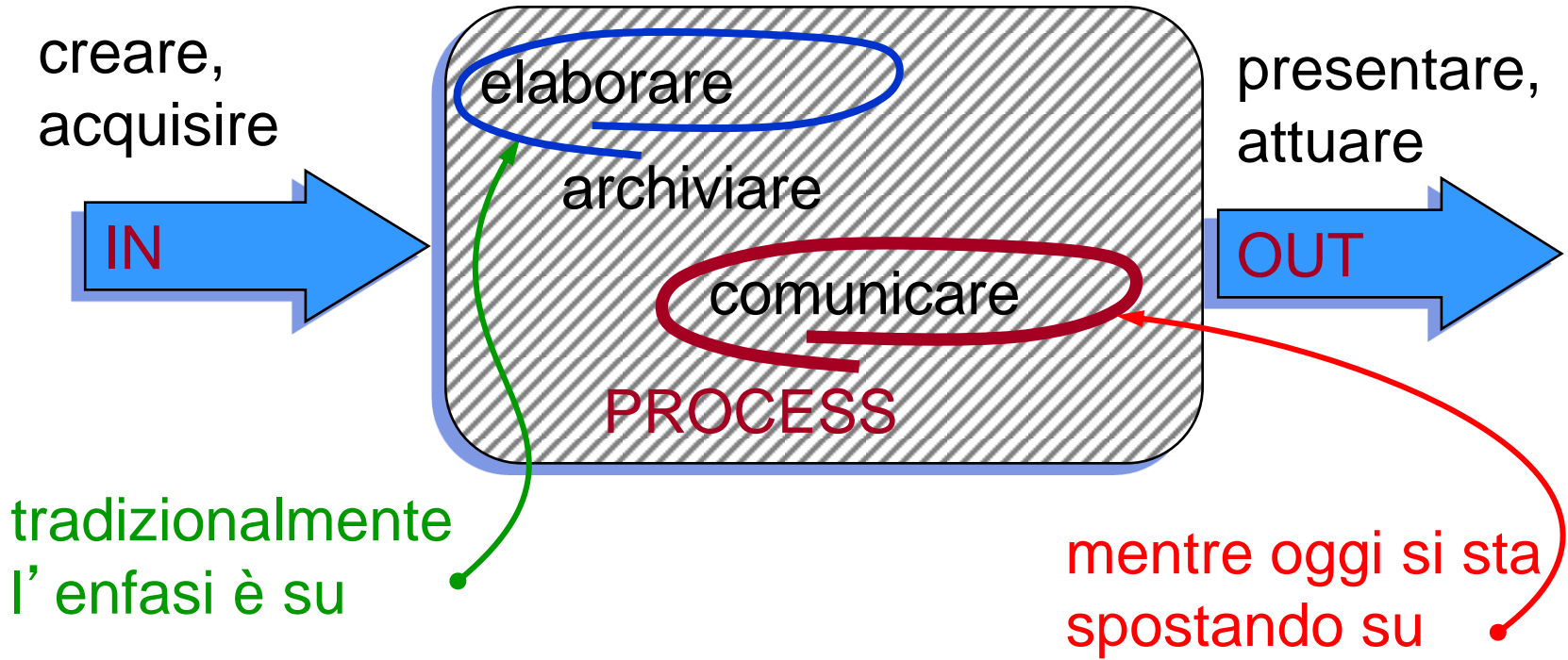

Comunicazione di Rete

Reti di comunicazione



... cioè sull' interconnessione in
 rete dei sistemi di elaborazione ...

Perche la rete?

➤ **Condividere risorse**

- utilizzo razionale di risorse HW (magari costose)
- Condivisione di software (programmi e dati da parte di utenti)
- affidabilità e disponibilità delle risorse

➤ **Comunicare tra utenti**

- scambio informazioni
- collaborazione a distanza

Cos'è una rete?

- Una rete informatica è un insieme di dispositivi collegati tra loro tramite sistemi di interconnessione (cablaggio o wireless).
 - Consente di comunicare e condividere informazioni e risorse.
 - Sono classificate a seconda delle dimensioni.
 - È possibile ospitarle in una sede singola oppure dislocarle in vaste aree.

I protocolli di comunicazione

- Per comunicare i calcolatori debbono seguire delle le **regole**: i protocolli di comunicazione.
- I protocolli di comunicazione specificano:
 - i formati dei dati
 - la struttura dei pacchetti
 - la velocità di trasmissione
 - ...
- Definire tutte queste proprietà tramite un unico protocollo è praticamente impossibile, per questo si definisce **un insieme di protocolli**:
 - ogni protocollo gestisce univocamente una componente ben definita della comunicazione
 - ogni protocollo condivide con gli altri protocolli i dati di cui essi necessitano

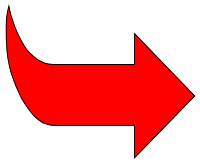
Alcuni protocolli applicativi

- HTTP
 - Per navigare sul web
- HTTPS
 - Per acquistare su web in modo sicuro
- SMTP
 - Per spedire email
- POP
 - Per ricevere email e scaricarle sul proprio PC
 - Una volta scaricate sul PC le email non sono leggibili con altri dispositivi ma non serve più essere collegati a internet per consultarle
- IMAP
 - Per ricevere email senza scaricarle sul proprio PC
 - La mail può essere letta da qualunque dispositivo ma bisogna essere collegati a internet

INTERNET E IL WORLD WIDE WEB

La storia di Internet

Inizi anni '60 - La ARPA (Min.Difesa USA) avvia un progetto che prevede la costruzione di una rete di computer.

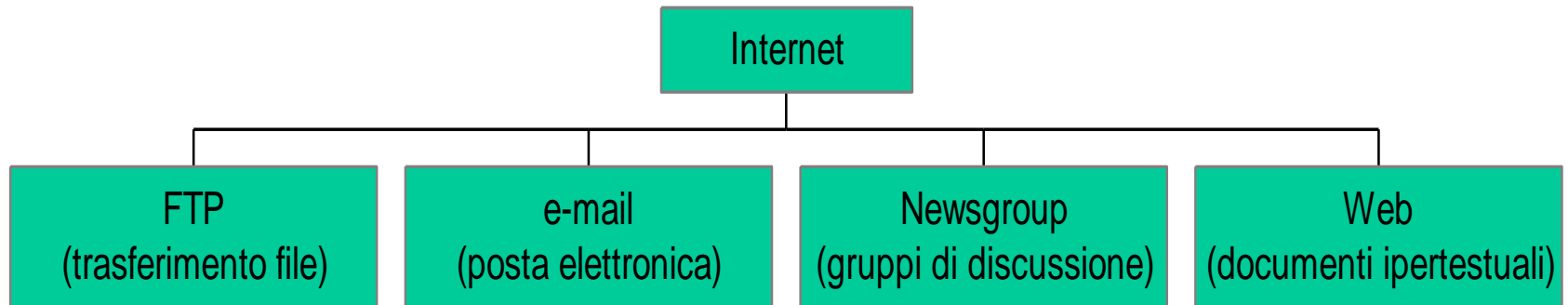


Novembre 1969: due computer di facoltà universitarie (UCLA e SRI) si collegano attraverso una rete BBN progenitrice dell' attuale Internet.

Oggi: né università né organi governativi gestiscono la rete, ma un' associazione volontaria, la

ISOC (Internet Society)

Internet e WWW non sono la stessa cosa



i servizi di Internet, dal più remoto al più recente

Il World Wide Web

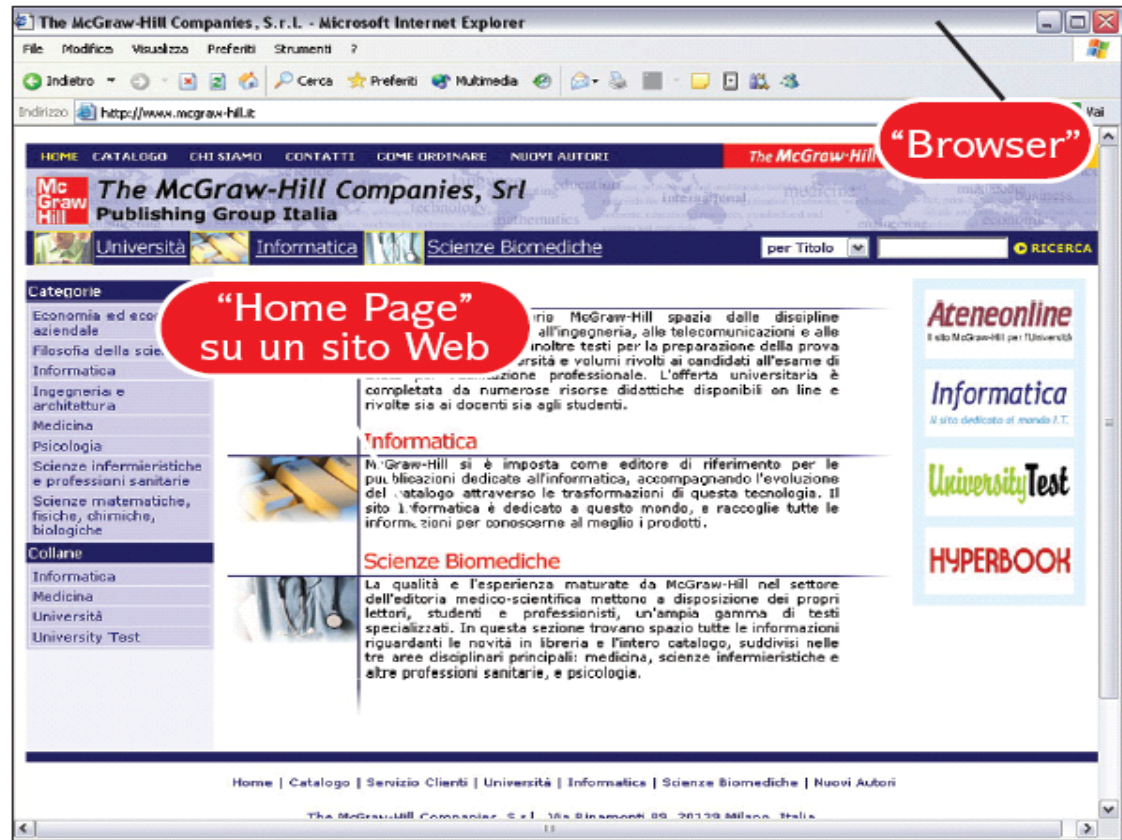
- Il servizio più recente di Internet
- Costituito da documenti che sono su computer diversi (anche a distanza) collegati tra loro
- I documenti sono consultabili per mezzo di programmi chiamati browser
 - Internet Explorer, Mozilla Firefox, Google Chrome, Opera, ecc.

La storia del Web

- Il Web è nato nel 1989
- Da un'idea di Tim Berners-Lee
 - Ricercatore del CERN di Ginevra
- Berners-Lee elaborò i pilastri del Web:
 - HTTP (HyperText Transfer Protocol)
 - Come comunicare
 - HTML (Hypertext Markup Language)
 - Come scrivere
 - URL (Uniform Resource Locator)
 - Dove trovare
- Nel 1998 nasce il World Wide Web Consortium (W3C)

Un pagina Web

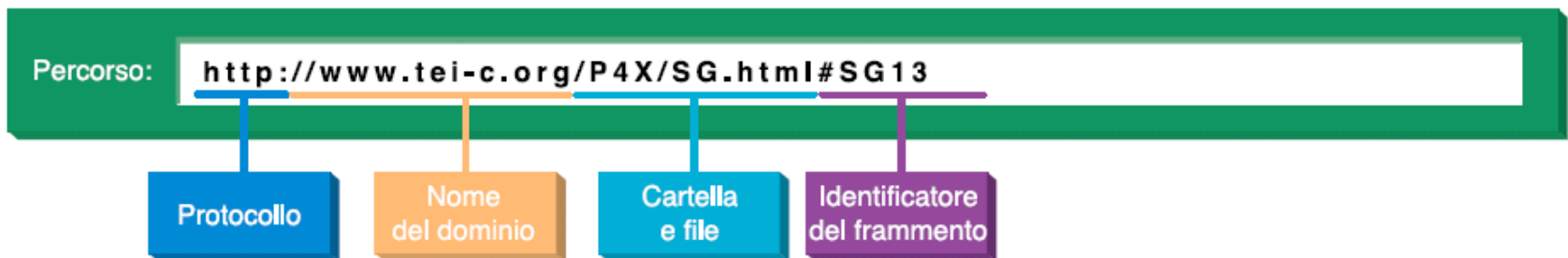
Ciò che appare all'utente sul suo schermo è l'unione di due elementi ben diversi: il **browser**, l'applicazione che consente di navigare tra le pagine web, e il **contenuto** di una pagina presente su un sito.



Home page del sito della McGraw-Hill Italia
<http://www.mcgraw-hill.it>

Analisi di un indirizzo web (URL)

- Un indirizzo URL è l'unione del metodo (protocollo) per trovare un file in Internet e l'esatta locazione di un elemento all'interno di quel file disponibile su un server. Ogni parte dell'URL identifica, sempre più specificatamente, la posizione dell'elemento.



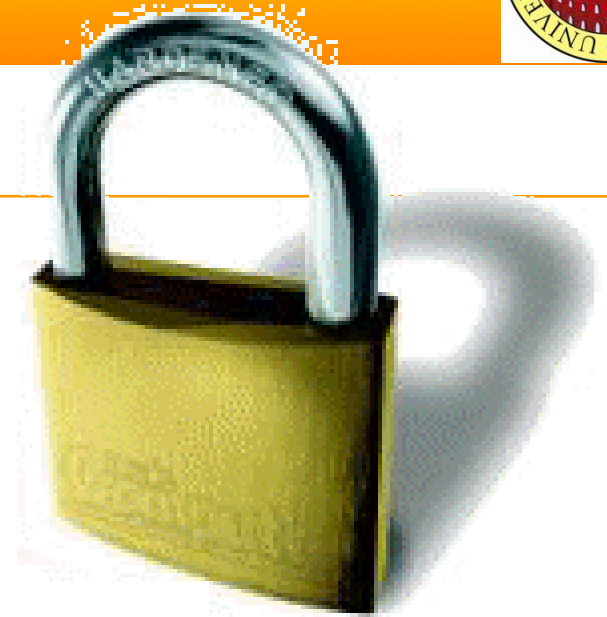
Indirizzo IP

- Un Indirizzo IP è un numero (a 32 bit) che identifica univocamente i dispositivi collegati con una rete informatica che utilizza lo standard IP (Internet Protocol)
- Ciascun dispositivo (router, computer, server di rete, stampanti, alcuni tipi di telefoni, ...) ha il suo indirizzo.

Indirizzi IP e DNS

- L' IP *non è di semplice comprensione* da parte dell'utente, ed è quindi uso comune assegnare ad ogni IP un *nome simbolico*
- Per fare questo si utilizza il **Domain Name System (DNS)**, che associa uno o più nomi ad ogni IP, e gestisce la conversione tra le due codifiche.





SICUREZZA

Cosa vuol dire sicurezza informatica

➤ Sicurezza “interna”

- Accesso sicuro ai propri dati, alle proprie informazioni.
- Copia delle informazioni importanti.
- Gestione di login, nickname e password personali.

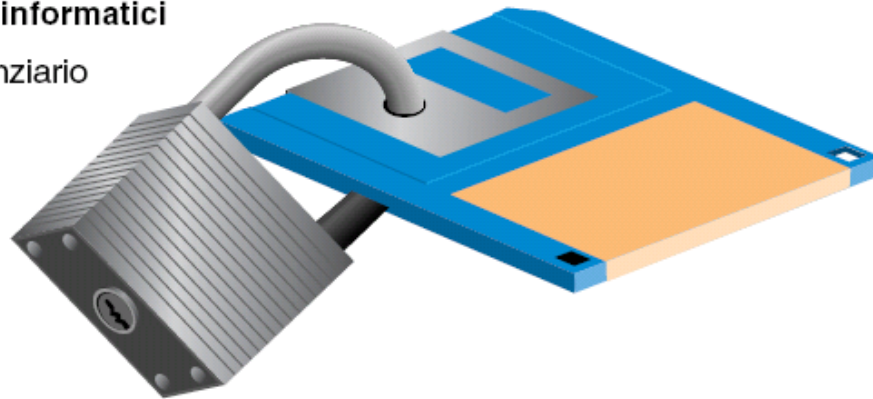
➤ Sicurezza “esterna”

- Certezza sul trattamento dei dati sensibili.
- Difesa dagli attacchi da virus e altro malware.
- Non commettere reati inconsapevolmente.

Crimini e criminali informatici

Le motivazioni dei criminali informatici

- Tornaconto personale o finanziario
- Divertimento
- Vendetta
- Favore personale
- Sfida
- Incidente
- Vandalismo



Tipi di *crimine* informatico

- Furti e manipolazioni dei dati
- Accessi abusivi a informazioni
- Attacchi "Denial of Service"
- Violazioni del copyright

Tipi di *criminale* informatico

- Cracker
- Dipendenti delle aziende colpite
- Persone in genere non autorizzate a svolgere determinate operazioni

La sicurezza in rete

- Le quattro principali aree in ambito di sicurezza in rete sono:
 - **segretezza dei dati:**
 - garantire che utenti non autorizzati possano leggere o modificare dati privati (e.g. crittografia)
 - **autenticazione:**
 - accertamento dell' identità del proprio interlocutore in rete, per evitare di fornire informazioni riservate ad estranei
 - **firme elettroniche:**
 - accertamento dell' autenticità dell' autore di un determinato documento "firmato"
 - **controllo di integrità:**
 - accertamento che un messaggio ricevuto non sia stato modificato durante la trasmissione.

La crittografia

- La crittografia è l'arte di progettare algoritmi (o cifrari) per crittografare un messaggio rendendolo incomprensibile a tutti tranne al suo destinatario
- Il destinatario, con un algoritmo simile deve essere in grado di codificarlo, attraverso un parametro segreto detto chiave (usato in precedenza anche dal mittente per la cifratura)

Alcuni consigli

- Se NON uso la crittografia, tutti possono leggere i dati che transitano via Internet...
- Se uso la crittografia, NESSUNO può decifrare il mio messaggio. A meno che:
 - non si riesca a “rompere” la codifica
 - non debba cedere la chiave
 - non sia il destinatario voluto (es. codice carta di credito)
- La crittografia rallenta un po' la comunicazione

Alcuni consigli

- Il **commercio elettronico** si effettua con il browser in modalità sicura (**https** con lucchetto)
 - La carta di credito per il commercio elettronico si usa SOLO se si conosce bene l'azienda in Internet.
- L'accesso dall'esterno è possibile alle condizioni che noi autorizziamo (impostazioni firewall)

Password

- L'uso di ***password non va confuso con la crittografia***
- Le password (e i relativi nomi utente) servono per accedere ad “aree riservate” (in locale o in rete) non per cifrare i dati
- Non usare parole di senso compiuto come password perché sono facilmente identificabili
 - i9C_1!kdNd è una password sicura
 - Gianni121290 (nome e data di nascita del fidanzato) non è una password sicura

Malware (<http://it.wikipedia.org/wiki/Malware>)

- Virus
 - Si attaccano a un file e vengono eseguiti ogni volta che il file infetto viene aperto
- Worm
 - Non necessita di attaccarsi a un altro eseguibile per diffondersi
- Backdoor
 - programmi che consentono un accesso non autorizzato al sistema su cui sono in esecuzione
- Cavallo di Troia
 - Inserito in un programma apparentemente utile contiene istruzioni dannose eseguite all'insaputa dell'utente
- Dialer
 - Accedono a internet modificando il numero telefonico con uno a tariffa speciale all'insaputa dell'utente. Nessun problema per chi usa ADS
- Spyware
 - Usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato
- Hoax
 - Sono bufale (catene di S. Antonio, richieste di aiuto per malattie, richieste di aiuto per trasferimento di denaro, ...)

I Virus

- In informatica il virus è un **frammento di codice** inserito all'inizio di un normale programma con lo scopo di *alterare o distruggere dati, rallentare le prestazioni di sistemi o bloccarli del tutto*
- Lo sviluppo di Internet ha favorito ed aumentato la diffusione di migliaia di tipologie di virus
- Per ogni virus “progettato” viene immediatamente codificato un nuovo **antivirus**:
 - programma che contiene grandi liste di virus regolarmente aggiornate e che ispeziona i file sospetti “riconoscendo” ed eliminando l’ eventuale codice pericoloso.
- Essendo spesso causa di distruzione o manomissione di dati importanti, la generazione di virus è ritenuta un **reato**

Virus: alcuni consigli

- Un virus è un programma scritto da programmatori!
- Gli antivirus possono bloccare alcuni dei virus riconosciuti (esistenti nel database dell'antivirus)
- Gli eseguibili allegati alle email vanno eseguiti SOLO se si è certi del contenuto (e di chi ha spedito la email)
- I virus possono essere eseguiti all'insaputa dell'utente
- I virus permettono lauti guadagni alle aziende che producono antivirus e s.o.
- Formattazione: cancella tutto il contenuto del disco, virus ma anche dati

Tecniche di attacco

- Sniffing
 - attività di intercettazione passiva dei dati che transitano in una rete telematica
- Spoofing
 - tipo di attacco informatico dove viene impiegata in qualche maniera la falsificazione dell'identità (es.: falsificazione dell'indirizzo IP)
- Phishing
 - truffa via Internet attraverso la quale un aggressore cerca di ingannare la vittima convincendola a fornire informazioni personali sensibili

Lo Spam



- La SPAM (Spiced Ham) era la carne in scatola fornita ai soldati dell' esercito americano, e si guadagnò una **fama negativa**
- In Internet lo “Spamming” consiste nell’**invio di messaggi pubblicitari** tramite posta elettronica in **nessun modo sollecitati** (“Junk Mail”)
- Lo Spamming danneggia il ricevente facendogli **perdere tempo e denaro** per scaricare posta inutile, e danneggia il gestore del server di posta con uno smisurato aumento di “traffico” nelle sue linee.

Evitare lo spam

- Evitare messaggi di spam è molto difficile: alcuni metodi sono troppo blandi mentre altri troppo restrittivi (fermano anche posta “legittima”).
- Tuttavia esistono norme pratiche che consentono di ridurre questo problema:
 - evitare di comunicare pubblicamente il proprio indirizzo email attraverso siti, guestbook, chat, messenger, ICQ, ecc.
 - spesso gli spammers reperiscono automaticamente gli indirizzi, cercando stringhe della forma [tizio@caio.ecc](#)
 - quindi, se desideriamo comunicare la nostra email in un contesto pubblico è buona norma scriverla nella forma: [tizioNOSPAM@caio.ecc](#)
- Se ricevo mail di spam NON rispondo