SEMINARIO DEL CORSO DI RETI DI TLC

INTRODUZIONE ALLA SICUREZZA NELLE RETI DI TLC

LEONARDO MACCARI: LABORATORIO LART

Sommario

- Come si definiscono i servizi di sicurezza
- Quali sono i rischi che si corrono
- Introduzione al networking
- Gli strumenti di attacco
- Gli strumenti di difesa

Servizi di sicurezza

- Una rete offre servizi, ovvero scambi di dati tra nodi della rete.
- I servizi possono essere resi sicuri attraverso varie tecniche (ad es. crittografia)
- In tal caso si parla di servizi di sicurezza, ovvero servizi che la rete offre per rendere sicuri gli scambi di dati
- Illustriamo con degli esempi (in negativo) quali sono i servizi di sicurezza èpiù richiesti

Mafiaboy contro Yahoo, Amazon, Ebay

I fatti

- Nel febbraio del 2000 un ragazzo di 17 anni, noto come *mafiaboy* inizia un attacco di tipo *DDOS*, distributed denial of service, contro alcuni siti molto noti.
- L'attacco viene portato da una cinquantina di computer da lui precedentemente compromessi appartenenti a reti di università, enti pubblici ecc. . . con molta banda a disposizione.
- I siti yahoo.com, eaby.com, cnn.com sono rimasti irraggiungibili per alcune ore
- Mafiaboy se l'è cavata con 8 mesi di riformatorio e l'interdizione di attività in forum, liste, gruppi dedicati ai temi del cracking

Disponibilità del servizio

Disponibilità

- Il servizio deve essere sempre raggiungibile
- La disponibilità viene violata se siete vittima di un attacco DoS: Denial of Service
- La disponibilità del servizio è la cosa più difficile da garantire:
  - Esistono sempre limiti fisici delle risorse
  - Realizzare un attacco DoS deve costare il più possibile
- La disponibilità si ottiene con una accurata progettazione della rete

Maryland contro Diebold

I fatti

- Nello stato del Maryland dal 2002 sono state introdotte le macchine DRE (Direct Recording Electronic) Voting Machine prodotte dall'azienda Diebold.
- Lo stato del Maryland ha commissionato diverse ricerche per valutare l'affidabilità delle macchine a ricercatori indipendenti.
- I ricercatori sono stati in grado di:
  - leggere i dati relativi alle votazioni
  - inserire codice nelle macchine, in modo da cambiarne il comportamento
  - modificare le schede magnetiche dei votanti per poter votare più volte.

Segretezza dei dati scambiati

Segretezza

- I dati scambiati devono rimanere riservati tra le parti che partecipano allo scambio
- Le reti ethernet permettono, generalmente, di fare *sniffing* dei pacchetti
- Per ottenere segretezza si devono utilizzare algoritmi di crittografia (simmetrici, asimmetrici, distribuiti. . .)

Integrità dei dati scambiati

Integrità

- I dati devono raggiungere la destinazione senza essere stati modificati
- Si possono modificare dati cifrati senza decifrarli (attacchi di *bit flipping*)
- Per ottenere l'integrità dei dati si devono utilizzare funzioni di *hashing*

Phishing

SANPAOLO.com

Gentile Cliente di **Sanpaolo IMI,**

Il Servizio Tecnico di Sanpaolo IMI sta eseguendo un aggiornamento programmato del software al fine di migliorare la qualità dei servizi bancari.

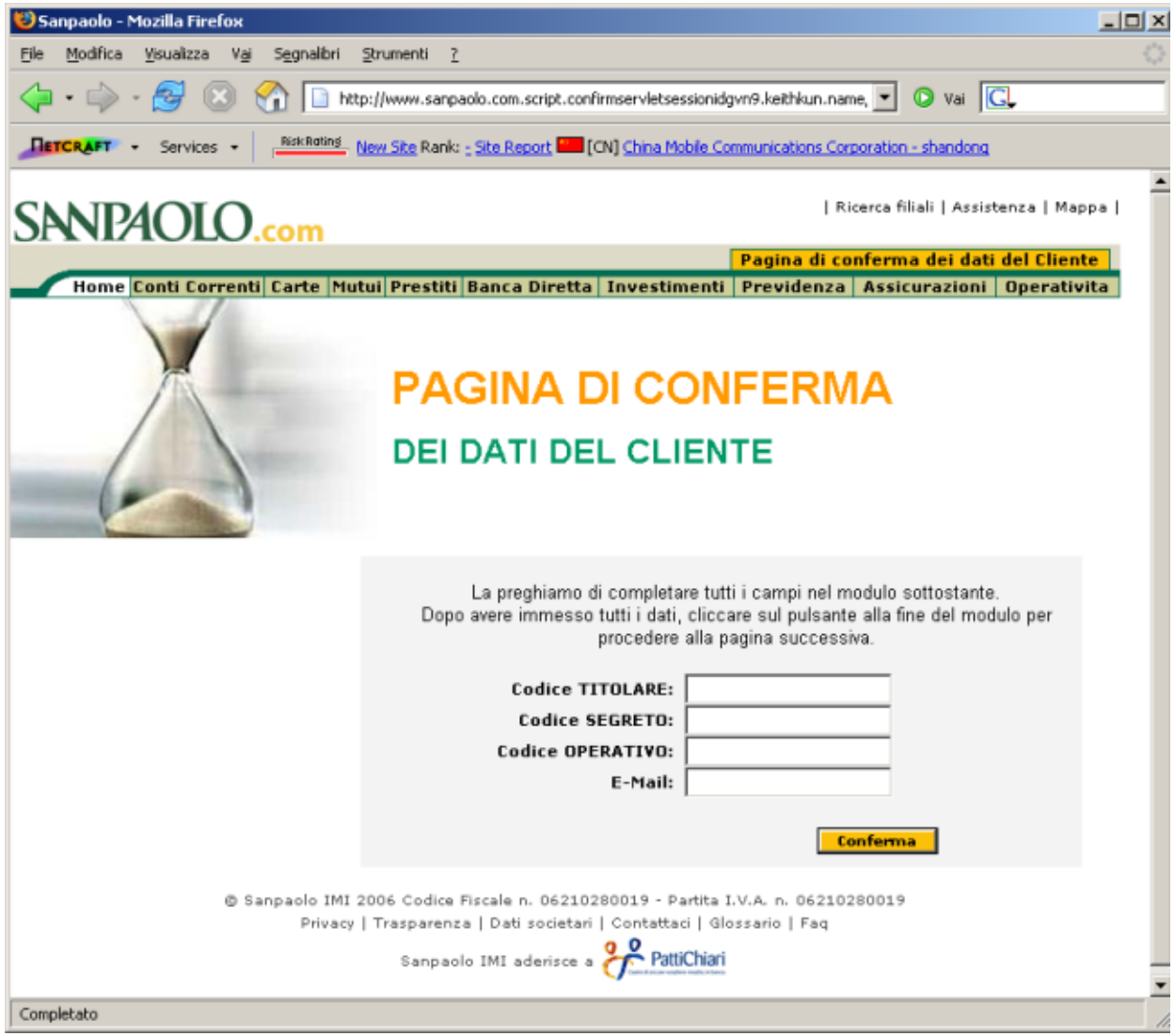
Le chiediamo di avviare la procedura di conferma dei dati del Cliente.
A questo scopo, La preghiamo di cliccare sul link che Lei troverà alla fine di questo messaggio.

http://www.sanpaolo.com/script/ConfirmServletSessionIDGvN9wq22FL7IIJ82kZ

Ci scusiamo per ogni eventuale disturbo, e La ringraziamo per la collaborazione.

© Sanpaolo IMI 2006 Codice Fiscale n. 06210280019 - Partita I.V.A. n. 06210280019

Phishing


Sanpaolo - Mozilla Firefox
File Modifica Visualizza Vai Segnalibri Strumenti ?
http://www.sanpaolo.com.script.confirmservletsessionidgvn9.keithkun.name,
Vai
Services
New Site Rank: - Site Report [CN] China Mobile Communications Corporation - shandong
SANPAOLO.com
| Ricerca filiali | Assistenza | Mappa |
Pagina di conferma dei dati del Cliente
Home Conti Correnti Carte Mutui Prestiti Banca Diretta Investimenti Previdenza Assicurazioni Operativita
PAGINA DI CONFERMA
DEI DATI DEL CLIENTE
La preghiamo di completare tutti i campi nel modulo sottostante.
Dopo avere immesso tutti i dati, cliccare sul pulsante alla fine del modulo per procedere alla pagina successiva.
Codice TITOLARE:
Codice SEGRETO:
Codice OPERATIVO:
E-Mail:
Conferma
© Sanpaolo IMI 2006 Codice Fiscale n. 06210280019 - Partita I.V.A. n. 06210280019
Privacy | Trasparenza | Dati societari | Contattaci | Glossario | Faq
Sanpaolo IMI aderisce a PattiChiari
Completato

Autenticazione del mittente dei dati scambiati

Autenticazione

- Chi riceve un'informazione deve essere sicuro che il mittente è effettivamente quello dichiarato
- I protocolli di internet spesso permettono di effettuare lo *spoofing* degli indirizzi mittente, ad esempio per le email

Le aste on-line:

Alcuni fatti

- Nell'ottobre 2003 la procura di Milano, in seguito ad un sequestro eseguito dall guadia di finanza di Milano indice un'asta on-line.
- Foto degli oggetti sequestrati sono disponibili su un sito, le offerte possono essere inoltrate via fax.
  - Chi garantisce che il mio fax sarà considerato?
  - Chi garantisce l'identità di chi effettua le offerte?
  - Chi garantisce la validità delle offerte?
  - Se le offerte possono essere facilmente invalidabili come si impediscono rialzi concordati?

Non ripudiabilità dei dati scambiati

Non ripudiabilità

- Chi invia un messaggio non può in seguito negare di averlo mandato
- Importante soprattutto a livello di applicazione, nello scambio di documenti

America On Line e la privacy dei suoi utenti:

I fatti

- Agosto 2006: il portale AoL, uno dei più grossi provider nonchè motore di ricerca americano mette erroneamente in rete un file di 440Mbyte contenente le ricerche effettuate negli utlimi 3 mesi da 500000 utenti.
- Per ogni ricerca viene riportato un ID anonimizzato dell'utente in questione, la stringa ricercata, i risultati e su quale dei risultati l'utente ha cliccato.
- Alcuni esempi di contenuti:

personal injury, auto accident pictures, divorce law,
blackberry, family law, florida divorce law,
palm beach county family connection,
florida criminal lawyer, [persons name],
[persons name HOUSE], [persons name and JUDGE],
code of judicial conduct

strippers men, men in briefs, men in speedos, tan speedos, tanning oil, man sexy brief, man swimsuit

Anonimato

La possibilità di immettere informazioni in una rete senza che queste siano direttamente collegabili all'identità del mittente.

- Esistono reti anonimizzanti:
  - Tor
  - freenet
  - Remailer anonimi
- Perchè si vuole anonimato:
  - Forse perchè si vogliono commettere atti illeciti senza essere rintracciati...
  - ...o forse perchè non si è in condizione di esercitare i propri diritti civili.
- Le reti anonimizzanti producono entrambe le conseguenze, ma non bisogna considerarle con pregiudizio. In ogni caso, perche' AoL mantiene quei database?

Malware[1]

Si definisce malware un qualsiasi software creato con il solo scopo di causare danni più o meno estesi al computer su cui viene eseguito.

- Virus: programmi che si diffondono copiandosi all'interno di altri programmi. Si trasmettono da un computer a un altro tramite lo spostamento di file infetti ad opera degli utenti.
- Worm: questi malware non hanno bisogno di infettare altri file per diffondersi, perché modificano il sistema operativo della macchina ospite in modo da essere eseguiti automaticamente e tentare di replicarsi sfruttando per lo più Internet.
- Trojan horse: software che oltre ad avere delle funzionalità lecite, utili per indurre l'utente ad utilizzarli, contengono istruzioni dannose che vengono eseguite all'insaputa dell'utilizzatore.
- Spyware: software che vengono usati per raccogliere informazioni dal sistema su cui sono installati e per trasmetterle ad un destinatario interessato.
- inoltre Dialer, Rootkit, Backdoor ecc. . .

[1] definizioni da wikipedia

Gli attaccanti

Hacker

Storicamente il termine hacker non ha un'accezione negativa. Hack significa letteralmente fare a pezzi, spezzare in modo irregolare, hackers si auto definirono alcuni scienziati del MIT (MAssachutsets Institute of Technology) riferendosi al loro piacere nel sezionare, scomporre gli apparati al fine di comprenderne e migliorarne il funzionamento.

- Un hacker generalmente non produce danni, non ruba denaro, non taglieggia...
- ...ma si diverte a verificare la sicurezza delle reti che incontra (e anche questo può costituire reato)
- Negli ultimi anni il termine è stato spesso abusato dai media, per indicare malfattori di vario tipo.

Gli attaccanti

Cracker

Un cracker è qualcuno il cui scopo è quello di penetrare nei sistemi informatici che non gli appartengono per renderli inutilizzabili o per guadagnarne qualcosa.

- Nel 99% dei casi, quando si sente parlare in televisione di hacker, si deve intendere un cracker, cioè una persona dotata tecnicamente che sfrutta le sue conoscenze per commettere azioni illegali.
- Dietro ad un cracker ci possono essere grossi interessi, associazioni a delinquere o terrorismo

Gli attaccanti

Lamer

Un lamer è una persona poco dotata tecnicamente, con pochi mezzi tecnici a disposizione, che raccoglie programmi su internet per riuscire a penetrare in reti che non gli appartengono.

- generalmente la motivazione del lamer è la gloria, il potersi vantare delle azioni svolte.
- il lamer è il prototipo dell'adolescente sveglio che cerca fama nel suo piccolo gruppo di conoscenze.

Evoluzione dell'attaccante

- 1983: Fred Cohen (University of Southern California) conia il termine *computer virus* come *un programma che colpisce altri programmi modificandoli in un modo da includere delle copie di se stesso*.
- Per anni i virus sono stati considerati un gioco fastidioso creato da hacker burloni. Monitor che si capovolgono di 90 gradi, fuochi d'artificio, solo raramente perdita di dati o altri danni. Chi crea i virus viene dipinto dai media come un piccolo genio del computer in vena di scherzi.
- Tutto questo cambia radiclamente nel 1989: in Indiana viene arrestato Fry Guy un ragazzo di 16 anni che utilizzando la sua bravura tecnica era riuscito a introdursi nelle centrali della AT&T e deviare le telefonate al 911 (il 113 americano) di parte di New York verso un telefono erotico. Gli scherzi cominciavano a essere pesanti.

Evoluzione dell'attaccante

- Nel 1991 Symantec rilascia il Norton Anti-Virus, la sicurezza diventa un business.
- Da allora ad oggi molte cose sono cambiate, sia tra gli attaccanti che tra gli esperti di sicurezza, alcuni esempi:
  - 12/2005: Il direttore dell'istituto SANS dichiara in una conferenza stampa che il network governativo americano subisce attacchi provenienti dalla Repubblica Poplare Cinese, e che data l'intensità degli attacchi, questi possono provenire soltanto da organizzazioni governative e militari.
  - 2005: il rapporto annuale dell'FBI sul cybercrime sostiene che nel 2005 il mercato del crimine digitale (attacchi, furti, taglieggiamenti ma anche pirateria) ha superato il fatturato del mercato della droga. Inoltre, la media del costo di una intrusione informatica per le aziende americane si aggira intorno ai 250.000 $.

Evoluzione dell'attaccante

- Per rendere più chiara l'idea descriviamo in breve cosa succede comunemente quando i nostri computer si prendono un virus:
  1. Alcune protezioni vengono disabilitate (antivirus, firewall)
  2. Il virus si diffonde in più canali possibili (email)
  3. Viene aperta una connessione ad un canale IRC (una chat)
  4. Nella chat si trovano connessi migliaia di altri computer infetti
  5. Alla chat si connette anche un amministratore che impartisce comandi ai computer, quali comandi?
     - Inviare email di SPAM
     - Raccogliere indirizzi email per costruire liste di SPAM
     - Raccogliere dati sensibili (password, numeri di carte di credito) presenti sul computer
     - Iniziare connessioni verso un singolo host per produrre un attacco denial of service
     - Portare altri attacchi verso terze macchine

Evoluzione dell'attaccante

- Esempio: Claria.com
  - Vende pubblicità online
  - distribuisce il software Gator utilizzando qualsiasi mezzo (licenze non valide, inserendolo in programmi su filesharing o utilizzando siti contenenti codice malevolo)

  - Nel 2004 ha prodotto vendite per 117.000.000 $

Evoluzione dell'attaccante

- Si intuisce che i tempi degli hacker burloni sono finiti, adesso i nemici sono associazioni più o meno legali che hanno a disposizione enormi capitali e scopi ben strutturati.
- Quando si viene attaccati le nostre informazioni personali sono a rischio, i nostri recapiti, numeri di carta di credito e password vengono raccolti e inseriti in database, questi database vengono utilizzati e venduti a nostra insaputa.
- Ancora peggio è quando l'attacco subito è un punto di partenza per un ulteriore attacco, visto che si prende parte ad un crimine.
- Se da una macchina da me amministrata parte un attacco verso terzi, sono io a dover dimostrare di non essere responsabile. Cosa comporta:
  - Perdita di connettività: il mio provider stacca la spina
  - Perdita di immagine verso clienti
  - Possibili coseguenze legali

Quantificare i danni:

Si può fare una cost analisys sulla sicurezza informatica? Normalmente chi è vittima di attacchi non diffonde la dimensione dei danni provocati per evitare il danno (ulteriore) di immagine, quindi non c'e' molta esperienza. Un esempio può essere il seguente, preso da una ricerca Forrester.

Quantificare i danni:

- Scenario: furto di un milione di dollari da una banca online con 250.000 clienti.

Rimborso del furto	100.000.000$
48 ore di down	96.000.000$
Controllo su tutti i conti	1.000.000$
Danni di immagine	6.000.000$
Aumento premi assicurativi	5.000.000$
Perdita di 10000 clienti	2.500.000$
Totale	111.500.000$

Pubbliche amministrazioni

- Finora abbiamo parlato di conseguenze economiche, vediamo alcuni esempi di insicurezze in ambito di pubblica amministrazione:
  - 21 ottobre 2002: la marina americana subisce un furto di quasi 600 computer, almeno 14 dei quali contenevano informazioni classificate.
  - 19 giugno 2006: un impiegato della U.S. Financial services viene derubato del proprio laptop, contenente i dati di previdenza sociale di 13000 lavoratori.
  - giugno 2006: un impegato del dipartimento dei veterani americano porta a casa un laptop contenente i dati privati di 26 milioni di persone e subisce un furto. I veterani chiedono un rimborso di 1000 euro per ogni fascicolo perso.

Elementi di networking

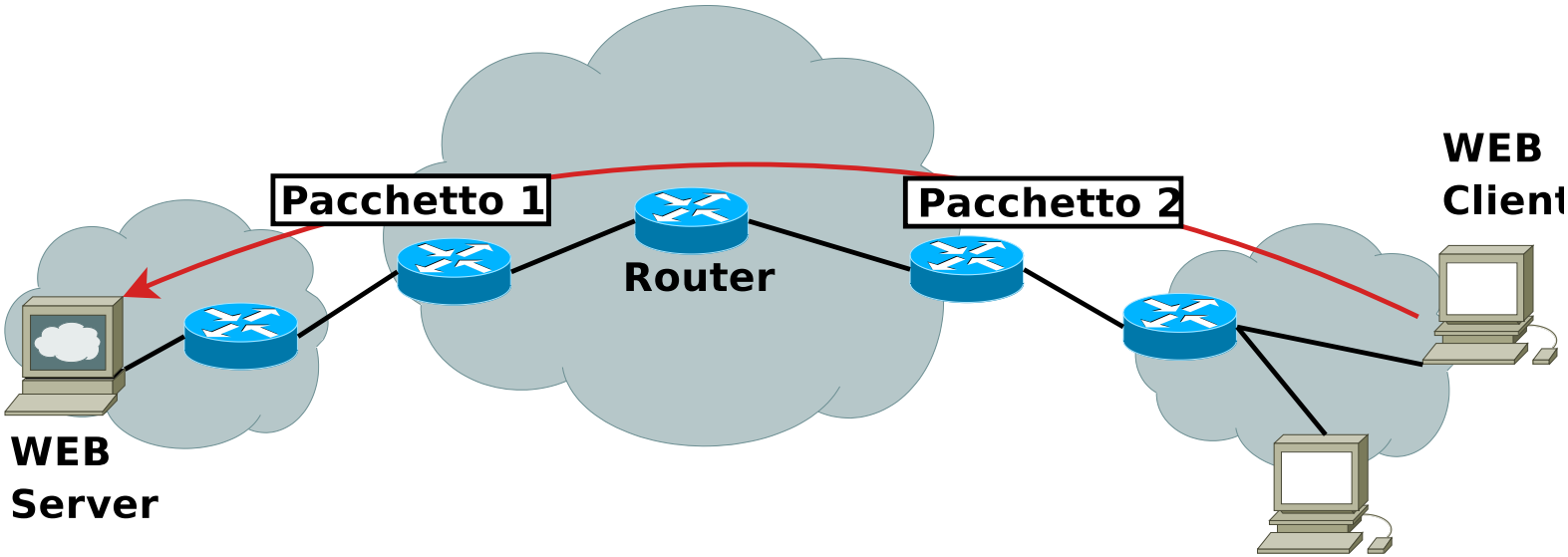
Per capire quali sono i pericoli più comuni legati alle reti di calcolatori è necessario capirne in parte il funzionamento. Ci limiteremo a illustrare come funzionano email e WWW.

I protocolli di base di internet

Lo scambio di messaggi che attraversano internet è governato da protocolli. Il protocollo che sta alla base delle comunicazioni è l'IP, Internet Protocol. L'IP stabilisce le seguenti regole:

- I messaggi sono trasportati in *pacchetti*, se dobbiamo trasferire un file, questo viene suddiviso in frammenti ognuno dei quali viaggia nella rete in modo indipendente. Le macchine intermedie che si occupano di inoltrare i pacchetti si chiamano router.
- Ogni macchina in Internet possiede un indirizzo, detto indirizzo IP o semplicemente IP. Gli indirizzi sono costituiti da quattro numeri interi tra 0 e 254 (ad esempio 64.233.167.99). In ogni pacchetto è contenuto l'indirizzo destinazione e quello mittente.
- I pacchetti devono essere ricostruiti a destinazione per ricreare l'informazione originale, per evitare che i pacchetti si perdano, duplichino, o arrivino con eccessivo ritardo esiste il protocollo TCP, che garantisce la gestione del flusso dei pacchetti, ovvero di una connessione.

Il protocollo IP



Il protocollo TCP

Sarebbe complicato spiegare nel dettaglio il protocollo TCP, ne descriviamo alcune parti salienti:

- Quando vogliamo scaricare un file, per esempio un'email, ci interessa che i pacchetti arrivino tutti e in ordine giusto. TCP numera tutti i pacchetti con dei numeri di sequenza in modo che nel momento in cui vengano ricevuti si può ricostruire il flusso corretto.
- TCP definisce anche dei servizi, ovvero un numero identificativo per il tipo di traffico che un server accetta. Ad esempio, per l'invio di posta elettronica si usa il numero 25. Un server di posta elettronica al momento della ricezione di un pacchetto controla che il pacchetto sia della classe 25, e in quel caso lo accetta. Si dice che il server *ha la porta 25 aperta*.
- Una volta ricevuto il pacchetto, le informazioni vengono inviate al programma che gira sul server e che si occupa di gestire la posta elettronica.

Il protocollo DNS: domain name system

Ogni macchina è identificata da un indirizzo IP, ma noi non li usiamo mai. Che cosa succede quando digitiamo www.google.it su un browser?

- Il nome di dominio www.google.it non è un indirizzo IP, quindi va tradotto in un indirizzo IP.
- Esistono degli archivi in rete che dato un nome di dominio ci restituiscono l'indirizzo IP.
- Il nostro browser quindi, prima chiede al server DNS la risoluzione dell'indirizzo IP, poi inizia la comunicazione vera e propria.
- Ecco spiegato perchè quando configurate una macchina per andare su internet vi viene chiesto un *indirizzo di server DNS*.

Il DDOS di Mafiaboy

Syn flood:

- Ogni volta che un server riceve un pacchetto con SYN=1 alloca delle risorse di memoria per gestire la connessione che sta per essere creata, quindi invia un pacchetto con i flag SYN=1, ACK=1 e fa partire un timeout per attendere l'arrivo del terzo pacchetto dell'handhake. Si dice che in quel momento sul server c'e' una connessione *half-open*.
- Se un attaccante invia un grande numero di pacchetti con SYN=1 e indirizzi IP mittente falsi, prima o poi la memoria del server si saturerà e il server comincerà a scartare pacchetti.
- In questo modo si impedisce ad altre macchine di accedere al servizio.

Attacchi a livello IV:

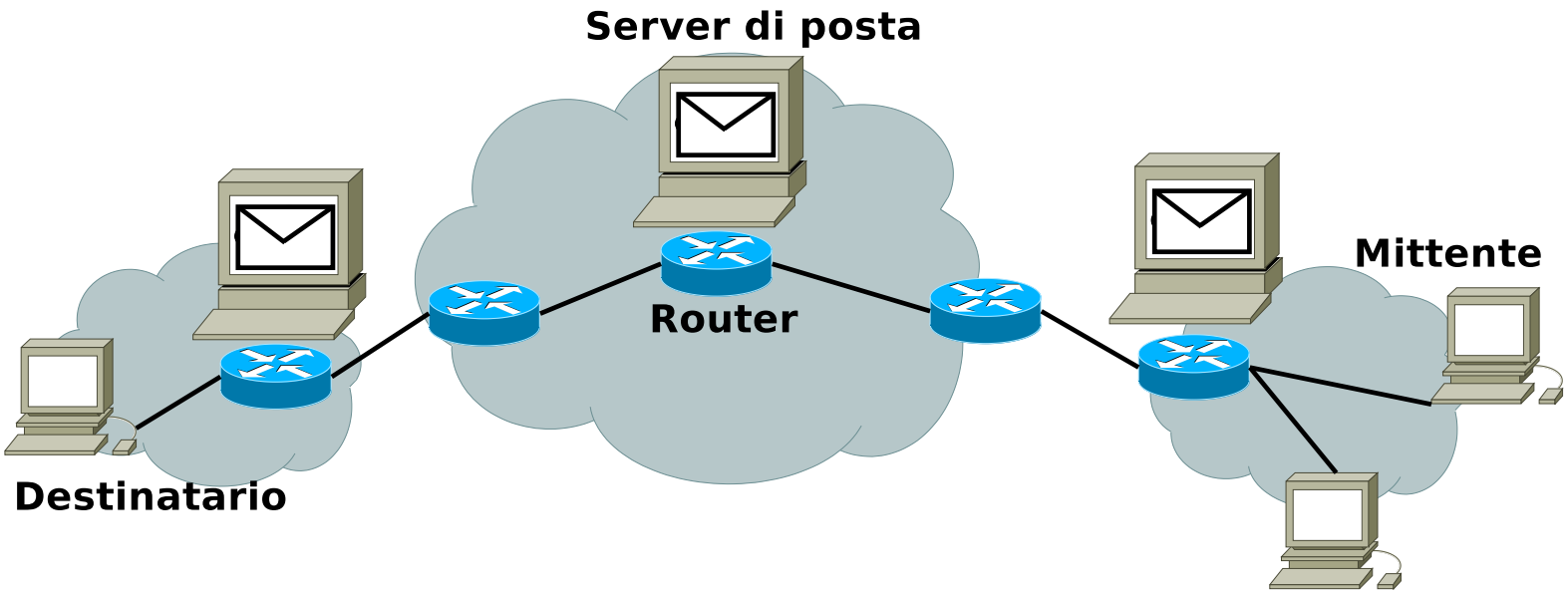
Syn cookies:

- Non esistono rimedi comunemente accettati per gli attacchi di Syn Flood, con poca banda a disposizione si possono raggiungere i limiti di memoria di un server.
- Un metodo per evitare questo attacco prevede l'utilizzo di syn cookies [**?**]:
  - quando si invia il pacchetto SYN=1 e ACK=1 non si sceglie un numero di sequenza casuale, ma si sceglie un numero che è la codifica di informazioni riguardanti la connessione e non si alloca nessuna memoria.
  - Quando si rieceve il terzo pacchetto della connessione, questo contiene l'ACK inviato, da cui si riestraggono le informazioni codificate. A quel punto la connessione è aperta.
  - Standard compliant?

Un esempio facile: la posta elettronica

- La posta elettronica non viene ricevuta direttamente sul vostro computer. Esiste un server di posta elettronica che mantiene le vostre email fino a quando voi non decidete di scaricarle.
- quando voi scrivete un email succedono le seguenti cose:
  - Scrivete il testo sulla vostra macchina diretto a maccari@lart.det.unifi.it.
  - Premete invio, il testo viene spezzato in pacchetti, i pacchetti viaggiano indipendenti verso il server di posta lart.det.unifi.it.
  - Quando arriva a destinazione viene salvato nella cartella maccari.
  - Durante il percorso può attraversare altri server di posta.

Posta elettronica



Posta elettronica

```
Received: from lenst.det.unifi.it (lenst.det.unifi.it [150.217.8.24])
    by cnit1.ing.unifi.it (8.12.8/8.12.8) with ESMTP
    for <maccari@cnit1.ing.unifi.it>; Mon, 2 Oct 2006 16:38:32 +0200
Received: from [67.87.24.53]
    by lenst.det.unifi.it (Postfix) with ESMTP id D2F2A2C6E57
    for <maccari@cnit1.ing.unifi.it>; Mon,  2 Oct 2006 16:38:28 +0200
Date: Mon, 02 Oct 2006 16:42:30 +0200
From: Leonardo Maccari <maccari@lenst.det.unifi.it>
User-Agent: Thunderbird 1.5.0.5 (X11/20060812)
To: maccari@cnit1.ing.unifi.it
Subject: prova

Solo una prova
-
            Leonardo Maccari, Telecommunication Network Lab,
Department of Electronics and Telecommunications, University of Florence
  http://lart.det.unifi.it/Members/maccari/  Lab Tel:+39 055 4796467
  Key fingerprint = 3129 C583 F03B 2E73 0115  C040 3489 0185 B592 19FE
```

Problemi della posta elettronica

Riferendosi ai servizi di sicurezza che abbiamo descritto nelle prime slides, la posta elettronica non ne garantisce alcuno:

- I nodi intermedi possono leggere il contenuto dei messaggi $\rightarrow$ niente segretezza
- I nodi intermedi possono modificare il contenuto dei messaggi $\rightarrow$ niente integrità
- Si possono madare messaggi con indirizzo mittente falsificato $\rightarrow$ niente autenticazione
- Non esiste prova della ricezione o dell'effettivo invio del messaggio $\rightarrow$ niente non ripudiabilità
- Anche se l'indirizzo email del mittente è falsificabile, l'indirizzo IP del mittente è reale e riportato negli header $\rightarrow$ niente anonimato

I pericoli veicolati dalla posta elettronica

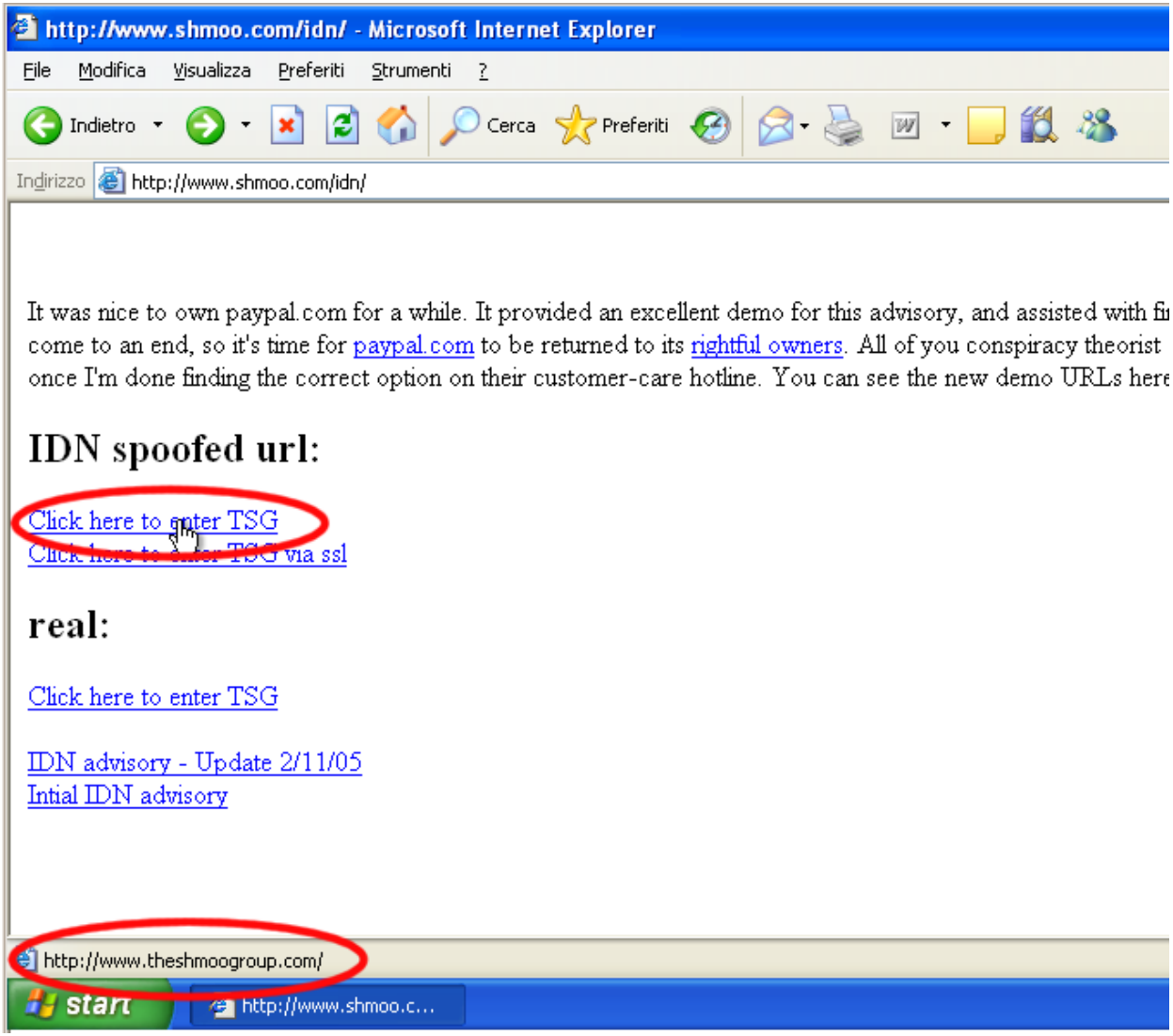
Le caratteristiche appena elencate fanno della posta elettronica un ottimo veicolo di attacchi:

- Attachment: allegato alle email si può trovare ogni sorta di virus, spyware, worm ecc. . . normalmente è compito dell'antivirus, se aggiornato, evitare che gli attachment danneggino il computer.
- Phishing: email che tentano di convincere chi le riceve a rivelare informazioni private, quali password o numeri di carta di credito.
- SPAM: email non richieste che pubblicizzano prodotti (N.B. più del 50% del traffico generato su internet è costituito da SPAM)

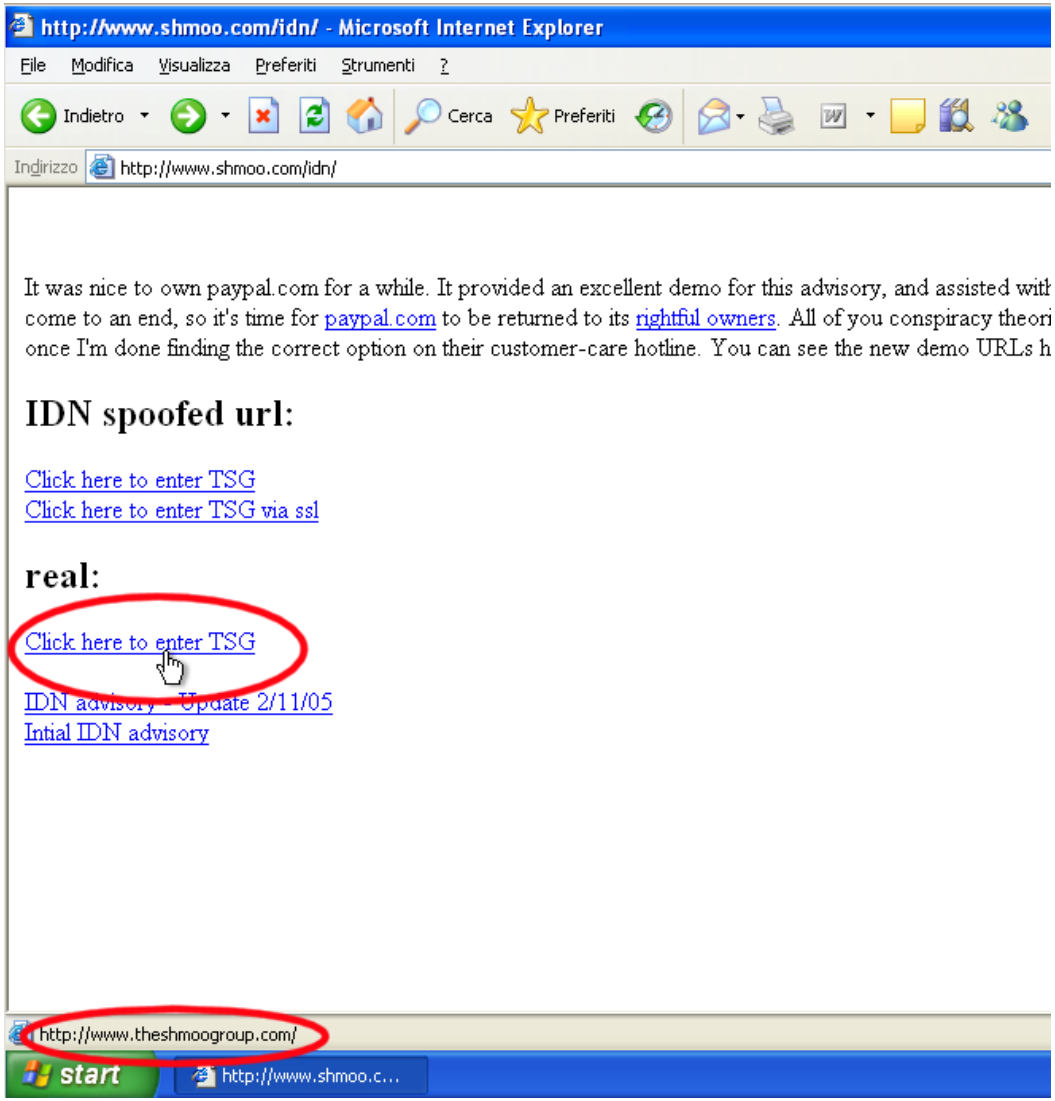
Sicuramente siete stati informati sui periocoli appena illustrati, ne cito un paio meno noti:

- Omographic attacks: consistono nel sostituire un indirizzo internet con uno diverso ma scritto in modo molto simile, un esempio:
  - In cirillico esiste un carattere del tutto simile alla *a*, ma diverso per il browser. Esistono url quindi del tutto simili alla vista a quelli originali ma che vengono reindirizzati su indirizzi IP diversi. Alcuni browser si accorgono che la codifica è diversa e vi avvertono.
  - Questo tipo di attacco è veicolato molto spesso in email di phishing.

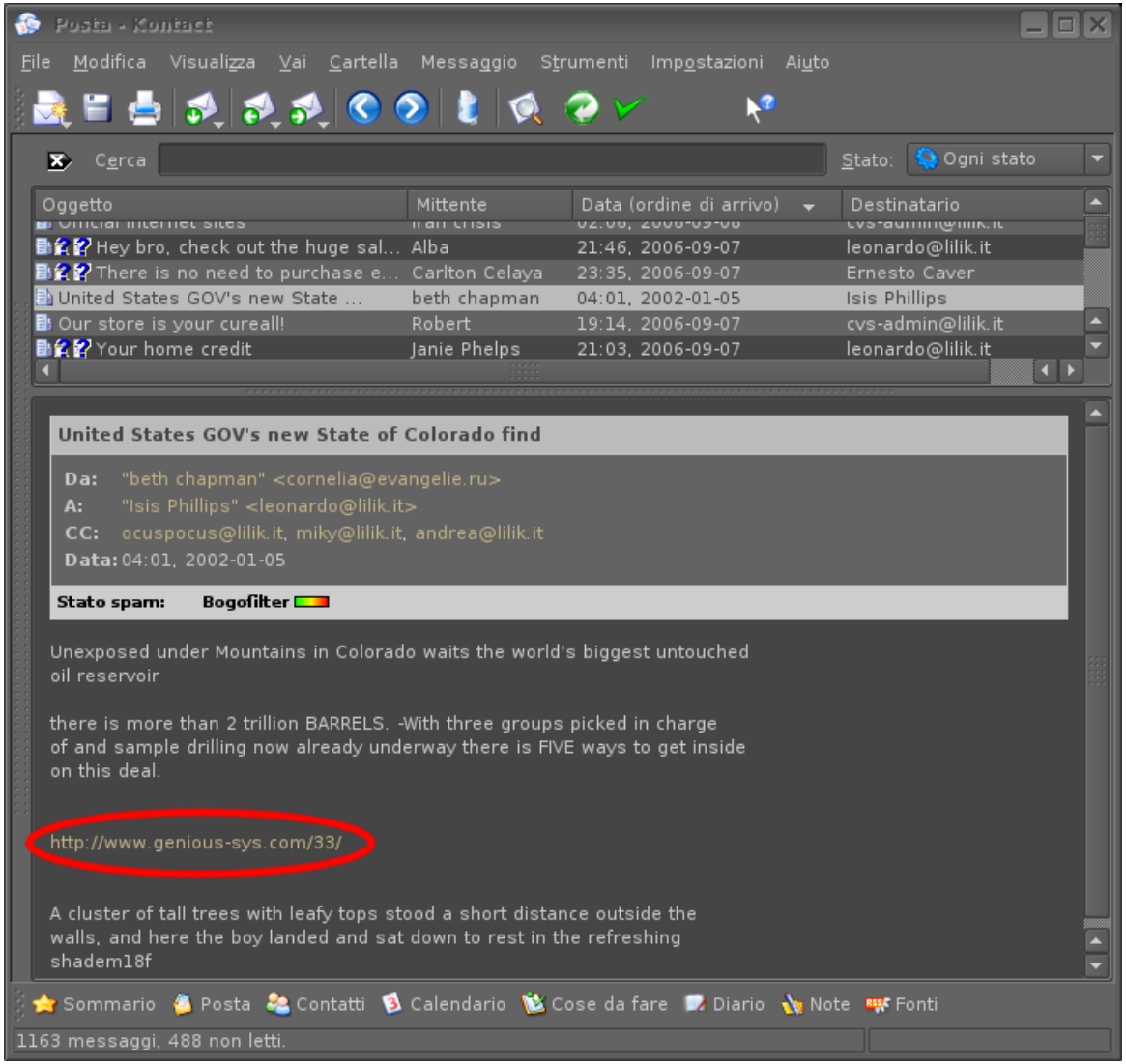
Omographic attacks



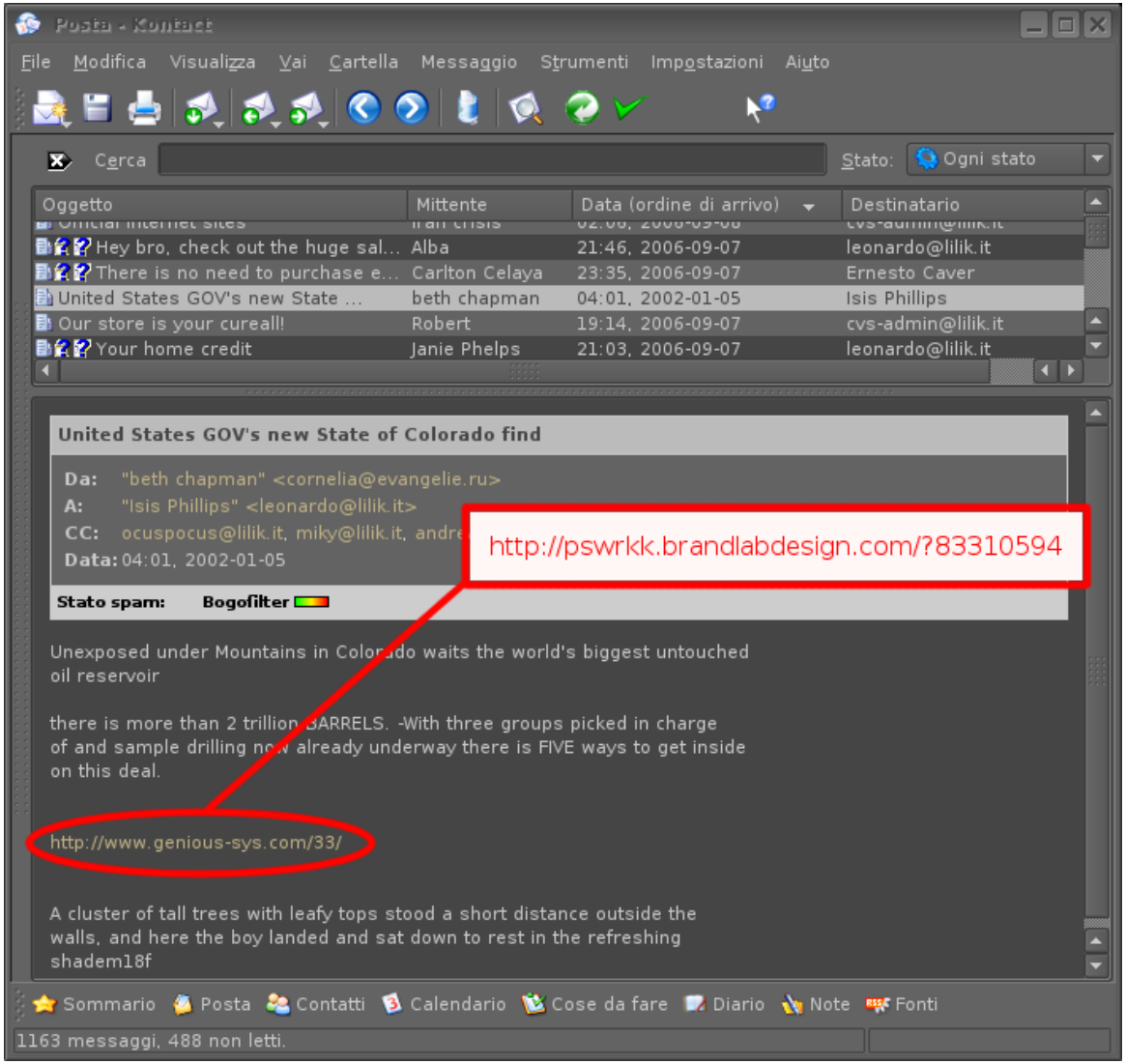
Omographic attacks



Url unici


Posta - Kontact
File Modifica Visualizza Vai Cartella Messaggio Strumenti Impostazioni Aiuto
Cerca
Stato: Ogni stato
Oggetto
Mittente
Data (ordine di arrivo)
Destinatario
Hey bro, check out the huge sal... Alba 21:46, 2006-09-07 leonardo@lilik.it
There is no need to purchase e... Carlton Celaya 23:35, 2006-09-07 Ernesto Caver
United States GOV's new State ... beth chapman 04:01, 2002-01-05 Isis Phillips
Our store is your cureall! Robert 19:14, 2006-09-07 cvs-admin@lilik.it
Your home credit Janie Phelps 21:03, 2006-09-07 leonardo@lilik.it
United States GOV's new State of Colorado find
Da: "beth chapman" <cornelia@evangelie.ru>
A: "Isis Phillips" <leonardo@lilik.it>
CC: ocuspocus@lilik.it, miky@lilik.it, andrea@lilik.it
Data: 04:01, 2002-01-05
Stato spam: Bogofilter
Unexposed under Mountains in Colorado waits the world's biggest untouched oil reservoir
there is more than 2 trillion BARRELS. -With three groups picked in charge of and sample drilling now already underway there is FIVE ways to get inside on this deal.
http://www.genious-sys.com/33/
A cluster of tall trees with leafy tops stood a short distance outside the walls, and here the boy landed and sat down to rest in the refreshing shadem18f
Sommario Posta Contatti Calendario Cose da fare Diario Note Fonti
1163 messaggi, 488 non letti.

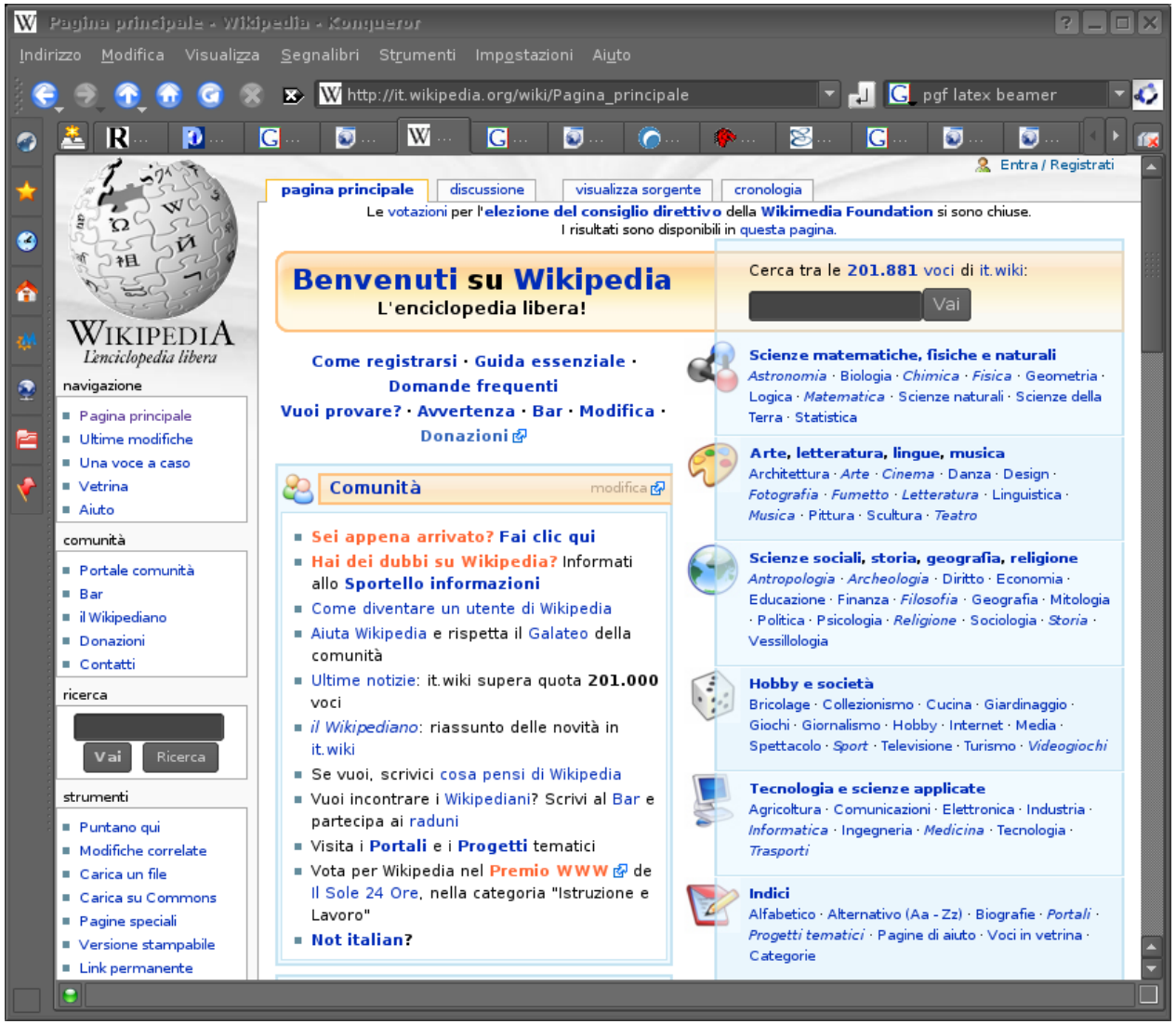
Url unici


Posta - Kontact
File Modifica Visualizza Vai Cartella Messaggio Strumenti Impostazioni Aiuto
Cerca
Stato: Ogni stato
Oggetto | Mittente | Data (ordine di arrivo) | Destinatario
Hey bro, check out the huge sal... | Alba | 21:46, 2006-09-07 | leonardo@lilik.it
There is no need to purchase e... | Carlton Celaya | 23:35, 2006-09-07 | Ernesto Caver
United States GOV's new State ... | beth chapman | 04:01, 2002-01-05 | Isis Phillips
Our store is your cureall! | Robert | 19:14, 2006-09-07 | cvs-admin@lilik.it
Your home credit | Janie Phelps | 21:03, 2006-09-07 | leonardo@lilik.it
United States GOV's new State of Colorado find
Da: "beth chapman" <cornelia@evangelie.ru>
A: "Isis Phillips" <leonardo@lilik.it>
CC: ocuspocus@lilik.it, miky@lilik.it, andre
Data: 04:01, 2002-01-05
Stato spam: Bogofilter
http://pswrkk.brandlabdesign.com/?83310594
Unexposed under Mountains in Colorado waits the world's biggest untouched oil reservoir
there is more than 2 trillion BARRELS. -With three groups picked in charge of and sample drilling now already underway there is FIVE ways to get inside on this deal.
http://www.genious-sys.com/33/
A cluster of tall trees with leafy tops stood a short distance outside the walls, and here the boy landed and sat down to rest in the refreshing shadem18f
Sommario Posta Contatti Calendario Cose da fare Diario Note Fonti
1163 messaggi, 488 non letti.

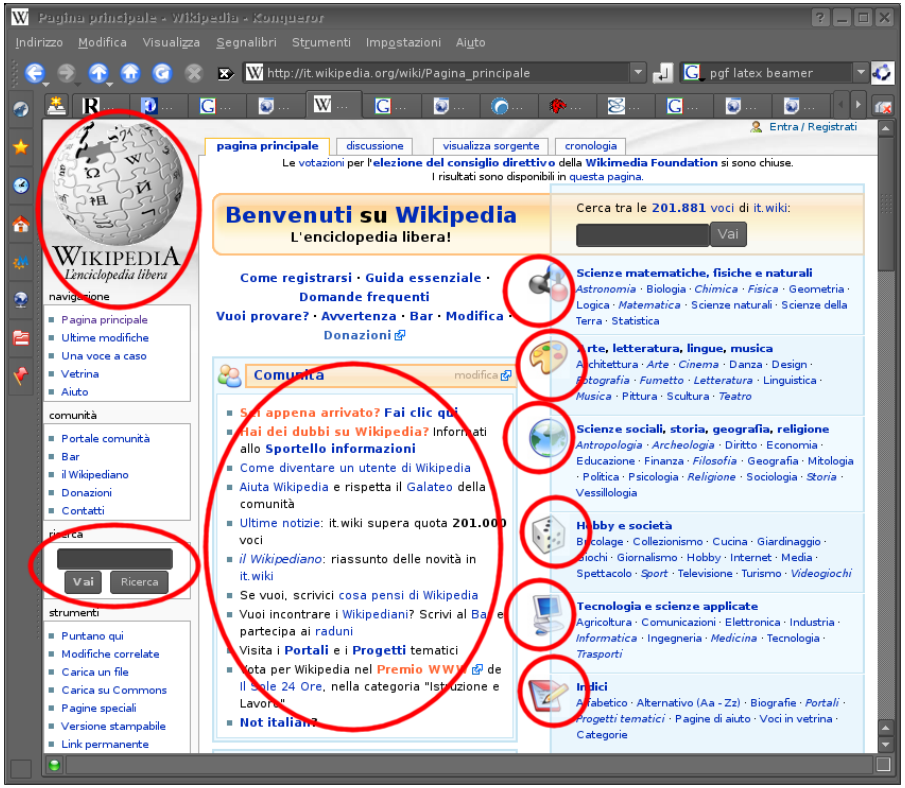
Url unici

- l'url su cui cliccate è un url unico, quindi ogni email di SPAM contiene un url diverso.
- cliccando sull'url state comunicando allo spammer le seguenti cose:
  - l'indirizzo di posta a cui lo SPAM è stato inviato esiste
  - probabilmente non utilizzate un antispam
  - probabilmente vi interessa l'articolo che viene pubblicizzato
- la conseguenza è che riceverete ancora più SPAM

Il WWW


Pagina principale - Wikipedia - Konqueror
Indirizzo Modifica Visualizza Segnalibri Strumenti Impostazioni Aiuto
http://it.wikipedia.org/wiki/Pagina_principale
pgf latex beamer
Entra / Registrati
pagina principale
discussione
visualizza sorgente
cronologia
Le votazioni per l'elezione del consiglio direttivo della Wikimedia Foundation si sono chiuse.
I risultati sono disponibili in questa pagina.
Benvenuti su Wikipedia
L'enciclopedia libera!
Cerca tra le 201.881 voci di it.wiki:
Vai
WIKIPEDIA
L'enciclopedia libera
navigazione
Pagina principale
Ultime modifiche
Una voce a caso
Vetrina
Aiuto
comunità
Portale comunità
Bar
il Wikipediano
Donazioni
Contatti
ricerca
Vai
Ricerca
strumenti
Puntano qui
Modifiche correlate
Carica un file
Carica su Commons
Pagine speciali
Versione stampabile
Link permanente
Come registrarsi · Guida essenziale · Domande frequenti
Vuoi provare? · Avvertenza · Bar · Modifica · Donazioni
Comunità
modifica
Sei appena arrivato? Fai clic qui
Hai dei dubbi su Wikipedia? Informati allo Sportello informazioni
Come diventare un utente di Wikipedia
Aiuta Wikipedia e rispetta il Galateo della comunità
Ultime notizie: it.wiki supera quota 201.000 voci
Il Wikipediano: riassunto delle novità in it.wiki
Se vuoi, scrivici cosa pensi di Wikipedia
Vuoi incontrare i Wikipediani? Scrivi al Bar e partecipa ai raduni
Visita i Portali e i Progetti tematici
Vota per Wikipedia nel Premio WWW de Il Sole 24 Ore, nella categoria "Istruzione e Lavoro"
Not italian?
Scienze matematiche, fisiche e naturali
Astronomia · Biologia · Chimica · Fisica · Geometria · Logica · Matematica · Scienze naturali · Scienze della Terra · Statistica
Arte, letteratura, lingue, musica
Architettura · Arte · Cinema · Danza · Design · Fotografia · Fumetto · Letteratura · Linguistica · Musica · Pittura · Scultura · Teatro
Scienze sociali, storia, geografia, religione
Antropologia · Archeologia · Diritto · Economia · Educazione · Finanza · Filosofia · Geografia · Mitologia · Politica · Psicologia · Religione · Sociologia · Storia · Vessillologia
Hobby e società
Bricolage · Collezionismo · Cucina · Giardinaggio · Giochi · Giornalismo · Hobby · Internet · Media · Spettacolo · Sport · Televisione · Turismo · Videogiochi
Tecnologia e scienze applicate
Agricoltura · Comunicazioni · Elettronica · Industria · Informatica · Ingegneria · Medicina · Tecnologia · Trasporti
Indici
Alfabetico · Alternativo (Aa - Zz) · Biografie · Portali · Progetti tematici · Pagine di aiuto · Voci in vetrina · Categorie

Parti diverse della stessa pagina vengono scaricate utilizzando connessioni TCP diverse.



WWW

Cosa succede quando caricate una pagina web:

- Scrivete l'URL nel browser e premete invio
- Aprite una connessione TCP verso il server DNS che vi restituisce l'indirizzo IP del server a cui vi volete connettere (questo passo è per voi trasparente)
- Scaricate dal server una pagina contenente l'indice di tutte i contenuti (testo, immagini ecc..)
- Il browser apre una connessione per ogni singolo contenuto
- A seconda della velocità di ogni singola connessione, la pagine si carica un frammento alla volta.
- Una volta caricata tutta la pagina non esistono più connessioni in corso, potete consultarla anche off-line.

WWW

Le caratteristiche di sicurezza del web sono le stesse della posta elettronica, cioè quasi niente:

- La risoluzione dell'indirizzo avviene in modo non autenticato: se il vostro server dei nomi è stato manipolato potete essere rediretti in una pagina falsa.
- Non c'è autenticazione, segretezza, non ripudiabilità, integrità dei dati. Ogni router intermedio potrebbe modificare le richieste che fate o le risposte che ricevete.

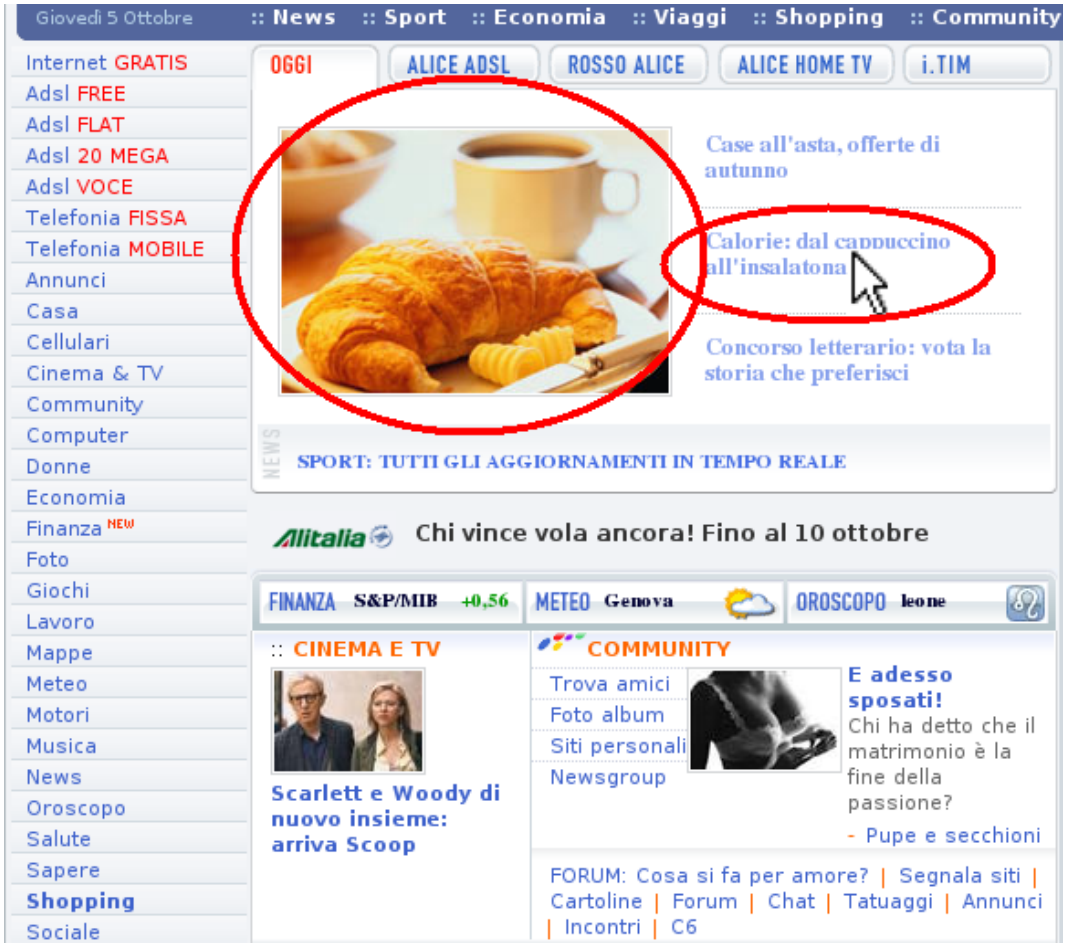
WWW - codice locale

Abbiamo detto che quando la pagina è stata caricata le connessioni sono terminate, quindi si può lavorare offline. Consideriamo il seguente esempio:

- cursore sulla prima riga

WWW - codice locale

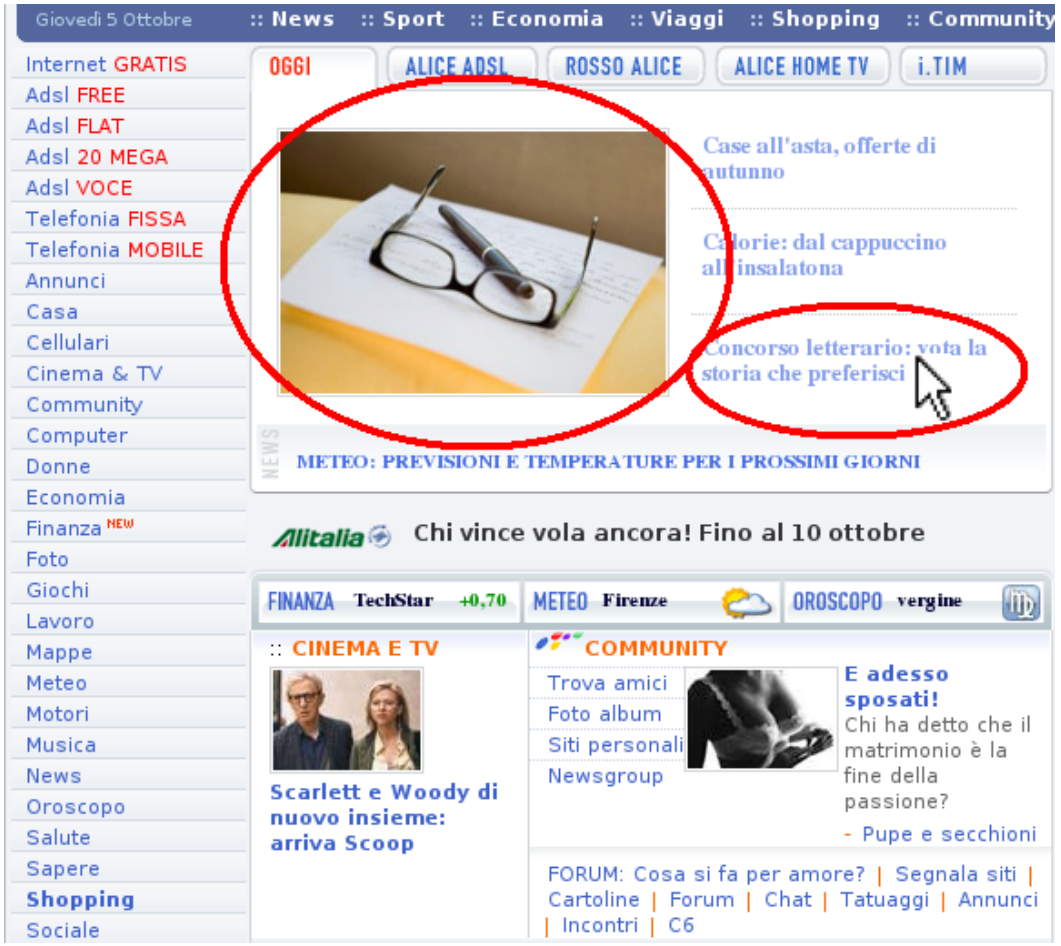
Abbiamo detto che quando la pagina è stata caricata le connessioni sono terminate, quindi si può lavorare offline. Consideriamo il seguente esempio:



- cursore sulla seconda riga

WWW - codice locale

Abbiamo detto che quando la pagina è stata caricata le connessioni sono terminate, quindi si può lavorare offline. Consideriamo il seguente esempio:



- cursore sulla terza riga

La connessione è chiusa ma la pagina cambia!

WWW - codice locale

Questo avviene perchè nella pagina è contenuto codice che viene scaricato in locale e con cui interagite senza avvertire il server. Il codice può essere di vario tipo:

- Javascript
- animazioni flash
- ActiveX
- ...

É come scaricare ed eseguire un programma dalla rete, ma le capacità che questi linguaggi hanno sono molto limitate (ad esempio non possono scrivere su disco).

WWW - codice locale

Può succedere che se il vostro browser non è aggiornato con tutte le patch di sicurezza, un codice locale possa eseguire operazioni molto più gravi:

- eseguire codice
- installare programmi (trojan, virus ecc..)

Quindi, sempre mantenere il sistema operativo (qualsiasi sistema operativo si usi) aggiornato.

Email & Web, riassumendo:

Cosa può succedere all'utente che clicca sullo SPAM:

- l'utente ingenuo può rivelare i propri dati personali ad un sito fraudolento.
- l'utente meno ingenuo, incoraggia comunque lo spammer a inviargli più email
- anche l'utente meno ingenuo, può ritrovarsi rediretto in un sito da cui riceve attraverso codice javascript/activex dei trojan/virus ecc..
- i virus non sono giochini, si può partecipare a crimini e diffondere informazioni private.

Alcuni strumenti di difesa

Esistono molti strumenti che potete utilizzare per aumentare il livello di sicurezza delle vostre comunicazioni. Alcuni di questi riguardano i vostri computer personali, altri sono controllati dall'amministratore della vostra rete. Altri ancora sono mezzi non tecnici, ma legati a buone pratiche di comportamento.

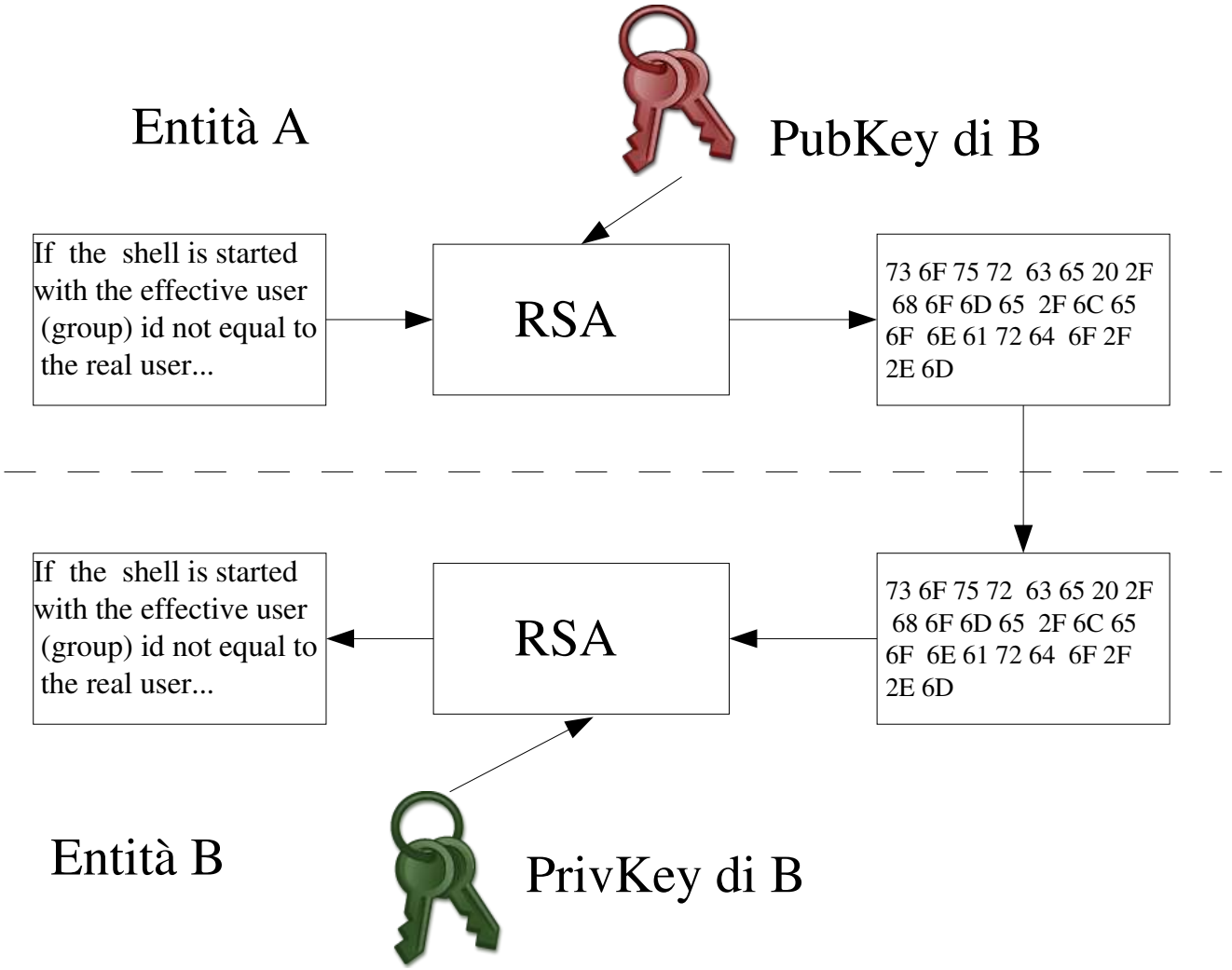
- Firma digitale e comunicazioni cifrate
- IDS/Firewall/Antivirus
- Attenzione al social engeneering!

Cifratura a chiave pubblica/privata

- Ogni soggetto possiede una coppia di chiavi
  - Chiave publica
  - Chiave privata
- Ciò che viene cifrato con una chiave può essere decifrato solo con l'altra
- E' computazionalmente impossibile risalire ad una chiave privata tramite la chiave pubblica

Cifratura e Decifratura

Solo B, conoscendo la chiave PrivKey, può decifrare il documento, si ottiene:



Riassumendo

- Ogni utente ha due chiavi legate in modo inscindibile da una formula matematica
  - una chiave viene resa pubblica
  - l'altra è in possesso del solo utente
- le chiavi pubbliche sono disponibili in un elenco centralizzato consultabile liberamente dagli utenti
- le coppie di chiavi pubbliche/private sono generate a cura dell'utente

La crittografia garantisce:

- Protezione dei documenti
  - integrità
  - confidenzialità
  - autenticazione
  - non ripudiabilità
- Verifica dell'identità dei corrispondenti
  - certificazione
  - autorizzazione

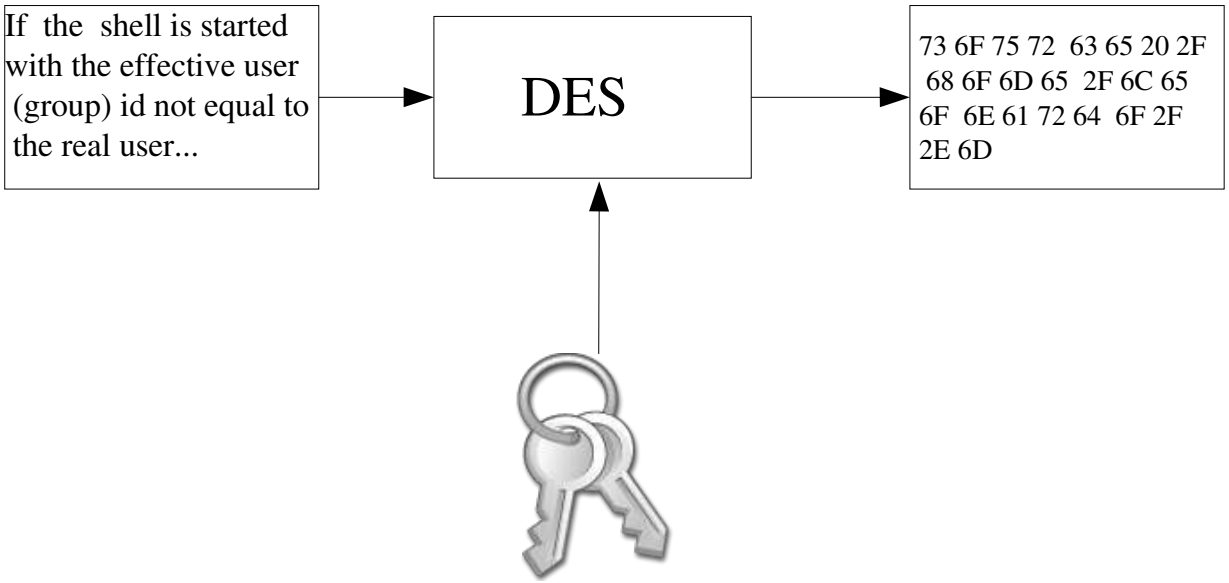
La crittografia garantisce:

- Elementi di un sistema crittografico:
  - cifrario (algoritmo)
  - chiave (informazione)
- Principio di Kerchoffs
  - il metodo si suppone noto a tutti
  - il segreto risiede nella chiave
- La conoscenza della chiave
  - consente di cifrare/decifrare documenti
  - può costituire prova certa di identità

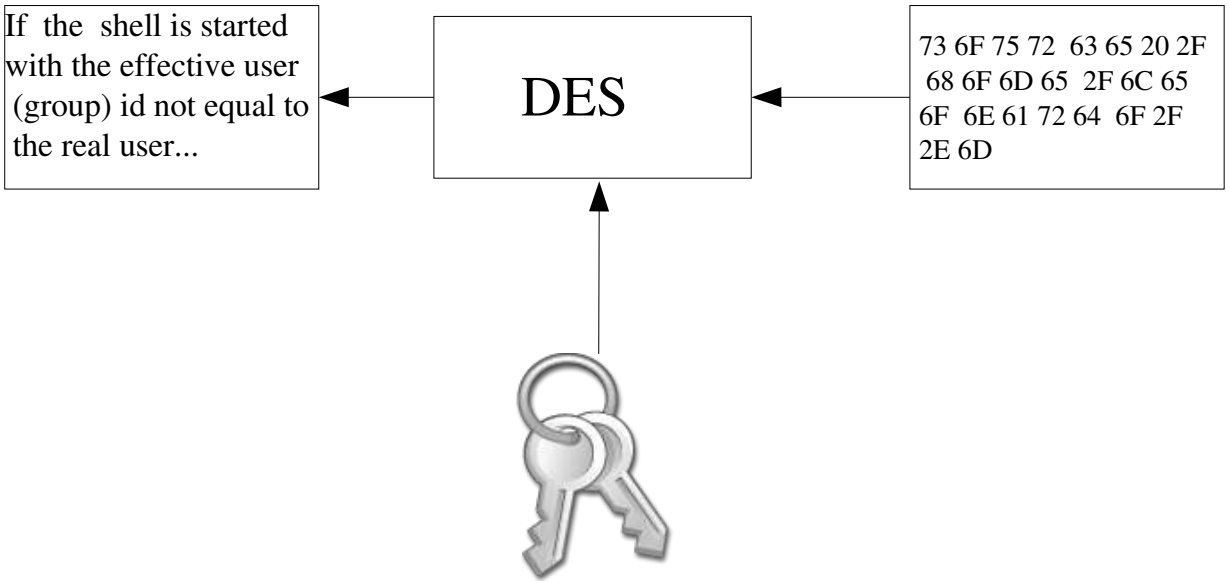
Chiave simmetrica

- unica chiave
- la chiave va concordata tra mittente e destinatario prima dello scambio dei dati
- problema di trasmissione sicura della chiave

Cifratura


If the shell is started with the effective user (group) id not equal to the real user...
DES
73 6F 75 72 63 65 20 2F
68 6F 6D 65 2F 6C 65
6F 6E 61 72 64 6F 2F
2E 6D

Decifratura

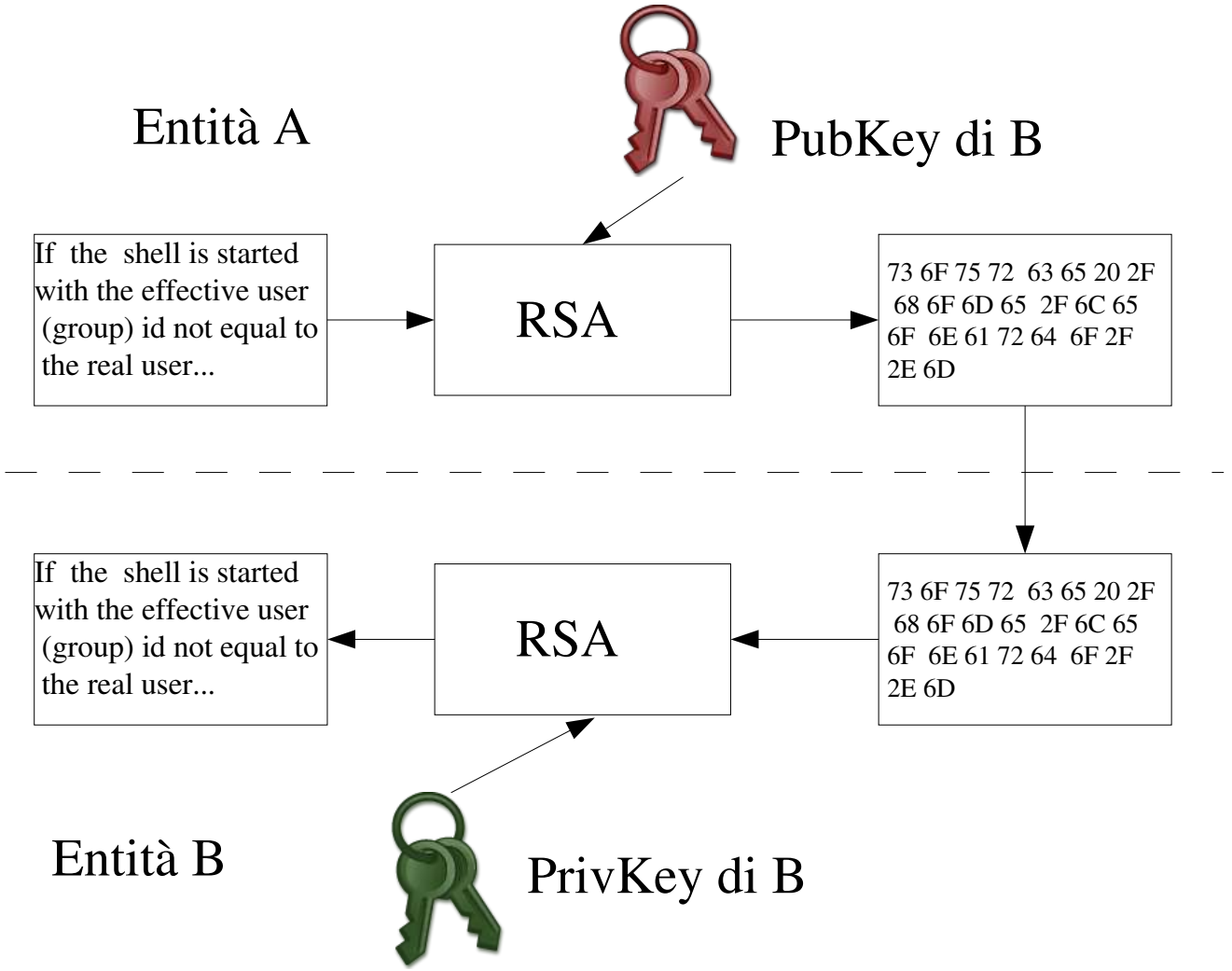


Cifratura a chiave pubblica/privata

- Ogni soggetto possiede una coppia di chiavi
  - Chiave publica
  - Chiave privata
- Ciò che viene cifrato con una chiave può essere decifrato solo con l'altra
- E' computazionalmente impossibile risalire ad una chiave privata tramite la chiave pubblica

Cifratura e Decifratura

Solo B, conoscendo la chiave PrivKey, può decifrare il documento, si ottiene:



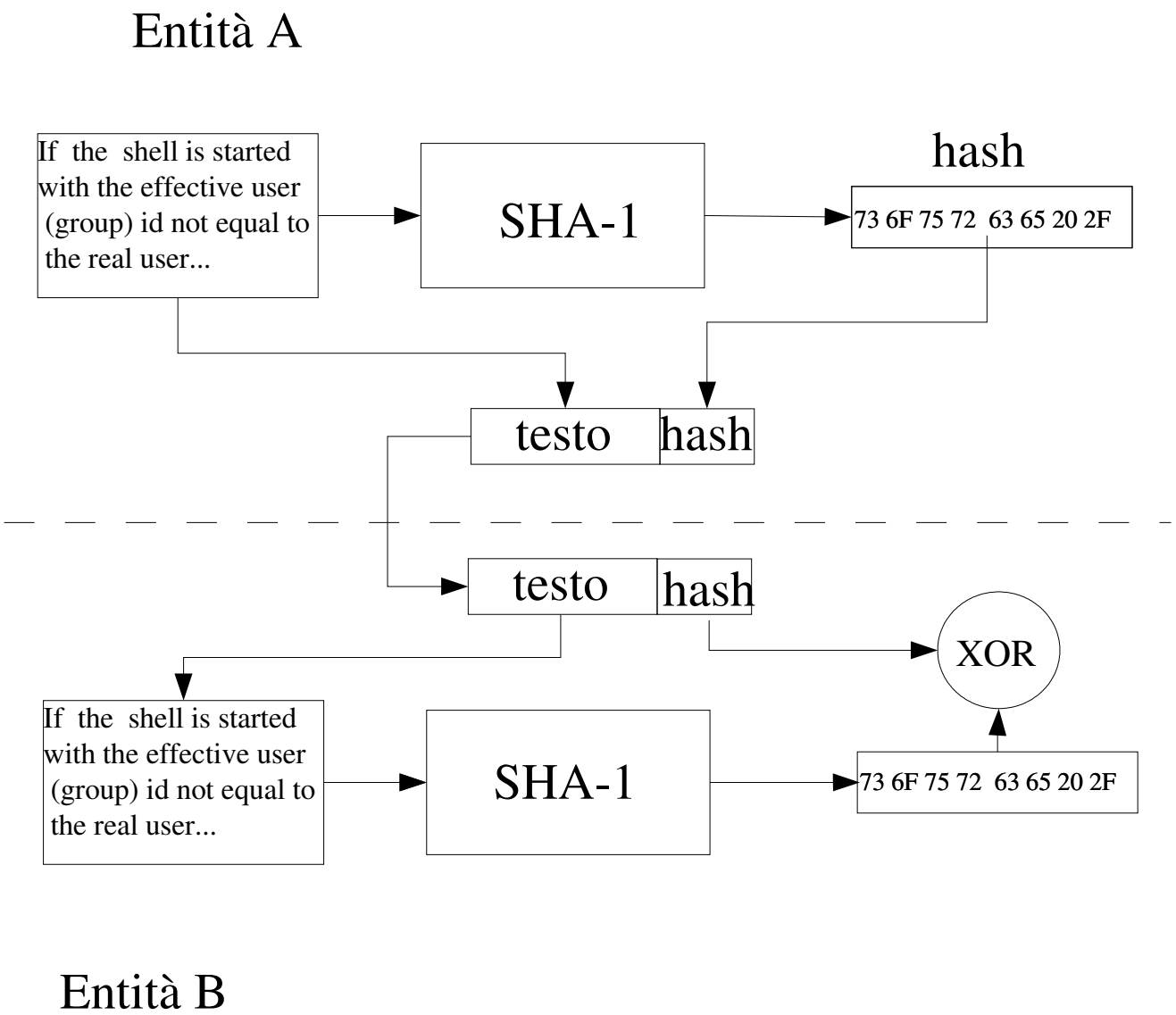
Riassumendo

- Ogni utente ha due chiavi legate in modo inscindibile da una formula matematica
  - una chiave viene resa pubblica
  - l'altra è in possesso del solo utente
- le chiavi pubbliche sono disponibili in un elenco centralizzato consultabile liberamente dagli utenti
- le coppie di chiavi pubbliche/private sono generate a cura dell'utente

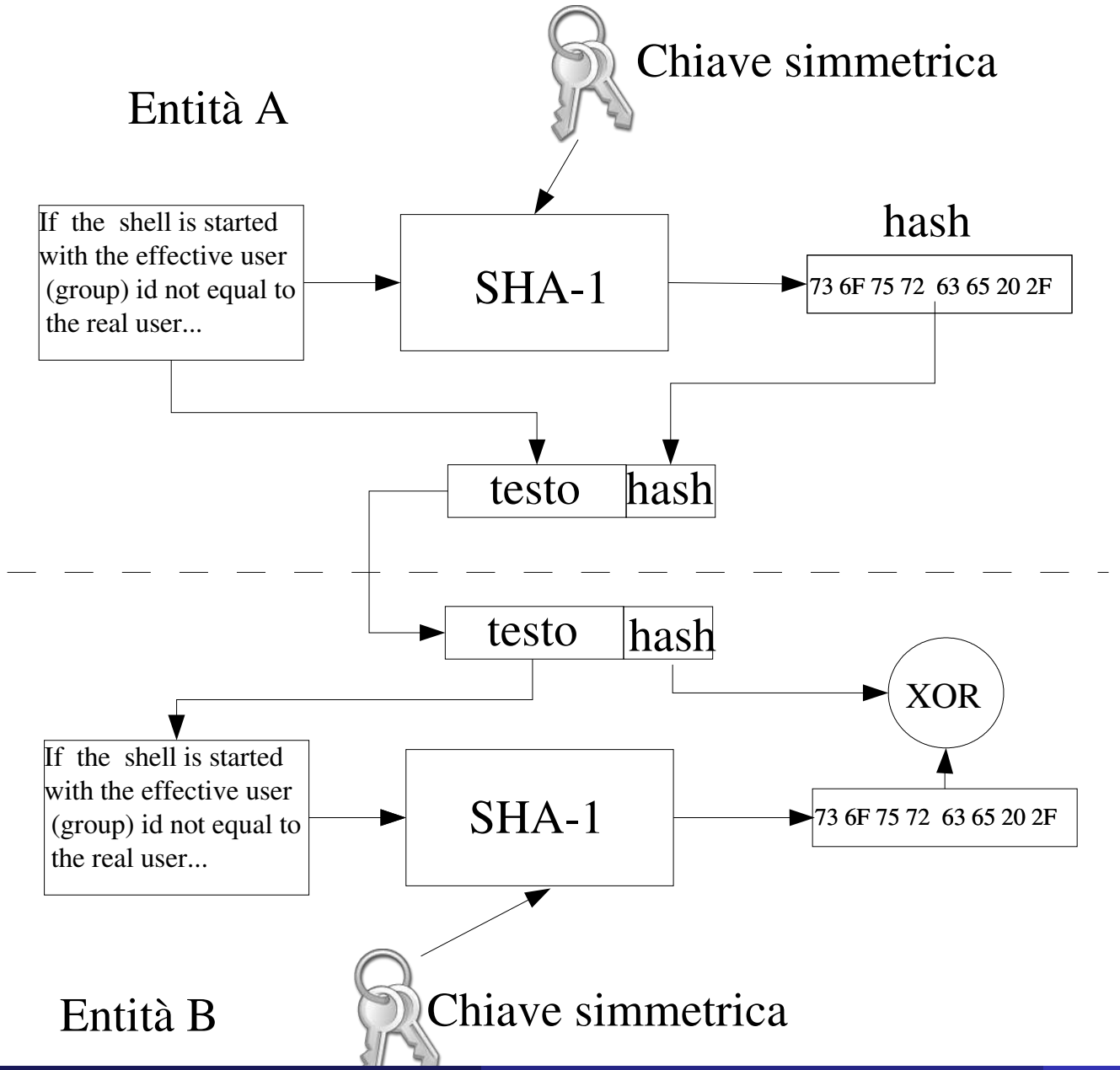
- Non è necessario concordare preventivamente una chiave di cifratura comune per scambiarsi un documento riservato
- La chiave privata di un utente è sempre segreta
- Attraverso la firma digitale si autenticano i propri messaggi in modo certo ed inequivocabile

- Funzione di hash
  - genera una impronta (digest) dei dati
  - non è reversibile (dal digest non si può ricavare il dato)

Hashing


Entità A
If the shell is started with the effective user (group) id not equal to the real user...
SHA-1
hash
73 6F 75 72 63 65 20 2F
testo
hash
testo
hash
XOR
If the shell is started with the effective user (group) id not equal to the real user...
SHA-1
73 6F 75 72 63 65 20 2F
Entità B

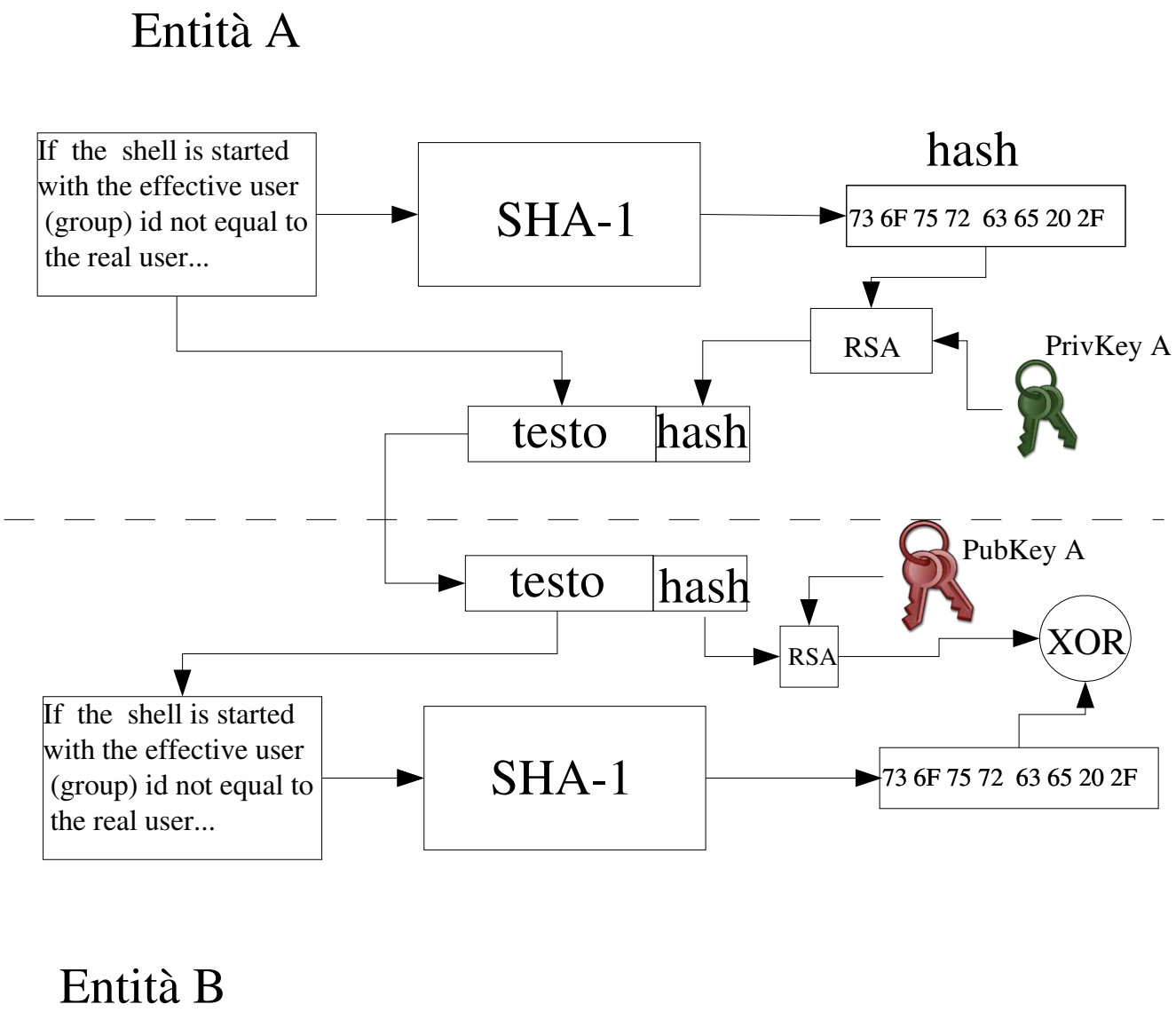
HMAC


Chiave simmetrica
Entità A
If the shell is started with the effective user (group) id not equal to the real user...
SHA-1
hash
73 6F 75 72 63 65 20 2F
testo
hash
testo
hash
XOR
If the shell is started with the effective user (group) id not equal to the real user...
SHA-1
73 6F 75 72 63 65 20 2F
Entità B
Chiave simmetrica

Firma digitale

- Le chiavi pubblica e privata sono invertibili
- Si può cifrare con la privata e decifrare con la pubblica
- Chi decifra è anche sicuro dell'identità del mittente

Firma digitale



Ente certificatrice

- Un ente che garantisce l'associazione tra chiave pubblica e persona fisica.
- L'ente possiede una sua coppia di chiavi pubblica/privata.
- Gli utenti conoscono l'ente (e la sua chiave pubblica) e si fidano delle certificazioni che rilascia.
- Alcuni enti di certificazione: Poste Italiane, Verisign ecc. . . .

Certificazione

- Come avviene la certificazione:
  - L'utente A genera una coppia di chiavi pubblica/privata.
  - L'utente A invia all'ente la propria chiave pubblica, un documento.
  - L'ente restituisce la chiave pubblica dell'utente A firmata con la priopria chiave privata. Il contenitore in cui si sposta la chiave è un certificato.
  - Questa procedura si fa una sola volta, alla creazione della chiave.

Certificazione

- Quando un secondo utente B deve parlare con A, riceve il suo certificato,
- verifica la firma digitale dell'ente certificatrice,
- a quel punto è sicuro che l'utente A è davvero chi dichiara di essere, perchè l'ente certificatrice è testimone per lui.

Certificato digitale

Contiene:

- Dati identificativi dell'entità che fa da garante
- un serial number che identifica univocamente il certificato
- periodo di validità (da/a)
- dati identificativi del soggetto a cui è rilasciato (utente o dispositivo)
- la chiave pubblica del soggetto
- la firma digitale dell'ente che ha emesso il certificato

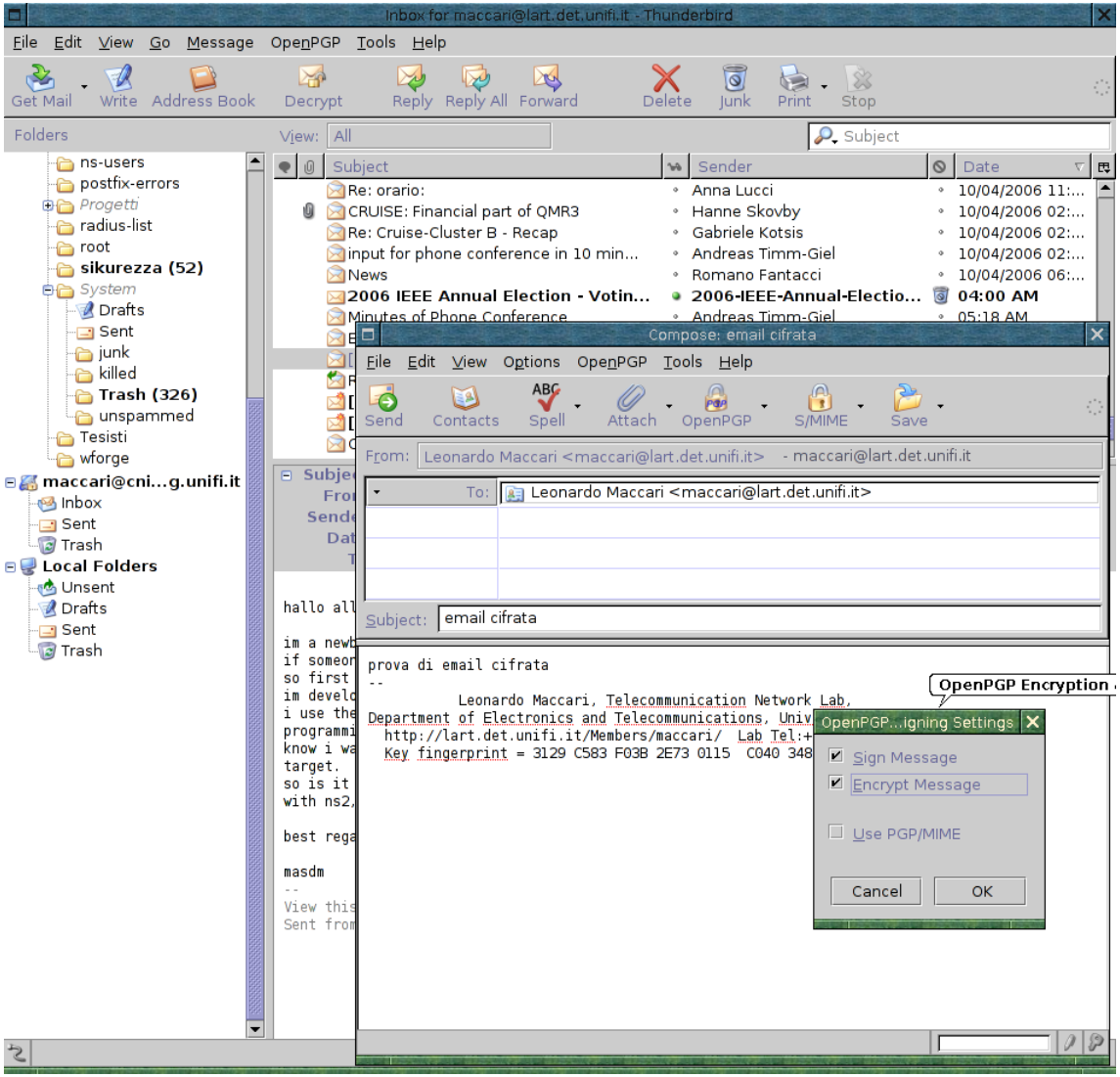
Certificato digitale

Come si usa la firma digitale

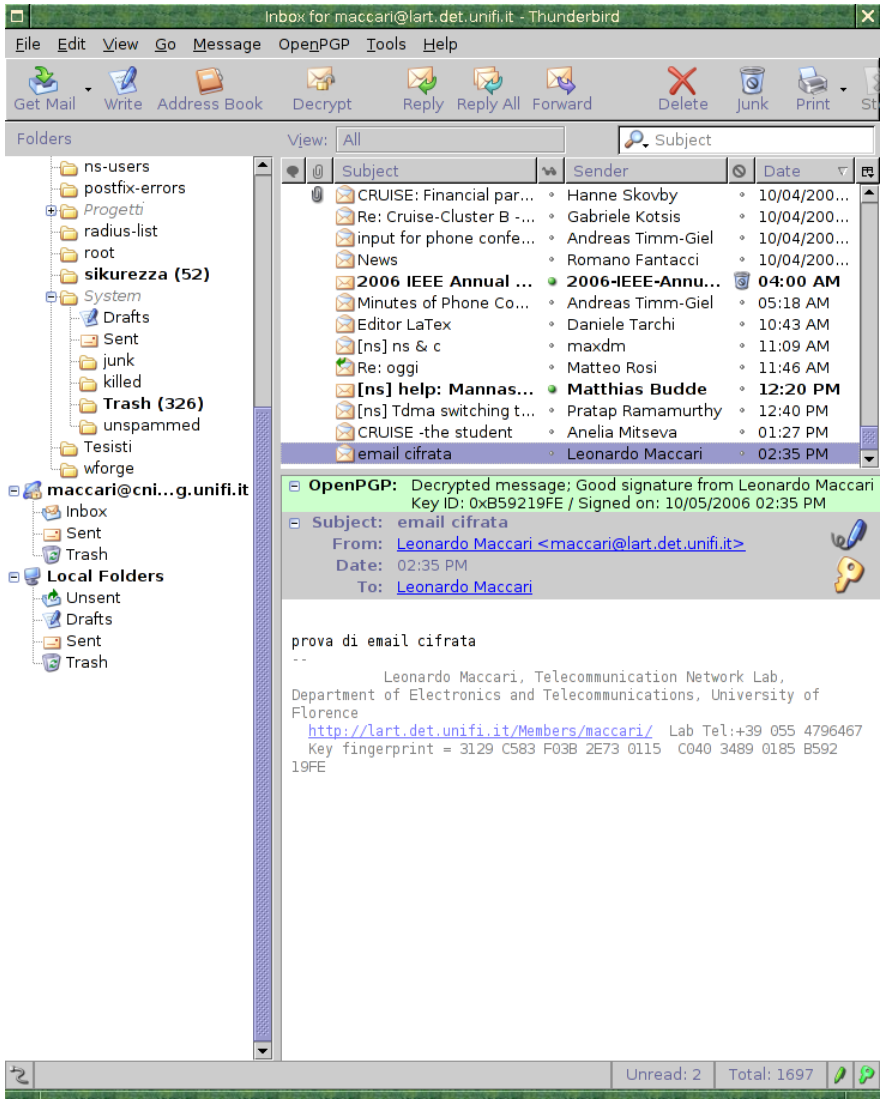
Può essere utilizzata per:

- Scambiarsi informazioni con assoluta riservatezza
- Essere sicuri dell'integrità e dell'autenticazione delle informazioni
- Ottenere la non ripudiabilità

Esempio: thunderbird con GPG



Esempio: thunderbird con GPG



Protocolli sicuri

I concetti visti per la posta elettronica possono essere trasportati anche nel WEB. Esistono protocolli sicuri che si basano sull'utilizzo di chiave pubblica e privata, se il protocollo di base del web è HTTP, la sua versione sicura si chiama HTTPS. Come funziona:

- quando vi collegate ad un sito con HTTPS il sito vi invia la sua chiave pubblica, con cui dovrete cifrare i dati successivi.
- il vostro browser vi chiede se volete o meno accettare la connessione, cioè se vi fidate della chiave che vi viene inviata.
- anche il vostro browser invia una chiave al server HTTPS. A quel punto la comunicazione può avvenire in maniera cifrata.

Protocolli sicuri

La descrizione appena fatta è una semplificazione del protocollo reale, ma basta per capire alcuni concetti fondamentali legati ai protocolli sicuri:

- Dovete essere a conoscenza della chiave pubblica del server.
- Come abbiamo detto in precedenza ogni parte della pagina viene caricata attraverso una connessione diversa, dovete essere sicuri di quali parti della comuniczione sono cifrati e quali non lo sono.

Protocolli sicuri

Un problema tipico: di chi è la chiave?

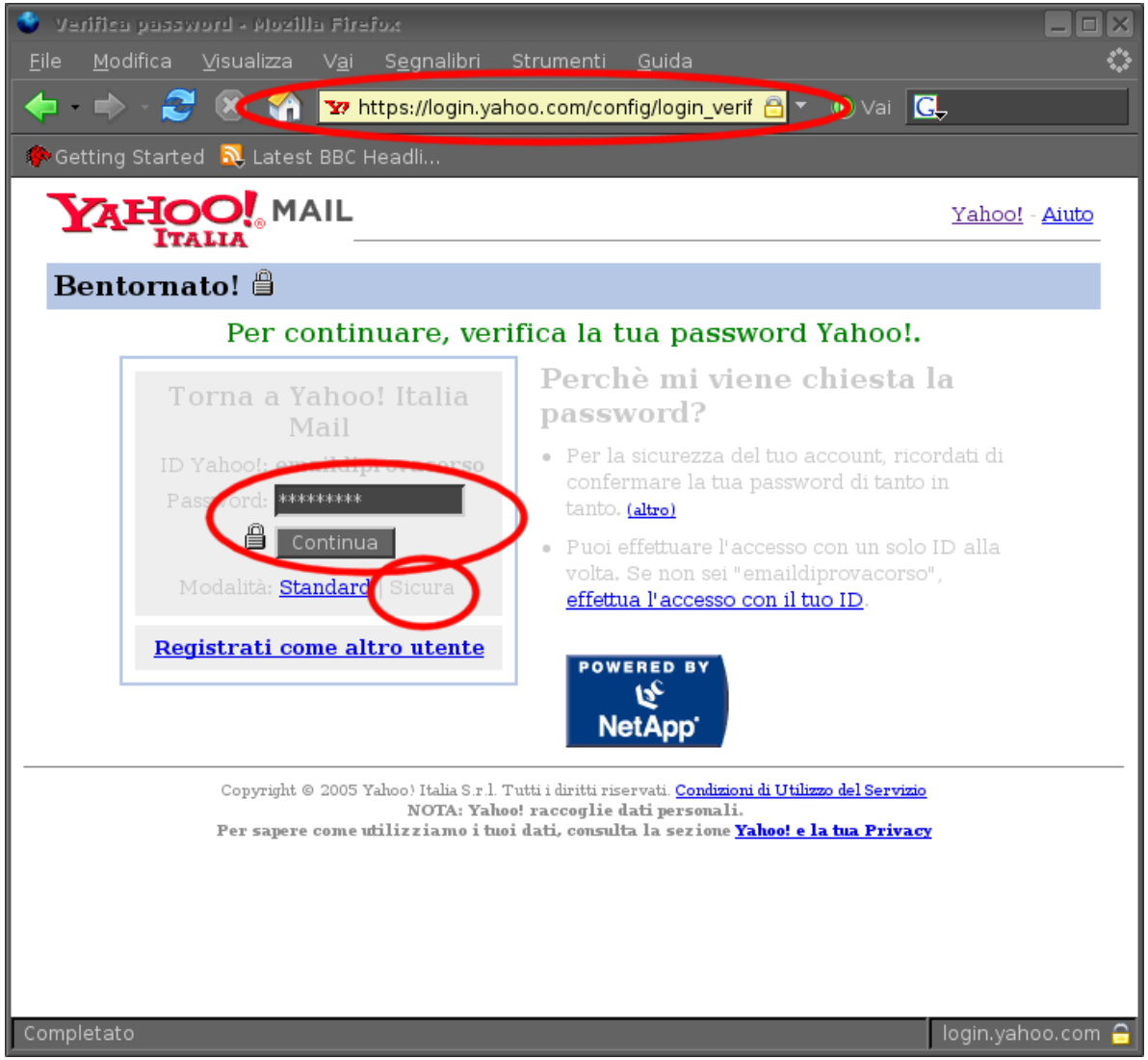
- Quando vi viene chiesto *vuoi accettare il certificato?* dal vostro browser, vi viene esplicitamente richiesto di verificare che il sito su cui state navigando è effettivamente il proprietario della chiave pubblica che vi propone.
- Il rischio che si corre è che la comunicazione sia effettivamente cifrata, ma che il destinatario non sia chi dice di essere!
- Senza entrare nei dettagli, esistono vari modi di associare un sito ad una chiave, in ogni caso, una volta accettata la chiave la prima volta, questa non dovrebbe cambiare se non per motivi validi.

Protocolli sicuri

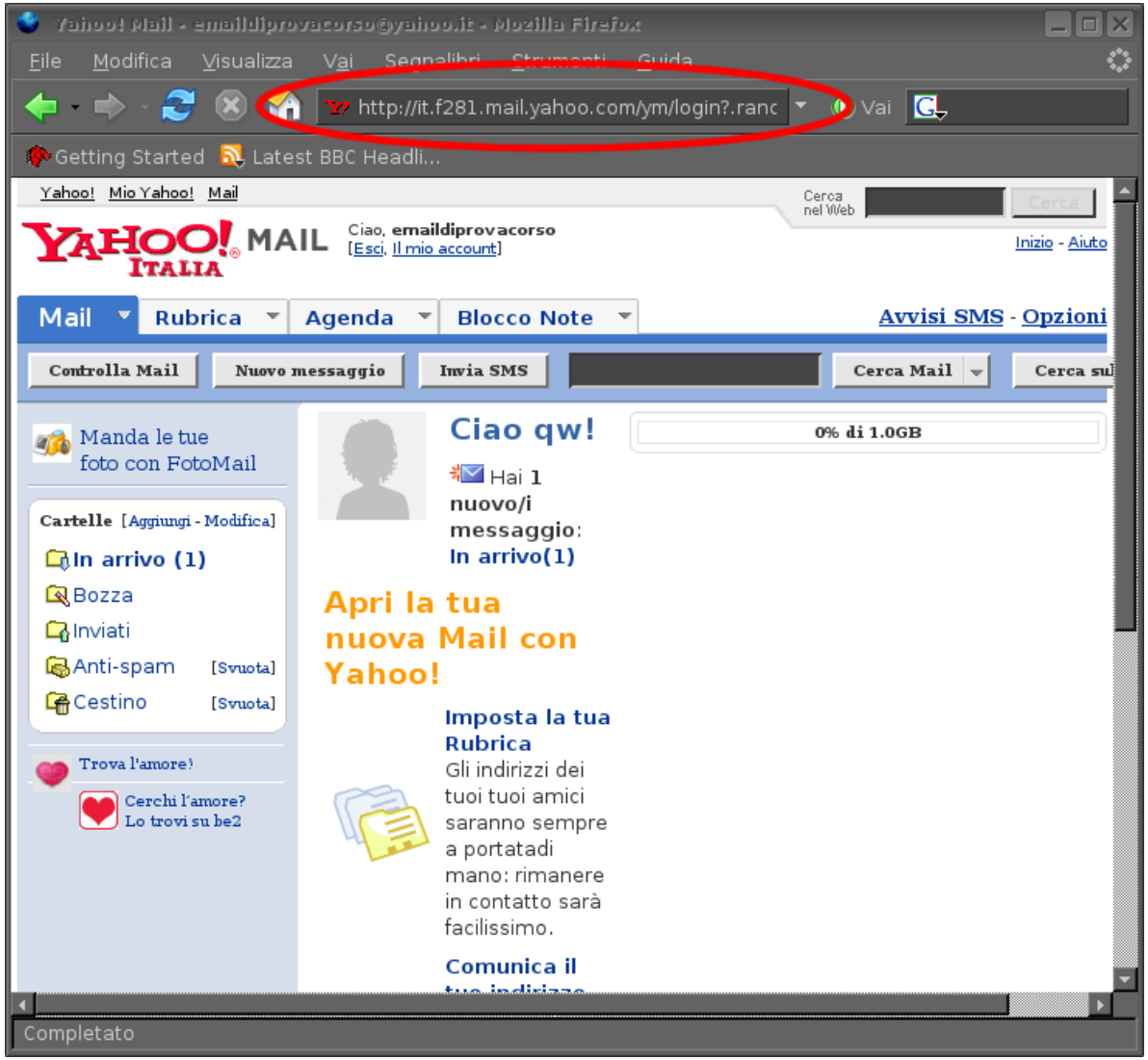
Un altro problema: che cosa esattamente è cifrato?

- Alle volte, per non rendere la comunicazione troppo pesante (la cifratura può essere un'operazione costosa) si cifrano solo alcune parti della pagina e non altre
- Alcuni siti cifrano solo alcune pagine del sito
- Il browser vi dovrebbe avvertire di quando questo avviene

SSL


Verifica password - Mozilla Firefox
File Modifica Visualizza Vai Segnalibri Strumenti Guida
https://login.yahoo.com/config/login_verif
Vai
Getting Started
Latest BBC Headli...
YAHOO! ITALIA MAIL
Yahoo! - Aiuto
Bentornato!
Per continuare, verifica la tua password Yahoo!.
Torna a Yahoo! Italia Mail
ID Yahoo!:
Password:
Continua
Modalità: Standard | Sicura
Registrati come altro utente
Perchè mi viene chiesta la password?
Per la sicurezza del tuo account, ricordati di confermare la tua password di tanto in tanto. (altro)
Puoi effettuare l'accesso con un solo ID alla volta. Se non sei "emaildiprovacorso", effettua l'accesso con il tuo ID.
POWERED BY NetApp
Copyright © 2005 Yahoo! Italia S.r.l. Tutti i diritti riservati. Condizioni di Utilizzo del Servizio
NOTA: Yahoo! raccoglie dati personali.
Per sapere come utilizziamo i tuoi dati, consulta la sezione Yahoo! e la tua Privacy
Completato
login.yahoo.com

SSL


Yahoo! Mail - emaildiprovacorso@yahoo.it - Mozilla Firefox
File Modifica Visualizza Vai Segnalibri Strumenti Guida
http://it.f281.mail.yahoo.com/ym/login?.ranc
Vai
Getting Started
Latest BBC Headli...
Yahoo! Mio Yahoo! Mail
Cerca nel Web
Cerca
YAHOO! ITALIA MAIL
Ciao, emaildiprovacorso
[Esci, Il mio account]
Inizio - Aiuto
Mail
Rubrica
Agenda
Blocco Note
Avvisi SMS - Opzioni
Controlla Mail
Nuovo messaggio
Invia SMS
Cerca Mail
Manda le tue foto con FotoMail
Cartelle [Aggiungi - Modifica]
In arrivo (1)
Bozza
Inviati
Anti-spam [Svuota]
Cestino [Svuota]
Trova l'amore!
Cerchi l'amore? Lo trovi su be2
Ciao qw!
0% di 1.0GB
Hai 1 nuovo/i messaggio:
In arrivo(1)
Apri la tua nuova Mail con Yahoo!
Imposta la tua Rubrica
Gli indirizzi dei tuoi tuoi amici saranno sempre a portatadi mano: rimanere in contatto sarà facilissimo.
Comunica il
Completato

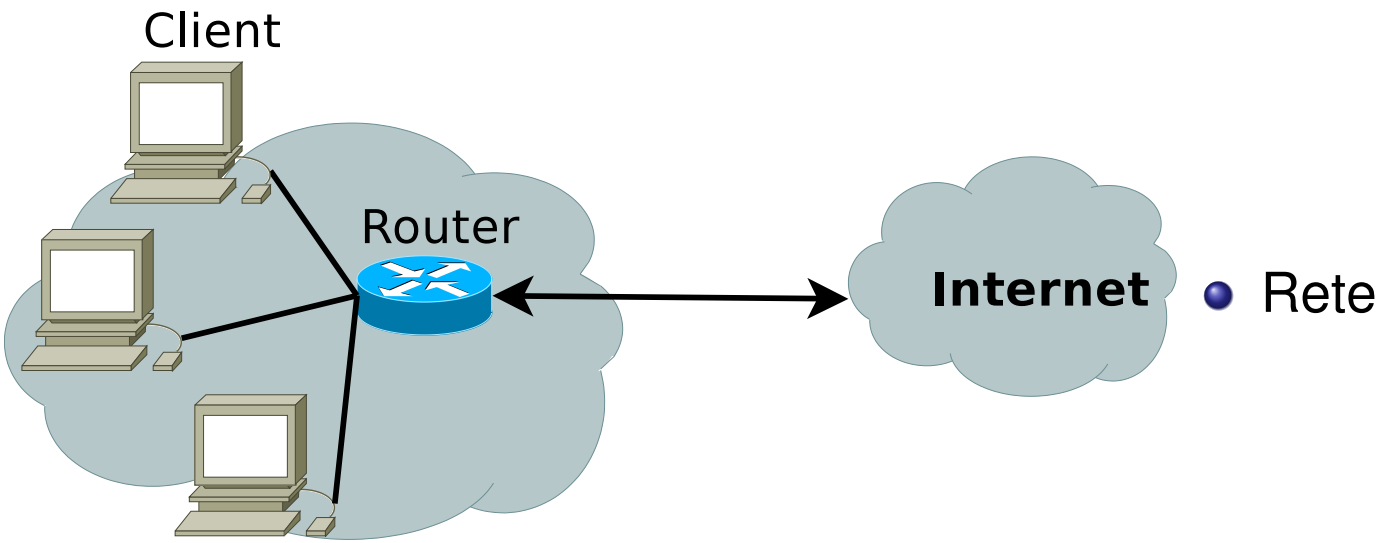
Protocolli sicuri

- In questo caso fate passare la vostra password su un protocollo sicuro
- ma il resto della comunicazione passa del tutto in chiaro
- Yahoo! per risparmiare risorse ha stabilito che il contenuto delle vostre email non è un un'informazione riservata.

Strumenti di amministrazione

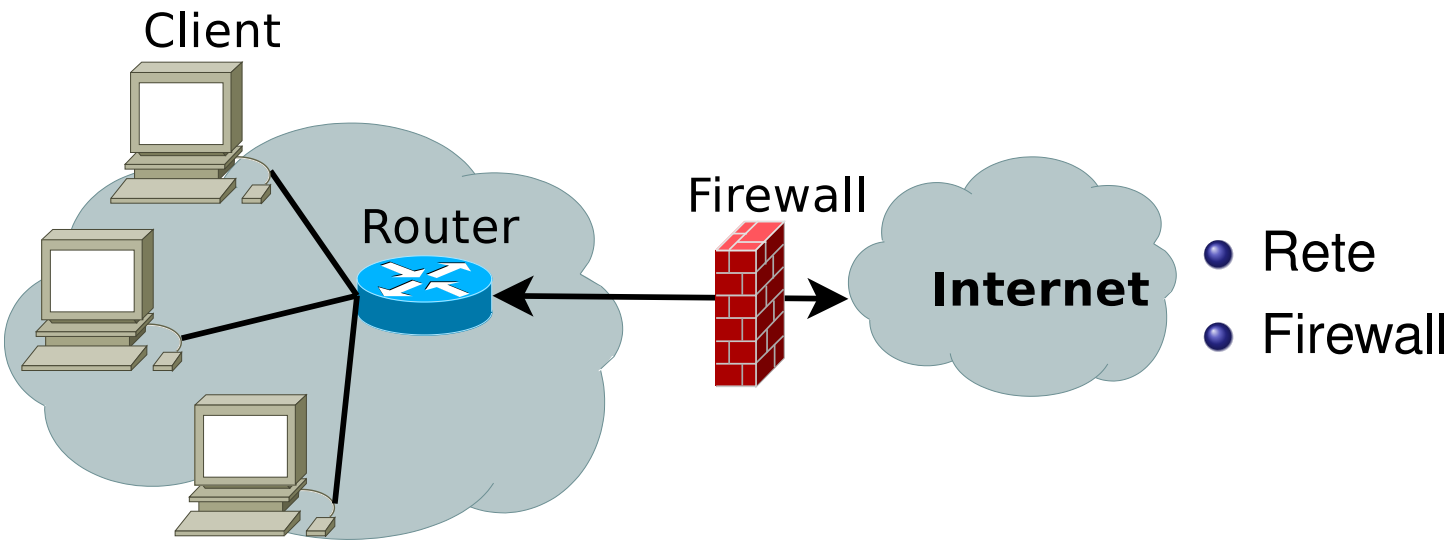
L'amministratore della rete può decidere di utilizzare alcuni strumenti per rendere la rete più sicura, introduciamo alcuni di questi strumenti per avere un glossario comune.

Firewall/IDS/Antivirus/Antispyware



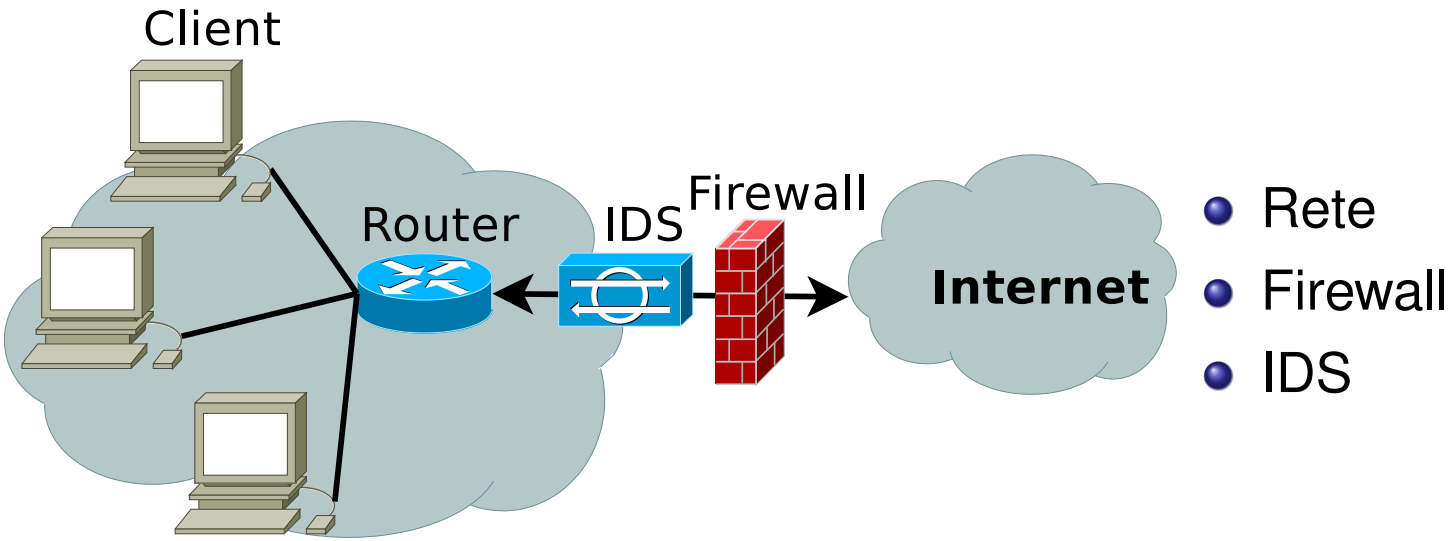
- Rete

Firewall/IDS/Antivirus/Antispyware



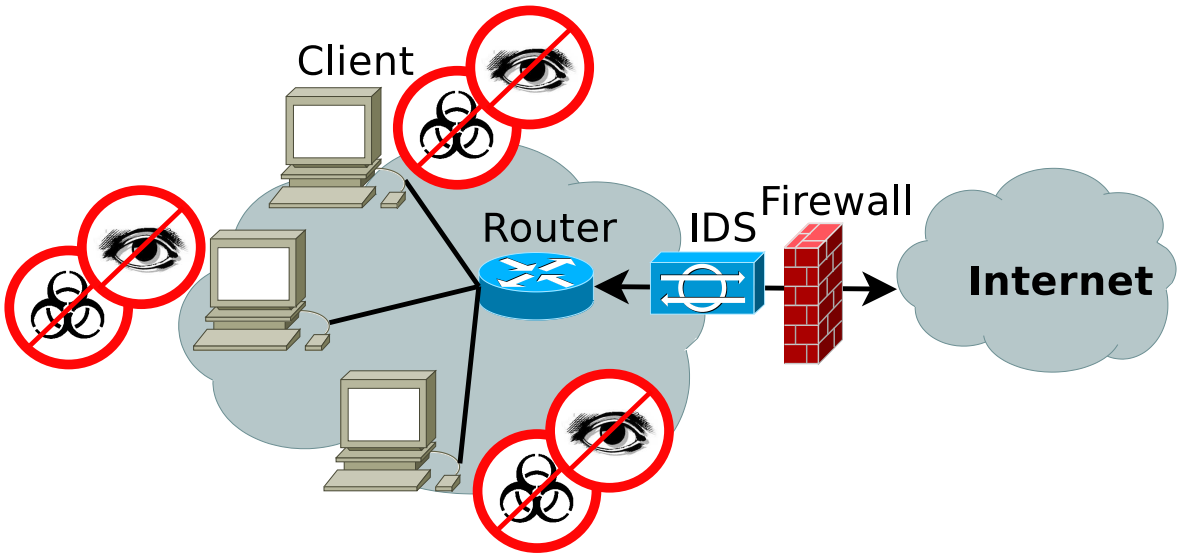
- Rete
- Firewall

Firewall/IDS/Antivirus/Antispyware



- Rete
- Firewall
- IDS

Firewall/IDS/Antivirus/Antispyware



- Rete
- Firewall
- IDS
- Antivirus/ Antispyware

Strumenti di difesa

- Firewall: serve a filtrare i pachetti in ingresso, in modo da evitare connessioni non desiderate. Ad esempio se utilizzate le condivisioni con netbios, non volete che queste siano disponibili ache fuori dalla vostra rete privata.
- IDS (intrusion detection system): ascoltano il traffico e cercano di capire se stanno avvenendo delle intrusioni o dei tentativi di attacco.
- Antivirus/Antispyware: analizzano lo stato dei singoli computer cercando tracce di virus/spiware. Contengono un elenco di tutti i malware esistenti e controllano file per file che non siano presenti nel disco fisso o in memoria. Vanno tenuti costantemente aggiornati.

Digital Rights Management

Con DRM si intendono i sistemi tecnologici mediante i quali i titolari di diritti d'autore possono esercitare ed amministrare tali diritti nell'ambiente digitale, grazie alla possibilità di rendere protetti, identificabili e tracciabili tutti gli usi in rete di materiali adeguatamente "marchiati".

- Ebook di Adobe o di Microsoft (vi impediscono di copiare il file, di copiare il contenuto ecc. . .)
- Mp3 scaricati da molti siti, iTunes (vi impediscono di spostare i file, copiarli in apparati non compatibili ecc. . .).

Digital Rights Management

I sistemi DRM servono, per definizione, ad evitare che un utente possa compiere certe azioni sul proprio computer. I problemi di sicurezza che sorgono sono numerosi: se il distributore del software non si fida di noi, possiamo noi fidarci di lui?

- come si può essere sicuri che il software fa solo quello che dice di fare?
- non fidarsi dei distributori di software è paranoico?

Qualche esempio:

Ottobre 2005: un ricercatore scopre che alcuni CD musicali Sony se ascoltati su un computer con sistema operativo windows installano nel sistema dei programmi senza chiedere il permesso:

- il programma si installa automaticamente senza chiedere il permesso (sembra che si sia installato in almeno 500.000 computer)
- il programma impedisce di copiare il contenuto del CD (cosa peraltro lecita, se per uso personale)
- il programma non può essere disinstallato
- il programma contiene codice (un player mp3) di cui Sony non possiede i diritti, quindi il programma stesso rompe le leggi sul copyright.
- dopo numerose proteste (e principi di azioni legali) la sony ha rilasciato un *uninstaller*. É stato dimostrato che dopo aver disinstallato il software, il sistema operativo presenta una grave falla di sicurezza, che può essere sfruttata da altri attaccanti.
- Il programma viene riconosciuto come un virus da Symantec e McAfee

Ancora esempi:

- Nel caso di Sony, il comportamento dell'azienda era palesemente scorretto, in altri casi può semplicemente accadere che l'azienda stessa sia vittima di un attacco che si propaga ai suoi utenti.
- Un comunicato stampa del 2000, ancora presente sul sito Microsoft spiega che qualcuno è riuscito a penetrare nella rete interna microsoft ed ha avuto accesso al codice dei programmi che erano in produzione.
- Il comunicato terminava con un laconico "*There's no evidence that any source code has been modified or corrupted*" (non abbiamo prove che il codice sia stato modificato o corrotto)
- . . . normalmente gli attaccanti cancellano le prove. . .
- Come si può essere sicuri che un programma che utilizziamo non compia azioni non previste?

Programmi con licenze libere/open source

Si possono utilizzare programmi con licenze libere:

- permettono di utilizzare il programma
- permettono di vedere, modificare, ridistribuire il codice sorgente

Sicurezza

- + si sa esattamente cosa fa il programma
- + si può migliorare/patchare, non bisogna aspettare le patch
- + il codice viene riutilizzato (anche dagli altri), quindi migliora
- - raramente esiste un team di sviluppatori pagati che progetta e implementa il software

Buone pratiche

Per chiudere ci soffermiamo su due temi che sono a stretto contatto con gli utenti finali, le password e il social engeneering.

La password

Quando decidete la password per i vostri account questa viene salvata in un un file in modo cifrato. Se la cifratura è robusta, l'unico modo per indovinare la vostra password è provarle tutte.

- un password cracker su un computer comune riesce a generare circa 7000 password per secondo.
- il dizionario Garzanti contiene circa 200.000 voci, se la vostra password è una parola di dizionario, ci vuole meno di mezzo minuto per indovinarla.
- Subito dopo aver terminato il dizionario senza successo il si prova a craccare altre password comuni del tipo *parola+numero*. Una password come *paola76* ha una vita di una 50ina di minuti.
- L'alfabeto possiede 25 lettere a cui si aggiungono 10 simboli di numeri. Per generare tutte le password lunghe 8 caratteri mescolando lettere e numeri ci vogliono 85 giorni, che non sono un'eternità.

La password

Riassumendo:

- le password devono essere piu' lunghe di 8 caratteri
- non devono contenere parole di senso compiuto
- devono essere una mescolanza di lettere maiuscole/minuscole, di numeri e di simboli di punteggiatura
- come ci si ricorda di una password come: NmDcDnV_1300 ?
- si genera come una filastrocca: Nel mezzo del cammin di nostra vita
- si possono scrivere le password? meglio di no. Se proprio necessario si scrivono in un posto non ricollegabile all'ambiente di lavoro.

Il social engeneering: la porta è sprangata, la finestra è aperta

Il social engeneering si basa su due assiomi:

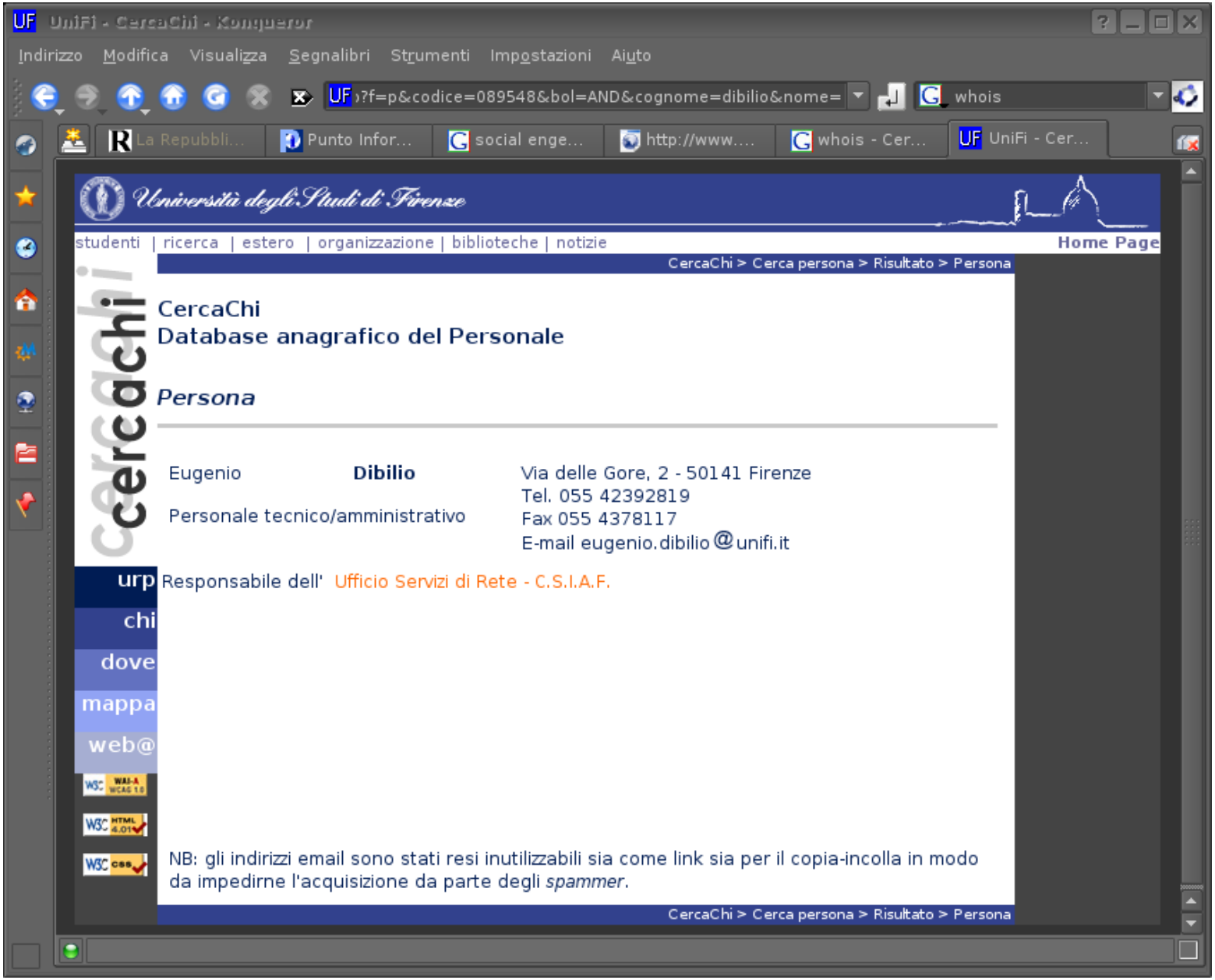
- Gli esseri umani tendono ad essere fiduciosi nel prossimo
- I computer sono migliori degli uomini nell'immagazzinare informazioni, gli uomini sono più disponibili a fornirle

Quello che si vuole ottenere sono informazioni private senza utilizzare mezzi tecnici, ma solo eludendo i rapporti umani

```
leonardociclope:~$ whois unifi.it
domain:       unifi.it
org:          Universita' degli Studi di Firenze
descr:        c/o CSIAF Centro Servizi Informatici
descr:        dell'Ateneo di Firenze
descr:        via delle Gore 2
descr:        I-50141 Firenze
descr:        Italian 2nd level domain
nserver:      150.217.1.32 dns.unifi.it
nserver:      150.217.1.135 cesit2.student.unifi.it
nserver:      dns3.nic.it
remarks:      fully managed
created:      before 19960129
expire:       20070129

person:       Cristina Mugnai

person:       Eugenio Dibilio
```


UniFi - CercaChi - Konqueror
Indirizzo Modifica Visualizza Segnalibri Strumenti Impostazioni Aiuto
whois
Università degli Studi di Firenze
studenti | ricerca | estero | organizzazione | biblioteche | notizie
Home Page
CercaChi > Cerca persona > Risultato > Persona
CercaChi
Database anagrafico del Personale
Persona
Eugenio Dibilio
Personale tecnico/amministrativo
Via delle Gore, 2 - 50141 Firenze
Tel. 055 42392819
Fax 055 4378117
E-mail eugenio.dibilio @ unifi.it
urp
chi
dove
mappa
web@
Responsabile dell' Ufficio Servizi di Rete - C.S.I.A.F.
NB: gli indirizzi email sono stati resi inutilizzabili sia come link sia per il copia-incolla in modo da impedirne l'acquisizione da parte degli spammer.
CercaChi > Cerca persona > Risultato > Persona

Da una rcerca banale su internet, il signor Dibilio si occupa di:

- amministrazione di reti con più di 1000/2000 clienti
- routing OSPF
- sistemi VOIP

É abbastanza per mandare un'email. Dall'email posso ricavare diverse informazioni:

- quali il server di posta che utilizza
- il client di posta
- magari l'IP della sua postazione
- se utilizza antispam (c'e' negli header?)
- usa ASCII o HTML?
- eventuali signature

A questo punto siete pronti per impersonare il signor Dibilio!

Si sceglie una segretaria di un dipartimento, ci si parla un paio di volte per capire che tipo è, si scrive una bella email alle 8 di sera con firma del signor Dibilio con il seguente contenuto:

```
All'att.ne di NOME COGNOME,
Abbiamo rilevato una quantità di traffico anomalo proveniente dalla sua
postazione di lavoro. C'e' il sospetto che nonostante il continuo e
metodico aggiornamento degli antivirus da parte del personale tecnico, la
sua macchina sia stata infettata da un nuovo virus sconosciuto, o per
negligenza si siano installati programmi illeciti.
La preghiamo quindi di collegarsi al seguente sito www.nomesito.com dove
scaricare un apposito programma per ripulire la sua postazione.

saluti,
Eugenio Dibilio.

PS domani non sarò in ufficio, per qualsiasi chiarimento la prego di
attendere un paio di giorni, nel frattempo applichi l'aggiornamento
che le ho indicato.
```

Conclusioni

I modi per utilizzare il social engeneering sono limitati solo dalla fantasia e dalla bravura dell'attaccante. É inutile sottolineare che:

- Per evitare di rendere la vostra rete vulnerabile contro questo tipo di attacchi non tecnici, è necessaria una formazione specifica del personale.
- Art. 494 codice penale:
  Chiunque al fine di procurare a sé o ad altri un vantaggio o di recare ad altri un danno, induce taluno in errore, sostituendo illegittimamente la propria all'altrui persona, o attribuendo a sé o ad altri un falso nome,. . . è punito se il fatto non costituisce un altro delitto contro la fede pubblica, con la reclusione fino a un anno