterne di propri sul bus.

In alcune architetture, il trasferimento dei dati verso e dai controller è diretto dagli stessi codici operativi LOAD e STORE già utilizzati per la comunicazione con la memoria principale. Quando la CPU invia un messaggio sul bus per memorizzare un pattern di bit in una posizione di memoria che è stata assegnata a un controller, il pattern viene ricevuto dal controller anziché dalla memoria principale. Se la CPU cerca di leggere dati da questa posizione usando un'istruzione LOAD riceverà un pattern di bit proveniente dal controller anziché dalla memoria principale. Un sistema di comunicazione di questo tipo è definito **memory-mapped I/O**. un'alternativa consiste nell'inserire codici operativi speciali nel linguaggio macchina per indirizzare i trasferimenti ai e dai controller.

DIRECT MEMORY ACCESS (DMA)

Capacità dei controller di accedere alla memoria principale nei nanosecondi in cui la CPU non utilizza il bus. L'utilizzo dell'accesso DMA ha anche effetto negativo → complica il traffico gestito dal bus. Il coordinamento delle attività sul bus è un problema di progettazione la cui risoluzione è piuttosto complessa.
Tale impedimento è noto come **collo di bottiglia di Von Neumann.**

HANDSHAKING

La stampa di un documento implica un costante dialogo bidirezionale detto **handshaking,** in cui il computer e la periferica si aggiornano l'un l'altro sul proprio stato e coordinano le loro attività. Questo dialogo implica una **parola di stato**, cioè un pattern di bit che riflettono la condizione del dispositivo periferico.

MEZZI DI COMUNICAZIONE PIÙ DIFFUSI

Due tipi di percorsi di comunicazione:

- **Comunicazione parallela** → sono trasferiti più segnali contemporaneamente, ognuno su una diversa linea. Trasferimento rapido ma percorso complesso.
- **Comunicazione seriale** → trasferimento di un solo segnale alla volta. Tecnica più lenta ma strutturalmente più semplice.

VELOCITÀ DI TRAFERIMENTO DATI

La velocità massima possibile in un caso particolare dipende dal tipo di percorso di comunicazione e dalla tecnologia impiegata → **larghezza di banda.**

CAPITOLO 3 – SISTEMI OPERATIVI

Un **sistema operativo** è il software che controlla le operazioni complessive di un computer, fornendo i mezzi attraverso i quali un utente può memorizzare e recuperare i file, l'interfaccia per richiedere l'esecuzione dei programmi e l'ambiente necessario per eseguirli.

3.1 EVOLUZIONE DEI SISTEMI OPERATIVI

L'esecuzione di ogni programma è chiamato **job**. Il caricamento di job riuniti in un singolo batch e la loro successiva esecuzione senza ulteriori interazioni con l'utente è detta **elaborazione di batch**.

Nei sistemi a elaborazione di batch, i job presenti nella memoria di massa aspettano l'esecuzione in una **coda di job**. Una cosa è una struttura dati in cui gli oggetti sono ordinati secondo il metodo **FIFO.** Gli oggetti vengono rimossi dalla coda nell'ordine di arrivo. In questi primi sistemi a ogni job era abbinato uno specifico insieme di istruzioni che descrivevano le fasi necessarie alla preparazione del computer. Tali istruzioni erano codificate in JCL e memorizzate nella coda insieme con il job cui facevano riferimento.

Lo svantaggio principale dell'uso di un operatore come intermediario tra il computer e gli utenti sta nel fatto che questi ultimi non hanno alcuna possibilità di interagire con i propri programmi dopo averli consegnati all'operatore. Sono stati sviluppati sistemi operativi in grado di garantire l'esecuzione di programmi che prevedevano un dialogo con l'utente tramite stazioni di lavoro o terminali remoti. Questa funzione è nota come **elaborazione interattiva.**

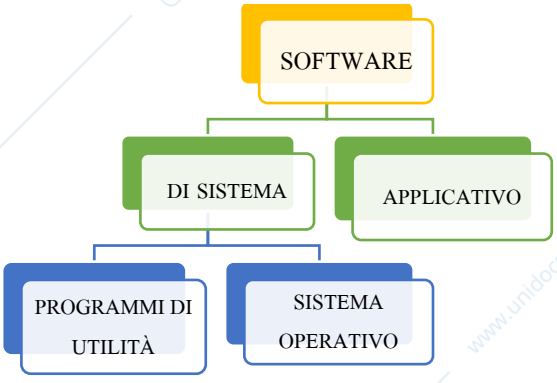
Il computer è obbligato a eseguire le sue attività in base a una scadenza; tale processo prese il nome di **elaborazione in tempo reale.**

Se il sistema operativo di un ambiente multiutente di questo tipo avesse continuato a eseguire un job alla volta, soltanto un utente avrebbe ricevuto un servizio un servizio soddisfacente in tempo reale. La soluzione a questo problema fu progettare sistemi operativi che fornissero i servizi contemporaneamente a più utenti mediante **time-sharing**. Sistema di multiprogrammazione è chiamato **multitasking,** un singolo utente esegue più compiti allo stesso tempo.

3.2 ARCHITETTURA DEL SISTEMA OPERATIVO

Due categorie principali:

- **Software applicativo** → consiste nei programmi per l'esecuzione di compiti particolari.
- **Software di sistema** → svolge compiti che sono comuni ai sistemi di elaborazione in generale. Fornisce l'ambiente in cui risiede il software applicativo. Può a sua volta essere diviso in due categorie:
    - Il sistema operativo
    - Software di utilità → è composto da programmi che eseguono attività fondamentali per la gestione dei computer. Si tratta di software che aumenta le funzionalità del sistema operativo.



COMPONENTI DI UN SISTEMA OPERATIVO

- **Interfaccia utente→** La parte di un sistema che gestisce la comunicazione con l'utente è chiamata **interfaccia utente.** Quelle più moderne sono le **interfacce utente grafica** in cui gli oggetti da manipolare sono rappresentati graficamente sul monitor per mezzo di icone.
    - Window manager: un componente fondamentale all'interno di queste è il **window manager.** Quando un'applicazione vuole visualizzare qualcosa sullo schermo, avvisa il window manager, che indirizza l'uscita nella finestra assegnata all'applicazione. È a sua volta il window manager che calcola la posizione del puntatore sullo schermo.

- **Kernel→** La parte interna di un sistema operativo è chiamata **kernel** e contiene i componenti software che eseguono le funzioni di base del computer.
    - Un componente di questo tipo è il **file manager** il cui compito è coordinare l'uso delle funzionalità relative alla memoria di massa. Gestisce l'archiviazione e il reperimento dei file archiviati. La maggior parte dei file manager prevede che i file siano raggruppati in **directory o cartelle.** Le directory possono a loro volta contenere **sottodirectory.** Una catena di directory è chiamata **percorso.**
    - Il kernel è composto anche da una raccolta di **driver di periferica,** unità software che comunicano con i controller delle periferiche.
    - Un altro componente è il **memory manager** che ha il compito di coordinare l'impiego della memoria principale del computer. Questo tipo di attività è importante in ambienti multitasking o multiutente. Nella memoria principale devono trovarsi contemporaneamente più programmi e blocchi di dati, ognuno dei quali risiede in un'area appositamente riservatagli dal memory manager.
    - **Scheduler e dispatcher** (vedi sotto)

AVVIO DEL SISTEMA OPERATIVO

L'avvio del sistema operativo si attua tramite **bootstrap** che il computer esegue ogni volta che viene acceso. È questo processo che trasferisce il sistema operativo dalla memoria di massa a quella principale. È necessario che un programma sia presente nella memoria principale all'accensione del computer, ma la memoria volatile del computer stesso viene cancellata ogni volta che la macchina viene spenta. Viene quindi costruita una memoria non volatile→ **ROM,** il cui contenuto può essere letto ma non alterato. Nella ROM è memorizzato in modo permanente un programma denominato **boot-loader**, che viene eseguito per primo all'accensione della macchina.

Processo di esecuzione del boot-loader + successivo avvio del sistema operativo = **avvio (boot) del computer**

3.3 COORDINAMENTO DELLE ATTIVITÀ DELLA MACCHINA

Due concetti importanti dei sistemi operativi:

- **Processo** → attività dinamica le cui proprietà cambiano con il loro passare del tempo
- **Programma** → insieme statico di istruzioni. La sua attività di esecuzione è il processo.

AMMONISTRAZIONE DEI PROCESSI

Le attività associate al coordinamento dei processi sono gestite da scheduler e dispatcher.

Scheduler tiene traccia dei processi presenti nel sistema. Quando un utente richiede l'esecuzione di un'applicazione è lo scheduler che aggiunge tale operazione all'insieme del processo corrente. Conserva nella memoria principale un blocco di informazioni chiamato **tabella dei processi.**

Il dispatcher è il componente del kernel che sovrintende all'esecuzione dei processi pianificati. Questo compito viene svolto dividendo il tempo in brevi segmenti detti **timeslice o quanto.** Il passaggio da un processo a un altro è denominato **commutazione di processo.** Ogni volta che un processo inizia il suo quanto di tempo, il dispatcher attiva un temporizzatore che misurerà il quanto successivo. Alla fine del quanto, il temporizzatore genera un segnale chiamato **interrupt.**

La CPU completa il ciclo macchina, salva la sua posizione nel processo corrente e inizia a eseguire un programma chiamato **gestore degli interrupt.**

L'effetto del segnale di interrupt è quindi l'interruzione del processo e il trasferimento del controllo al dispatcher. A questo punto il dispatcher sceglie dalla tabella il processo che ha la priorità più alta tra quelli pronti, riavvia il temporizzatore, e consente al processo selezionato di iniziare il suo quanto di tempo.

Per il corretto funzionamento di un sistema multiprogrammato è fondamentale la possibilità di interrompere un processo e riattivarlo successivamente. Il contesto da riprodurre è lo stato del processo che comprende il valore del contatore di programma e anche i contenuti dei registri e delle celle di memoria appropriate. Nelle macchine progettate per essere multiprogrammate il salvataggio di queste informazioni è parte della reazione della CPU al segnale di interrupt.

Queste funzioni facilitano il compito del dispatcher nell'eseguire una commutazione di processo e costituiscono un buon esempio dell'influenza delle esigenze dei sistemi operativi sulla progettazione dei computer moderni. L'uso della multiprogrammazione ha portato ad un aumento dell'efficienza complessiva di una macchina. Senza la multiprogrammazione ogni processo viene completato prima che inizi quello successivo, e ciò significa che viene sprecato molto tempo aspettando che i dispositivi periferici completino i task o che un utente faccia la richiesta successiva.

In questo caso lo scheduler aggiorna la tabella dei processi in modo che rifletta lo stato di attesa e il dispatcher assegna un nuovo quanto a un processo pronto. In seguito quando il controller indicherà che la richiesta di I/O è stata completata, lo scheduler riclassificherà il processo come pronto. Mentre la richiesta di I/O viene eseguita possono essere portati avanti molti altri task e così l'intero insieme di processi potrà arrivare a termine in un tempo totale minore del caso in cui i processi stessi fossero eseguiti in sequenza uno dopo l'altro.

3.4 GESTIONE DELLA COMPETIZIONE TRA PROCESSI

Un compito importante del sistema operativo è l'assegnazione delle risorse del computer ai processi. Il file manager assegna l'accesso ai file o lo spazio del disco per la creazione di nuovi file; il memory manager assegna lo spazio in memoria; lo scheduler assegna lo spazio nella tabella dei processi e il dispatcher le porzioni di tempo.
Quando un processo deve stampare i suoi risultati richiede al sistema operativo l'accesso al driver della stampante. A questo punto il sistema operativo decide il da farsi: se la stampante non è già impiegata da un altro processo, il sistema operativo deve garantire l'accesso e permettere al processo di continuare. Il sistema operativo deve tenere traccia delle sue assegnazioni. Vengono usati dei flag:
stato set (impegnato) stato clear (libero).

STALLO

Condizione in cui due o più processi non possono continuare perché ognuno attende l'accesso a risorse destinate all'altro.
L'analisi degli stalli ha rilevato che essi possono verificarsi solo se sono soddisfatte tutte e tre le condizioni:

1. Competizione per risorse non condivisibili
2. Le risorse sono richieste su base parziale; cioè un processo può richiedere anche altre risorse in secondo momento.
3. Una volta che una risorsa è stata assegnata a un processo, non può essere recuperata forzatamente.

3.5 SICUREZZA

ATTACCHI ESTERNI

Per controllare l'accesso il sistema operativo usa delle informazioni ad ogni procedura di login. Gli account vengono stabiliti da una persona nota come **superutente o amministratore**. L'amministratore è anche in grado di monitorare l'attività del sistema allo scopo di individuare eventuali comportamenti distruttivi. Un aiuto in questa operazione proviene da diverse utilità, o **software di monitoraggio**, che registrano e quindi analizzano tutto ciò che avviene nel computer. Il software di monitoraggio ricerca anche il **software di sniffing** che registra le attività e le riferisce al potenziale intruso.

ATTACCHI INTERNI

Le CPU di sistemi multiprogrammati sono progettate in modo da operare in uno di due **livelli di privilegio.**

- **Istruzioni privilegiate→** può eseguire tutte le istruzioni nel suo linguaggio macchina. Istruzioni che modificano il contenuto dei registri dei limiti della memoria o il livello di privilegio delle CPU. Alla prima attivazione la CPU è in modalità privilegiata; quando termina il processo di boot, tutte le istruzioni sono eseguibili.
- **Istruzioni non privilegiate→** le istruzioni in linguaggio macchina sono limitate.

CAPITOLO 4 – NETWORKING E INTERNET

4.1 ELEMENTI DONDAMENTALI DELLE RETI

La necessità di condividere informazioni e risorse tra computer ha dato origine alle **reti**. Gli utenti in rete possono scambiarsi messaggi e condividere risorse distribuite su tutto il sistema.

CLASSIFICAZIONE DELLE RETI

Le reti si classificano in:

- **PAN (PERSONAL…)** → è utilizzata per comunicazioni a breve raggio.
- **LAN (LOCAL…)** → è di soluto costituita da una serie di computer distribuiti in un singolo edificio o in un complesso di edifici.
- **MAN (METROPOLITAN…)** → è una rete di dimensione intermedia, come quella di una comunità locale.
- **WAN (WIDE…)** → Una rete geografica collega computer che possono trovarsi in città vicine oppure alle estremità opposte al mondo.

Un'altra dicotomia riguarda la struttura interna delle reti, che può essere di pubblico dominio o gestita da una singola entità. Una rete del primo tipo è detta **rete aperta**, una rete del secondo tipo è detta **rete chiusa o proprietaria.**

Internet è un sistema aperto, in cui la comunicazione è gestita da una serie di standard nota come famiglia di protocolli TCP/IP.

Un altro modo per classificare le reti si basa sulla topologia, cioè sulla configurazione di collegamento dei computer. Due delle tipologie più diffuse sono il bus e la **stella.** La configurazione a stella è diffusa nelle reti wireless, in cui la comunicazione avviene mediante onde radio e la macchina centrale, detta **access point** fa da fulcro del coordinamento di tutte le comunicazioni. A volte si costruisce una rete a bus collegando ciascun computer a una posizione centrale in cui si trova un dispositivo denominato **hub.**

PROTOCOLLI

In una rete bus basata sugli standard Ethernet, per coordinare il diritto a trasmettere messaggi esiste un protocollo noto come **CSMA/CD.** Questo protocollo prevede che ogni messaggio trasmesso da un qualsiasi computer venga inoltrato a tutti i computer sul bus. Ogni computer riceve tutti i messaggi, ma trattiene solo quelli indirizzati a sé stesso. Il risultato è un sistema simile a quello usato da un piccolo gruppo di persone durante una conversazione.

Le reti wireless adottano la politica di cercare di evitare le collisioni anziché di rilevarle, e tali politiche vengono classificate come **Carrier Sense, Multiple Access with Collision Avoidance.**

UNIONE DI RETI

A volte può essere necessario connettere reti esistenti per formare un sistema di comunicazione più esteso.

Il più semplice di essi è il **ripetitore**. Un **ponte** è simile al ripetitore. Considera gli indirizzi di destinazione di ciascun messaggio e inoltra il messaggio solo quando questo è destinato a un computer sull'altro lato. Due macchine che si trovano sullo stesso lato del ponte possono scambiarsi messaggi senza interferire con la comunicazione che avviene all'altro lato.

Un **commutatore** è fondamentalmente un ponte con più connessioni, cosa che gli permette di collegare più bus anziché solo due. Un commutatore considera gli indirizzi di destinazione di tutti i messaggi e inoltra solo quelli destinati agli altri raggi.

In questi casi le reti devono essere connesse in modo da costituire una rete di reti → **internet o inter-rete.** La connessione internet è gestita da dispositivi noti come **router** → computer dedicati all'inoltro di messaggi. I router forniscono collegamenti tra diverse reti ma consentono a ogni rete di conservare le sue particolari caratteristiche interne.

Il processo di inoltro si basa su un sistema di indirizzi per cui a tutti i dispositivi di un'internet vengono assegnati indirizzi univoci.

Una macchina che intenda inviare un messaggio a un'altra rete allega al messaggio l'indirizzo internet della macchina destinataria, quindi invia il messaggio al router locale, che si occupa di inoltrarlo nella direzione giusta.

In ogni router esiste una **tabella di instradamento** che contiene i dati noti al router sulle direzioni in cui i messaggi devono essere inviati.

Il punto in cui una rete si collega a un'internet è detto **gate-way.**

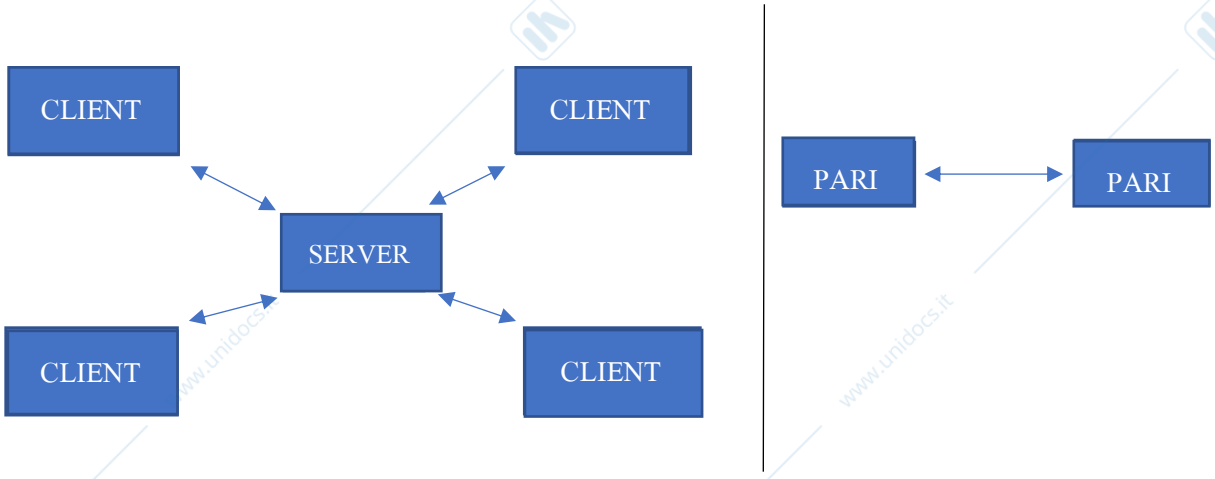
COMUNICAZIONE TRA PROCESSI

Le attività in esecuzione sui vari computer in una rete hanno spesso la necessità di comunicare per coordinare le azioni ed eseguire i compiti loro affidati. Tale correlazione è detta **comunicazione tra processi**. Una convenzione diffusa per questo tipo di comunicazione è la **client/server.**

Client → computer che formula richieste

Server → computer che le soddisfa

Un altro modello è quello **peripatetico**: se il modello client/server implica la comunicazione di un processo con molti altri, quello peripatetico prevede che i processi forniscano e ricevano servizi reciprocamente. Il modello peripatetico coinvolge i processi solo per la durata della loro esecuzione.



SISTEMI DISTRIBUITI

Sistemi costituiti da unità software che eseguono processi su computer diversi. Ne esistono di vari tipi:

- **Cluster computing** → molti computer indipendenti operano in stretta collaborazione per fornire potenza computazionale o servizi paragonabili a quelli di macchina molto più grandi. Sono utilizzati per fornire alta disponibilità e bilanciamento del carico.
- **Grid computing** → i legami sono meno stretti rispetto ai cluster, ma comunque cooperano per svolgere compiti di grande impegno. Può coinvolgere software specializzato per semplificare la distribuzione di dati e algoritmi alle macchine.
- **Cloud computing** → grandissimi gruppi di computer condivisi in rete sono allocabili per l'utilizzo da parte dei clienti all'occorrenza, è l'ultima tendenza nel settore dei sistemi distribuiti.

4.2INTERNET

ARCHITETTURA INTERNET

È un insieme di reti inter-connesse. Tali reti vengono costruite e mantenute da organizzazioni dette **Internet Service Provider** (ISP).

Il sistema di reti gestite da ISP è classificabile in modo gerarchico:

- **ISP di primo livello** → reti geografiche internazionali di alte velocità e capacità. Considerate la spina dorsale di Internet.
- **ISP di secondo livello** → connessi a quelli di primo livello, tendono ad avere una copertura più regionale e a essere meno potenti.

Reti di primo e secondo livello sono dei router che forniscono l'infrastruttura di comunicazione di Internet.

- **ISP d'accesso o terzo livello** → intermediario che fornisce l'accesso al nucleo descritto prima. È un inter-rete indipendente, **intranet**, gestita da una singola autorità che si occupa di fornire accesso a Internet ai singoli utenti.

I dispositivi che i singoli utenti connettono agli ISP di accesso sono noti come **sistemi finali o host**. La strategia prevede la connessone dell'AP a un ISP d'accesso, e quindi la fornitura dell'accesso tramite ISP in questione ai sistemi finali nel raggio di trasmissione dell'AP. La zona coperta dell'AP o da un gruppo di AP è spesso chiamata **hot spot.**

INDIRIZZAMENTO DEI DATI SU INTERNET

Ogni internet necessita di un sistema di indirizzamento che assegni a ciascun computer del sistema un indirizzo univoco, chiamato **indirizzo IP**. Un indirizzo IP era costituito da 32bit ora è in corso il processo di conversione al formato a 128bit. Gli indirizzi IP sono solitamente scritti con **notazione decimale puntata**, nella quale i byte degli indirizzi sono separati da un punto, e ciascun byte è espresso da un intero rappresentato nella tradizionale notazione decimale.

Gli indirizzi in forma di pattern di bit sono ben poco adatti a essere memorizzati dell'utente umano. Tale sistema si basa sul concetto del **dominio**, che può essere considerato una regione di internet gestita da una singola autorità quale un'università.

Ciascun dominio dev'essere registrato presso l'ICANN; il processo è gestito da aziende chiamate **registrar**, il cui ruolo è stato assegnato dall'ICANN stessa. Nell'ambito del processo di registrazione, al dominio viene assegnato un **nome di dominio** mnemonico. I nomi di dominio sono spesso descrittivi delle organizzazioni che li registrano, il che ne aumenta l'utilità per gli esseri umani.

In alcuni casi per organizzare i nomi all'interno di un dominio si utilizzano più estensioni, denominate **sottodomini**, che spesso rappresentano reti diverse entro la giurisdizione del dominio. Il software utilizzato deve essere in grado di convertire l'indirizzo mnemonico in un indirizzo IP prima di poter trasmettere il messaggio. Questa conversione viene eseguita con l'aiuto di numerosi server, **name server.** Questi name server sono utilizzati come una sorta di servizio elenchi per tutta internet che prende il nome di **domain name system**.

APPLICAZIONI INTERNET

Un'applicazione news-reader contattava i server usando il **Network News Transfer Protocol** e un'applicazione per accedere a un altro computer da grande distanza utilizzava il protocollo **Telnet** o **Secure Shell**. Un numero sempre maggiore di queste applicazioni è divenuto gestibile attraverso **Hyper Text Transfer Protocol (HTTP)**.

- **Posta elettronica** → SMTP definisce un modo in cui i computer di una rete possono interagire nella trasmissione di un messaggio email da un host a un altro. Le parole chiave HELO, MAIL, RCPT, DATA e QUIT sono definite con precisione nei termini del modo in cui staranno inviate, delle opzioni a cui possono essere associate e dell'interpretazione. Per accedere ai messaggi arrivati e accumulati sul server di posta dell'utente esistono due famosi protocolli:
  - **POP3** → prevede che l'utente trasferisca i messaggi sul proprio computer, da cui potrà leggerli, salvarli in varie cartelle, modificarli e manipolarli.
  - **IMAP** → consente all'utente di manipolare messaggi ed elementi correlati sul computer su cui si trova il server di posta. L'utente che debba accedere alla sua posta da computer diversi potrà conservare tutto sul server, e quindi potrà accedere a tutti i suoi messaggi da qualsiasi computer.
- **VoIP** → prevede l'uso dell'infrastruttura Internet a supporto di comunicazioni vocali simili a quelle dei tradizionali sistemi telefonici. VoIP consiste di due processi su due diverse macchine che trasferiscono dati audio mediante il modello P2P.
  - I **soft phone** consistono in un software che consente a due o più computer di condividere una chiamata con una dotazione hardware minima.
  - Una seconda forma di VoIP consiste in **adattatori per il telefono analogico** ovvero dispositivi che permettono all'utente di connettere il normale telefono ai servizi telefonici forniti da un ISP d'accesso.

- Una terza forma prende la forma di telefoni VoIP emebedded, cioè dispositivi che sostituiscono il telefono tradizionale con un apparecchio equivalente connesso direttamente a una rete TCP/IP.

- **Streaming multimediale via Internet:**
  - **N-unicast** → obbliga il server a inviare singoli messaggi a ciascun client in tempo reale, e a tutti i messaggi devono essere inoltrati dai server vicini.
  - **Multicast** → trasferisce il problema della distribuzione ai router di Internet. Un server trasmette un messaggio a più client per mezzo di un unico indirizzo, e delega ai router di Internet il riconoscimento della significanza di tale indirizzo.
  - **Streaming on-demand** → l'utente si aspetta di visualizzare o ascoltare elementi multimediali in un momento arbitrario a sua scelta. I servizi di streaming su larga scala utilizzano le **reti di distribuzione di contenuti**.
  - **Anycast** → consente all'utente finale di connettersi automaticamente al server più vicino di un gruppo definito, contribuisce all'impiego pratico delle CDN.

4.3 IL WORD WILD WEB

Concetto di ipertesto, ovvero documenti interconnessi. Un formato ipertestuale per documenti che possono contenere **collegamenti ipertestuali** ad altri documenti, un protocollo per trasferire in rete gli ipertesti e un processo server che fornisce le pagine di ipertesto a richiesta.

IMPLEMENTAZIONE DEL WEB

I pacchetti software che consentono agli utenti di accedere agli ipertesti si dividono in due categorie:

- **Browser** → risiede nella macchina dell'utente e si incarica di ottenere in modo organizzato i materiali richiesti dall'utente stesso. (Firefox, Chrome, Safari ecc…)
- **Server web** → risiede nel computer contenente i documenti ipertestuali a cui accedere, e il suo compito consiste nel fornire l'accesso ai documenti sotto il suo controllo ai client che ne facciano richiesta. I documenti ipertestuali vengono solitamente trasferiti tra i browser e i server web attraverso protocollo chiamato **HTTP.**

Per individuare e recuperare i documenti viene assegnato ad ognuno un indirizzo univoco detto **URL.** Ogni URL contiene le informazioni necessarie ad un browser per contattare il server corretto e richiedere i documenti desiderati. Quindi è necessario inserire nel browser l'URL del documento desiderato e chiedere al browser di recuperare e visualizzare il documento.

http://eagle.mu.edu/authors/Shakespeare/Julius_Caesar.html

protocollo richiesto per accedere al documento – nome mnemonico dell'host che contiene il documento – percorso che indica la posizione del documento all'interno del file system dell'host – nome del documento.

HTML

Un documento ipertestuale è simile a un documento di testo tradizionale. La differenza è che esso contiene anche simboli detti **tag** o **marcatori**, che descrivono come dovrebbe apparire il documento sullo schermo e quali voci devono essere collegate ad altri documenti. Questo sistema è conosciuto come **HTML**. L'autore di una pagina web descrive le informazioni necessarie al browser per presentare la pagina sullo schermo dell'utente e per trovare i documenti correlati cui fa riferimento.

XML

È uno stilo standardizzato per definire sistemi di notazione che rappresentano dati sotto forma di file di testo. Sulla base dello standard XML sono stati sviluppati sistemi detti **linguaggi di markup** per rappresentare espressioni matematiche, presentazioni multimediali e musica. HTML è il linguaggio di markup basato su XML standard sviluppato per rappresentare le pagine web. L'approccio di XML è quello di sviluppare uno standard generale per i vari linguaggi, che a loro volta possono essere specializzati per le applicazioni più diverse.

ATTIVITÀ LATO CLIENT E LATO SERVER

Il server web costruisce pagine web contenenti informazioni provenienti dal server di posta e invia al client tali pagine, il cui browser le visualizza. Il browser consente all'utente di creare messaggi e inviare le relative informazioni al server web, che inoltra i messaggi ai server di posta affinché esso li invii. Per eseguire le attività vi sono diversi sistemi: (attività lato client)

- Includere nel documento HTML sorgente programmi scritti nel linguaggio Java-Script. Da qui il browser può estrarre i programmi ed eseguirli come richiesto.
- Trasferire insieme alla pagina web alcune unità di programma aggiuntive, dette applet e scritte nel linguaggio Java.
- Approccio di Flash con il quale possono essere realizzate presentazioni multimediali lato client di grandi dimensioni.

(attività lato server)

- Uso di un insieme di standard chiamato CGI in base al quale i client potevano richiedere l'esecuzione dei programmi memorizzati sul server.
- Sun Microsystem: consente ai client di avviare l'esecuzione lato server di piccole unità di programma dette servlet. Una versione semplificata dell'approccio servlet si ha quando l'attività lato server richiesta è quella di costruire una pagina web personalizzata.

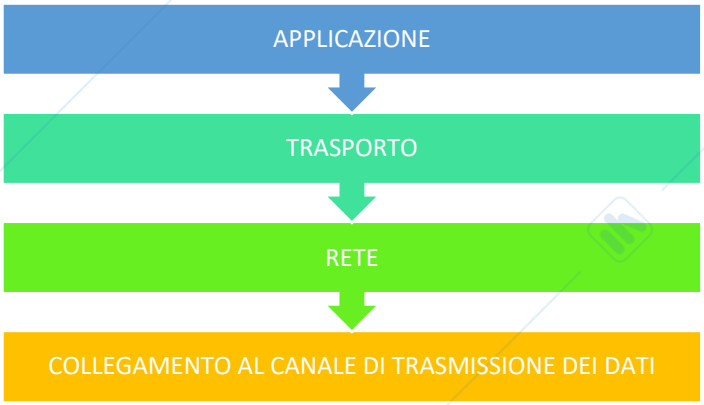
4.4 PROTOCOLLI INTERNET

I LIVELLI DEL SOFTWARE DI INTERNET

Un compito fondamentale del software di rete è fornire l'infrastruttura necessaria per trasferire i messaggi da un computer a un altro. Su Internet questo passaggio è realizzato tramite una gerarchia di componenti software.

I quattro livelli sono:

Un messaggio ha origine nel livello di applicazione. Viene fatto passare attraverso i livelli di trasporto e di rete dove viene poi preparato per la trasmissione e alla fine il livello di collegamento lo invia a destinazione.



- **Livello applicazione:** Il livello di applicazione è costituito dai componenti software che richiedono la comunicazione via Internet per eseguire i propri compiti. Per inviare e ricevere messaggi su Internet, il livello di applicazione usa quello di trasporto.
- **Livello di trasporto:** Un compito importante del livello di trasporto è accettare i messaggi del livello di applicazione e garantire che siano formattati nel modo corretto per la trasmissione in Internet. Divide i messaggi lunghi in segmenti più piccoli che vengono inviati in Internet come singole unità. I segmenti possono passare senza problemi, mentre un messaggio lungo costringe gli altri ad attendere che sia passato. Aggiunge numeri sequenziali ai piccoli segmenti che produce, dopodiché passa tali segmenti, **pacchetti**, al livello rete. Stabilire a quale applicazione è diretto un messaggio in ingresso è un compito importante del livello trasporto. Tale operazione è gestita assegnando **numeri di porta** univoci.
- **Livello rete:** Tocca al livello rete decidere in quale direzione debba essere inviato il pacchetto a ciascun passaggio del suo percorso in Internet. Ha il compito di mantenere la tabella di inoltro del router, e di usarla per determinare la direzione in cui inoltrare i pacchetti.
- **Livello collegamento:** Ha il compito di ricevere e trasmettere i pacchetti. Deve quindi gestire i dettagli di comunicazione specifici della rete in cui risiede il computer. Ogni volta che un pacchetto è trasmesso viene ricevuto dal livello collegamento all'altra estremità della connessione.

LA FAMIGLIA DI PROTOCOLLI TCP/IP

La richiesta di reti ha comportato la necessità di pubblicare degli standard che consentono ai produttori di fornire dispositivi e software perfettamente funzionanti anche in rapporto a prodotti in altri fornitori. Uno degli standard è il modello di riferimento **OSI.**

La famiglia di protocolli TCP/IP è l'insieme di standard di protocollo usato da Internet per implementare la gerarchia quattro livelli appena descritta. Esistono varie differenze fondamentali tra TCP e UDP:

- Una delle quali è che prima di trasmettere un messaggio richiesto dal livello applicazione, il livello trasporto basato su TCP inoltra il messaggio al livello trasporto alla destinazione comunicandogli che sta

per essere inviato un messaggio. Invece il livello trasporto basato su UDP invia semplicemente un messaggio all'indirizzo che gli è stato fornito, e poi dimentica della sua esistenza.

- Un'altra differenza è che i livelli trasporto TCP del mittente e del destinatario cooperano tramite conferme di ricezione e ritrasmissioni dei pacchetti.
- TCP è dotato sia di **controllo del flusso**, che implica che il livello trasporto all'origine del messaggio possa modulare la velocità di trasmissione dei segmenti allo scopo di non intasare la sua controparte a destinazione, sia di **controllo della congestione**, che significa che la velocità di trasmissione del livello trasporto TCP all'origine può essere regolata in funzione della congestione del tratto tra esso e la destinazione del messaggio.
- IP è lo standard di Internet per l'implementazione dei compiti assegnati al livello rete. **Instradamento** prevede che l'aggiornamento della tabella di routing del livello per adeguarla alle variazioni della situazione.

4.5 SICUREZZA

TIPOLOGIA DI ATTACCHI

I sistemi di computer e i loro contenuti possono essere attaccati in molti modi, gli attacchi prevedono l'uso di software dannoso il **malware** che può essere trasferito ed eseguito su un computer o può attaccarlo a distanza.

- **Virus:** è un software che infetta un computer inserendosi nei programmi già presenti sulla macchina. Quando il programma ospite viene eseguito, viene eseguito anche il virus.
- **Worm:** è un programma autonomo che si trasferisce autonomamente attraverso una rete, insinuandosi nei computer e inoltrando copie di sé stesso ad altri computer. I worm possono semplicemente auto-replicarsi o compiere azioni molto più dannose. Una tipica conseguenza di un worm è il suo duplicarsi e diffondersi incontrollato.
- **Cavallo di Troia:** è un programma che entra in un computer sotto forma di applicazione legale. Una volta nel computer, il cavallo di Troia esegue attività supplementari che possono avere conseguenze pericolose. I cavalli di Troia si presentano spesso sotto forma di allegati ai messaggi e-mail.
- **Spyware:** raccoglie informazioni sulle attività che si svolgono nel computer su cui risiede e la importa al mandante dell'attacco. Lo spyware è utilizzato per scopi dichiaratamente dolosi.
- **Phishing:** modo esplicito per ottenere le informazioni semplicemente chiedendole. Il processo implica la diffusione di alcune esche sperando che qualcuno abbocchi.
- **DoS/negazione di servizio:** attacchi provenienti da un software che viene eseguito su altri computer del sistema. Vengono lanciati contro grandi server web commerciali in Internet per disturbare gli affari o bloccare completamente l'attività. Chi attacca installa il software su computer ignari che generano messaggi intasando il bersaglio. È necessaria la disponibilità di computer "complici".
- **Spam:** simile al DoS ma il volume dello spam è raramente sufficiente a sovraccaricare il sistema.

PROTEZIONE E RIMEDI

- **Firewall:** può essere installato presso il gateway di un'organizzazione per filtrare i messaggi che entrano ed escono dall'area. Può anche bloccare i messaggi, questa funzione è uno strumento valido per interrompere un attacco di negazione del servizio. Sono utilizzati anche per proteggere i singoli computer.
- **Filtri anti-spam:** concepiti per fermare la posta elettronica non desiderata. Alcuni imparano a compiere tale distinzione attraverso un processo di auto-formazione nel quale l'utente indica alcuni elementi di spam fintanto che il filtro acquisisce esempi sufficienti a distinguerli autonomamente.
- **Server proxy:** unità software che agisce da intermediario tra un client e un server allo scopo di proteggere il client dalle azioni dolose del server. Senza un server proxy, un client comunica direttamente con un server, il quale ha così l'opportunità di raccogliere alcune informazioni sul client. Il server può raccogliere molte informazioni sulla struttura dall'intranet e può utilizzarle per attività nocive. Per contrastare questa situazione, un'organizzazione può allestire un server proxy per un tipo di servizio specifico.
  Il primo vantaggio di questa impostazione è che il server remoto non ha modo di sapere che il server proxy non è il vero client, di cui non conoscerà mai l'esistenza. Il vero server non ha modo di scoprire le caratteristiche interne dell'intranet. Il secondo vantaggio è che il server proxy filtra tutti i messaggi inviati dal server al client.
- **Software antivirus:** individua e rimuove i virus.

CRITTOGRAFIA

Versione sicura di HTTP→ **HTTPS** utilizzata dalla maggior parte delle istituzioni finanziarie per dotare i clienti di un accesso Internet protetto ai loro conti. L'ossatura di HTTPS è il sistema di protocolli chiamato **SSL**. La maggior parte dei browser segnala l'uso di SSL visualizzando una piccola icona a forma di lucchetto sullo schermo. Uno degli argomenti più affascinanti è quello della **crittografia a chiave pubblica**, che prevede tecniche per cui i sistemi di crittografia sono progettati in modo che per decifrare i messaggi non basti sapere come sono stati cifrati. Un sistema di crittografia a chiave pubblica implica l'uso di due valori chiamati **chiavi**:

- **Chiave pubblica:** usata per cifrare i messaggi. La chiave pubblica viene distribuita a tutti coloro che potrebbero voler inviare messaggi a una determinata destinazione.
- **Chiave privata:** usata per decifrarli. Viene mantenuta segreta. Il mittente del messaggio può quindi cifrare usando la chiave pubblica a inviare il messaggio a destinazione con la certezza che i suoi contenuti sono al sicuro. L'unica parte che può decifrare il messaggio è infatti il destinatario che possiede la chiava privata.

Uno degli approcci per risolvere questo problema è quello di stabilire siti Internet affidabili, chiamati **autorità di certificazione**. Queste autorità forniscono ai loro client informazioni affidabili sulle chiavi pubbliche attraverso pacchetti chiamati certificati. Un **certificato** è un pacchetto che contiene il nome di una parte e la sua chiave pubblica.

In alcuni sistemi a chiave pubblica, i ruoli delle chiavi pubbliche e private possono essere invertiti; questo significa che un testo può essere codificato con la chiave privata e, poiché solo una parte ha avuto accesso a tale chiave, si

garantisce che il testo così codificato provenga da quella parte. Il possessore della chiave privata può produrre un pattern di bit, detto **firma digitale**, che lui solo sa come produrre.

Usare una firma digitale può essere semplice come cifrare un messaggio; tutto ciò che il mittente deve fare è cifrare il messaggio da trasmettere usando la sua chiave privata. Quando il messaggio viene ricevuto, il destinatario utilizza la chiave pubblica del mittente per decifrare la firma.

CAPITOLO 10 – TEORIA DELLA COMPUTAZIONE

10.6 CRITTOGRAFIA A CHIAVE PUBBLICA

Metodo di codifica e decodifica dei messaggi → **algoritmo RSA.** Grazie a questo algoritmo è possibile cifrare i messaggi usando un insieme di valori noti come **chiavi di codifica**, e poi de cifrarli usando altri valori noti come **chiavi di decodifica**. Chi conosce le chiavi di codifica può cifrare i messaggi ma non decifrarli.

Queste tecniche costituiscono un sistema di **crittografia**, o **cifratura**, a **chiave pubblica**, un termine che riflette il fatto che le chiavi usate per cifrare i messaggi possono essere di pubblico dominio senza influire sulla sicurezza.

NOTAZIONE MODULARE

Per descrivere il sistema di crittografia a chiave pubblica RSA è comodo usare la notazione $x \% m$. $9 \% 7$ è uguale a 2 (resto 2). Si noti che $x \% m$ è x stesso se x è un intero compreso nell'intervallo da 0 a $m - 1$. Per esempio $4 \% 9$ è pari a 4.

CRITTOGRAFIA A CHIAVE PUBBLICA RSA

Sistema di codifica a chiave pubblica basato sull'algoritmo RSA. Scegliamo due numeri primi p e q, il cui prodotto è rappresentato da n. Scegliamo poi altre due interi positivi, e e d, tali per cui $e \times d = k(p - 1)(q - 1) + 1$, per un intero positivo k. Chiameremo questi valori e e d perché faranno parte del processo di cifratura e decifrazione.

Un sistema a cifratura a chiave pubblica con l'algoritmo RSA si realizza selezionando due interi primi, p e q, da cui vengono generati i valori n, e e d. I valori n ed e vengono usati per cifrare i messaggi e sono le chiavi pubbliche; i valori n e d vengono usati per decifrare i messaggi sono le chiavi private.