Sistemi Di Elaborazione Dell'informazione

Dott. Antonio Calanducci

Lezione IV: Internet e la posta elettronica

Corso di Laurea in Scienze della Comunicazione

Anno accademico 2009/2010

Outline

- **Internet**
  - Indirizzi, World Wide Web, URLs, ipertesti, HTML
  - Siti sicuri (HTTPs) e certificati digitali
    - cenni di crittografia
  - pericoli e sistemi di protezione
- **E-mail**
  - netiquette e firma digitale
  - spam, phishing

Storia di Internet

- 1983, in USA nasce ARPANET, prima rete di computer per scopi militari:
  - trasmissione delle informazioni in caso di attacchi nucleari
  - pacchetti e routing alternativo garantivano la comunicazione in qualsiasi condizione
- 1980, ARPANET si diffonde alle università
  - separazione del mondo militare
  - nasce Internet, prima in USA e poi in Europa

Internet

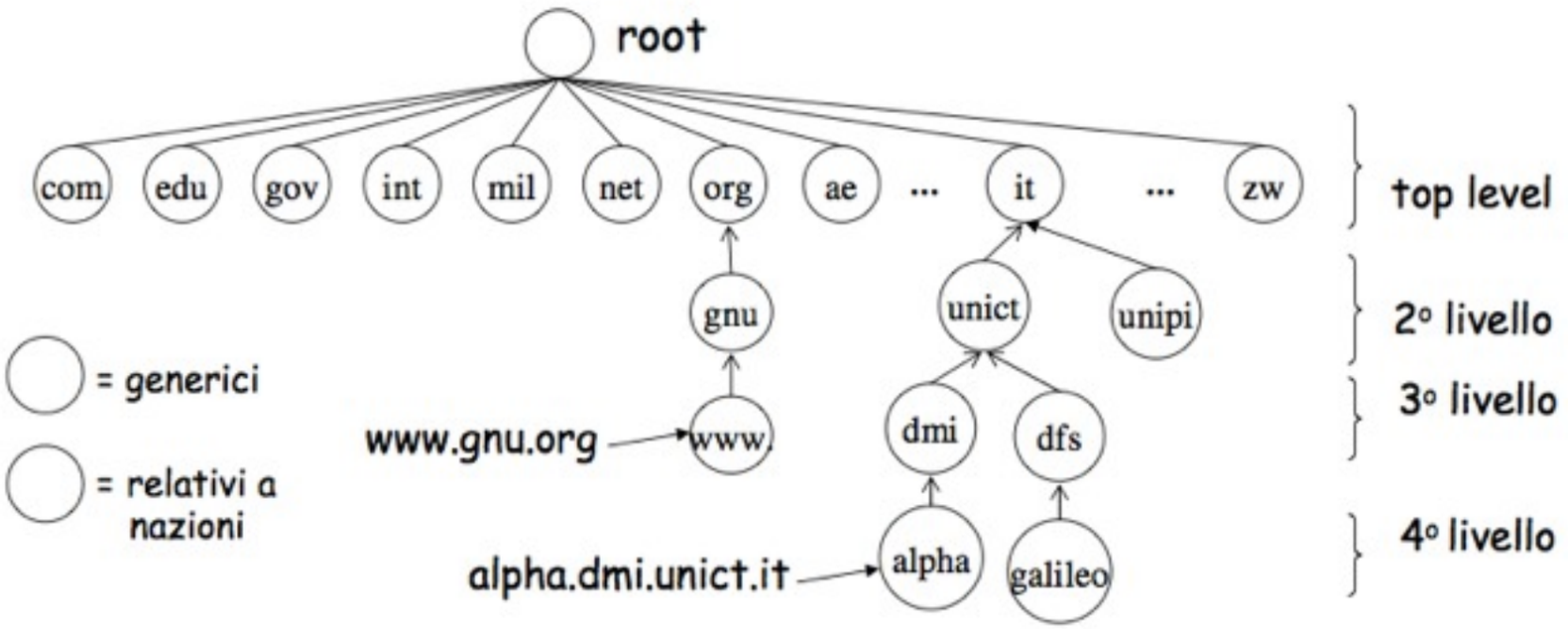
- È una rete mondiale di computers (e dispositivi abilitati) ad accesso pubblico
- la Rete delle reti
  - collega le reti nazionali dei vari paesi del mondo
- uno dei principali mezzi di comunicazione di massa
- basata sul protocollo di comunicazione TCP/IP e lo scambio di pacchetti
- ogni nodo su Internet è identificato dall'indirizzo IP
  - hanno un corrispondente simbolico

Indirizzi Internet

- Organizzati logicamente in una struttura gerarchica di **domini**:
  - Domini di *primo livello* (Top Level Domain) nazionali:
    - .it, .es, .fr, .jp, .eu, etc..
  - Domini di *primo livello* generici:
    - .com, .gov, .org, .edu, etc.
- I domini sono a loro volta suddivisi in sotto-domini (dominio di secondo livello, terzo livello, etc)
  - es: flett.unict.it

Esempi indirizzi

- Indirizzo completo di un nodo:
  - <nome host>.<sottodominio>.<sottodominio>. ... .<dominio-di-1-livello>
- Es:
  - glibrary.ct.infn.it
  - www.flett.unict.it
  - s1stem1.wordpress.com
  - alpha.dmi.unict.it



DNS

- Ogni nodo è identificata da un indirizzo IP e da uno o più (alias) indirizzi simbolici
  - 193.206.208.35 = glibrary.ct.infn.it, corsomac.ct.infn.it (alias)
  - 151.97.124.101 = www.flett.unict.it

- il Domain Name Server (DNS) è un database distribuito che tiene traccia delle associazioni tra indirizzi IP e indirizzi simbolici
  - ogni computer collegato ad internet deve poter raggiungere un server DNS per navigare correttamente

WWW e ipertesti

- Il World Wide Web (o Web) è il principale **servizio** di Internet:
  - insieme di documenti multimediali, composti da testo, grafica, animazioni, filmati, suoni, **collegati** tra loro
  - **ipetesti**, pagine web collegate tra loro da **hyperlinks** o **links**
    - consultazione non sequenziale, percorsi diversi
- ogni sito web è un ipertesto, pagine web memorizzate su uno o più computers (**server web**), a cui è possibile accedere tramite un browser (client web)
- Internet è un enorme ipertesto

Linguaggio HTML

- HyperText Markup Language: è il linguaggio per scrivere le pagine Web
  - istruzioni racchiuse tra marcatori, i *tag*, tra < .. >

```
<HTML>
<HEAD>
<TITLE>Una pagina web</TITLE>
</HEAD>
<BODY>
<P>Hello, world!</P>
</BODY>
</HTML>
```

URL

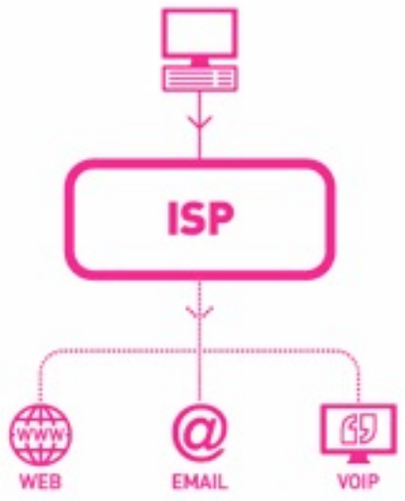
- **Uniform Resource Locator** è l'indirizzo di una risorsa su Internet
  - es:
    - http://s1stem1.files.wordpress.com/2010/03/sistemi-lezione-ii.pdf
  - Componenti di una URL:
    - protocollo (HTTP)
    - indirizzo nodo (s1stem1.files.wordpress.com)
    - percorso sul server (/2010/03/)
    - nome del file (sistemi-lezione-ii.pdf)
- Altri protocolli Internet: ftp://, https://, feed://

Altri servizi di Internet

- Posta elettronica
- Gruppi di discussione (newsgroups)
- Trasferimento di files (FTP, File Transfer Protocol)
- Instant Messaging (chat)
- Telefonia (VOIP: Voice Over IP)
- File sharing (BitTorrent, eMule)

Accedere ad Internet

- ISP o **Internet Service Providers**:
  - erogatore del servizio Internet su linea telefonica
  - intermediario tra l'utente domestico e la rete Internet



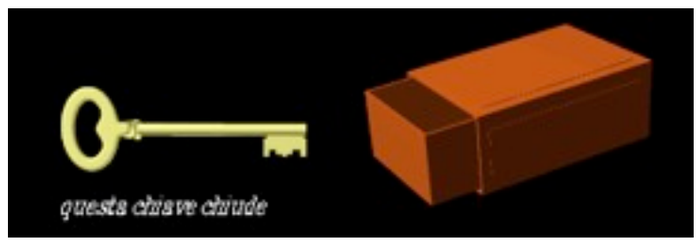
- Es: Tiscali, Telecom, FastWeb, Wind-Infostrada
  - in genere forniscono anche una casella di posta elettronica e spazio Web
  - assegnano un indirizzo IP dinamico al router o modem

Web sicuro: crittografia

- HTTP è un protocollo in “chiaro”, le informazioni che passano dal client al server viaggiano sulla rete nel formato in cui sono state generate
  - es.: pagine Web, formato HTML, formato testuale
  - problema: man-in-the-middle, chi legge il traffico di rete (“sniffa”) può violare la vostra privacy, o peggio modificare l’informazione
  - soluzione: la **crittografia** consente la cifratura del dati scambiati tra client e server
    - solo il client ed il server in grado di interpretare la comunicazione

Crittografia

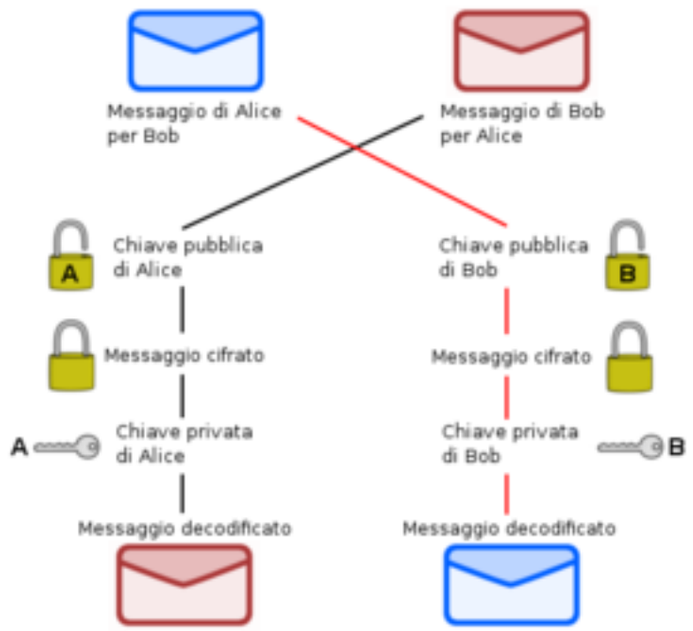
- è un procedimento matematico che impiega algorimi sofisticati per rendere incomprensibile un messaggio a chi non ha la **chiave** per decodificare l'informazione.
  - Crittografia a chiave simmetrica



    - la stessa chiave per crittografare e decodificare
    - la chiave deve essere condivisa tra mittente e destinatario
  - Crittografia a chiave asimmetrica:
    - due chiavi: una pubblica ed una privata
    - la chiave pubblica per crittografare, quella privata per decodificare

Crittografia asimmetrica

- Alice vuole mandare un messaggio a Bob
  - Alice crittografia il messaggio con la chiave pubblica di Bob
  - il messaggio cifrato viaggia in rete
  - Bob decodifica il messaggio cifrato con la sua chiave privata
- Bob vuole mandare un messaggio ad Alice
  - Bob crittografa il messaggio con la chiave pubblica di Alice
  - Alice decodifica il messaggio cifrato con la sua chiave privata



Web sicuro: HTTPS

- La connessione viene crittografata, usando il protocollo crittografico SSL (Secure Socket Layer) o TLS (Transport Layer Security), con un meccanismo a chiave asimmetrica:
  - le informazioni (es: numero di carta di credito) che il client (il browser) invia al server web sono crittografate con la chiave pubblica del server
  - la chiave pubblica del server è contenuta nel **certificato digitale** del server
    - il certificato è il "passaporto" digitale di un utente (o servizio) su Internet, garantisce l'identità di un soggetto
    - è rilasciato dalle Certification Authority (garante)

Minacce alla sicurezza

- **virus:** parti di software in grado di autoreplicarsi ed infettare altri files, generalmente senza farsi rilevare dall'utente

- **worms:** software in grado di autoreplicarsi, sfruttando Internet (posta elettronica principalmente) come canale di diffusione

- **trojan horses (cavalli di troia)**: software in grado di nascondersi all'interno di altri programmi, che vengono mandati in esecuzione dal programma che li "ospita"
  - in genere aprono delle "backdoor"
  - non si autoreplicano

Minacce alla sicurezza

- **spyware:** software in grado di carpire informazioni del sistema su cui sono in esecuzione e di trasmetterle ad estranei
- **dialer:** intecettano la connessione ad internet tramite linea telefonica, e tentano di modificare il numero telefonico verso numerazioni a tariffazione speciale
- **keylogger:** software in grado di registrare tutto ciò che un utente digita sulla tastiera
- **malware** (malicious software): un qualsiasi software creato con lo scopo di causare danni nel computer su cui è eseguito

Progettegersi su Internet

- **Antivirus**: un software atto a eliminare virus e malware (trojans, worms, dialer)
  - ogni malware ha la propria “firma” (o definizione)
  - l’aggiornamento dell’antivirus è il processo di download delle firme dei nuovi malware che ogni giorno vengono creati
- **Firewall:** è un sistema hardware e/o software che controlla lo scambio d’informazioni tra un dispositivo e la rete, in modo da intercettare tentativi di intrusioni, bloccando il traffico (in ingresso e in uscita)
  - basato su un sistema di regole in cascata

E-mail

- da *Electronic Mail*, è il principale servizio di comunicazione che usa la rete Internet come mezzo di comunicazione
- Requisiti per il funzionamento:
  - collegamento ad Internet
  - indirizzo di posta elettronica e password
  - indirizzo del server di posta in entrata (POP o IMAP server) e indirizzo del server di posta in uscita (SMTP server)

Struttura di un indirizzo e-mail

- es: antonio.calanducci@ct.infn.it
  - *nome utente* o *userID* o *account* o *username* (antonio.calanducci)
  - simbolo @ (si legge “at”, significa “presso”)
  - dominio (ct.infn.it)
- *Consiglio*: sul Web (per esempio su Blog e forum), indicare il proprio indirizzo sostituando @ con “ AT “, per evitare spam
  - es antonio.calanducci AT ct.infn.it

Campi in una e-mail

- "**A**": indirizzo del destinatario diretto
- "**Cc**": (Carbon Copy), copia per conoscenza, indirizzi di coloro che è bene siano a conoscenza del messaggio
- "**Ccn**" (o **Bcc**, Blind Carbon Copy), copia per conoscenza nascosta: gli indirizzi di coloro a cui si invia il messaggio che però non si desidera vengano visti dagli altri destinatari
  - molto utile per invio a mailing list (evita spam e conserva la privacy)
- **Oggetto** (o Subject): buona norma (netiquette=galateo della rete)
- **Contenuto**: del messaggio
- **Allegati**: uno o più file da spedire insieme al messaggio

Trasmissione di una mail

- Il messaggio viene editato su un client (desktop o web) e-mail, compilandone tutti i campi
- viene trasmesso dal client al **server SMTP** (Simple Mail Transfer Protocol) del proprio ISP
- il server SMTP estrapola il **dominio** del destinatario dall'indirizzo e-mail
  - chiede al server DNS chi è il server di posta in entrata per il dominio
  - invia al **server di posta in entrata** del destinatario il messaggio
- Il server di posta in entrata del destinario "consegna" l'email nella mailbox dell'utente associato all'username dell'indirizzo del destinatario
- Il destinario legge l'email scaricando il messaggio dal server di posta in entrata (POP3) o accedendovi direttamente (IMAP)

Netiquette

- E’ l’insieme di regole che disciplinano il comportamento di un utente di Internet nel rapportarsi con altri utenti (il galateo della Rete)
- Nel caso del servizio di posta elettronica:
  - indicare sempre l’Oggetto
  - Contenuto: sintetico e chiaro
  - Inoltrare (Forwarding): chiedere il consenso del mittente originario
  - eseguire il controllo ortografico
  - non usare i caratteri tutti in maiuscolo (=URLARE)
  - usare il campo bcc per non violare la privacy di destinatari che non si conoscono tra di loro
  - citare il testo a cui si risponde (quoting)

Firma digitale

- Procedura con la quale si garantisce l'identità del mittente di un'e-mail
  - basata sull'uso di chiavi asimmetriche (pubblica e privata) legate al certificato digitale, rilasciato da una Certification Authority

Considerazioni sulla sicurezza

- **Spamming**: invio di massa di e-mail con contenuto commerciale, nelle caselle di posta (mailbox) di più persone
  - fornire il proprio indirizzo solo a persone affidabili (non pubblicarlo su forum, bacheche, blog)
  - creare un secondo indirizzo e-mail per i servizi di cui sopra
  - configurare i filtri anti-spam sul proprio client di posta
- **Phishing**: sistema di frode per indurre l'utente a rivelare informazioni personali o finanziare
  - basata sullo spamming
  - una mail contiene un link che riproduce in maniera fedele la pagina web della login page di banche e istituti di credito