

SICUREZZA IN RETE

panoramica sugli strumenti

A cura di:

Ing. Michele Mordenti

Forlì, 28 Marzo 2007



Associazione Culturale
FoLUG
Forlì Linux User Group

SOMMARIO

- Presentazione del FoLUG
- Software libero
- Password
- Firewall
- LOG/IDS
- Antivirus / Antispyware
- Parental Control

Presentazione del FoLUG

Forlì Linux User Group

- L'Associazione si propone di promuovere e diffondere la conoscenza e l'uso dei moderni strumenti telematici ed informatici, con particolare attenzione al "*software libero*"

<http://www.folug.org>

Software Libero

- 0) Libertà di utilizzo del software per qualsiasi scopo lecito;
- 1) Libertà di modificare il programma;
- 2) Libertà di distribuire copie, gratis o dietro pagamento;
- 3) Libertà di distribuire versioni modificate.

Hacker

Riabilitare la parola Hacker

- Hacker:

dall'inglese *To hack*, smontare - fare a pezzi.

Persona amante della tecnologia, di fatto l'ha creata:

Internet, GNU/Linux
modello etico innovativo

- Cracker:

chi penetra e rompe sistemi altrui.

Hacking / Cracking

Riabilitare la parola Hacker

- Hacking:
Compiere un hack, modificare un oggetto per farlo funzionare in un modo non previsto dal consueto senza infrangere alcuna legge
Esempio: installare un software diverso su un dispositivo cablato, GNU/Linux over Microsoft XBOX
- Cracking:
Compiere azioni illecite su un sistema su del quale non si dispongono i necessari diritti

Copyright ©

Il software è composto da:

- Codice sorgente
- Codice macchina (per linguaggi compilati)
- Licenza d'uso

Troppo spesso ci si dimentica dell'ultimo punto!

Rispetto delle leggi come valore educativo da trasmettere agli alunni

Il software libero nella scuola incentiva la diffusione della cultura e il rispetto delle leggi sul copyright (nessun incentivo al software “pirata” a casa)

Sicurezza del FLOSS

FLOSS: *Free/Libre Open Source Software*

- Software aperto:

stabilità, sicurezza e controllo del programma

- Software proprietario:

non sappiamo nulla su cosa faccia il programma, il calcolatore è in mani altrui!

Backdoor, Spyware & Virus

La Sicurezza non è un prodotto

- La sicurezza è un processo, un insieme di azioni, regole e comportamenti.
- La sicurezza non è un prodotto in vendita negli scaffali dei negozi.
- La sicurezza è inversamente proporzionale alla comodità di accesso al calcolatore.

Regole dell'azienda

- E' di fondamentale importanza redarre un documento che definisca le regole di accesso, utilizzo e manutenzione del reparto IT dell'azienda.

Gestione delle password

- Cambiare frequentemente l'uso delle password (non più di tre mesi)

- Utilizzare Password robuste

Niente nomi propri, nomi di oggetti comuni (es. frutti, stagioni). Usare almeno 8 caratteri alternando caratteri e numeri.

- Ordinare le password in base alla importanza del dato da proteggere

Gestione degli utenti

- Utilizzare l'utente amministratore di sistema solo quando strettamente necessario
- Per il lavoro quotidiano creare un utente senza privilegi speciali

- Protezione della propria privacy

Cifrare elettronicamente i propri dati sensibili

Firma digitale e Posta Elettronica Certificata (PEC):

garanzia dell' integrità del documento, identificazione certa del firmatario e non ripudio del documento ai sensi di legge

- Algoritmo a chiave simmetrica
- Algoritmo a chiave asimmetrica
- Concetto di HASH

Software applicativo:

<http://www.gnupg.org/>



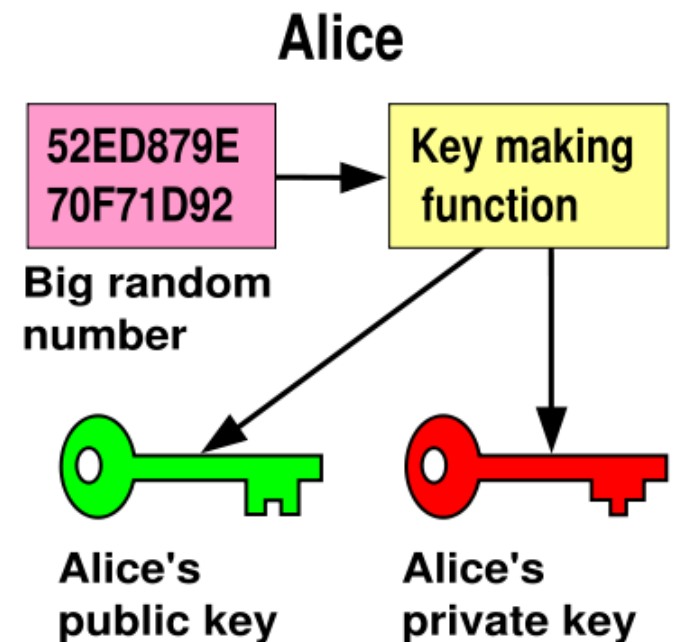
Algoritmi di Protezione

- **Algoritmo a chiave simmetrica**

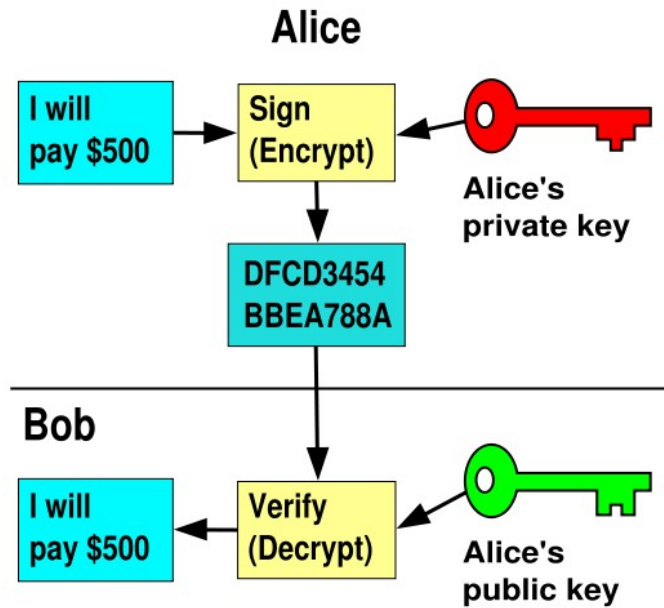
La chiave di cifratura/decifratura è la stessa per entrambi i soggetti. La chiave deve essere trasmessa attraverso un canale sicuro.

- **Algoritmo a chiave asimmetrica**

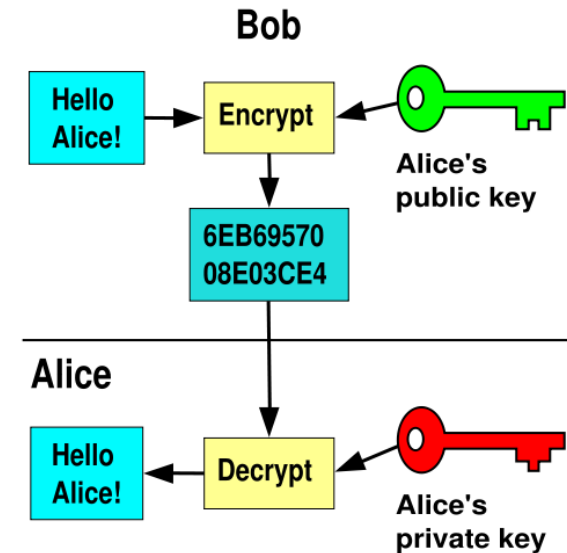
Ogni soggetto possiede due chiavi, una privata ed una pubblica. La chiave privata non verrà mai compromessa rimanendo sempre in possesso del proprietario, mentre la chiave pubblica può e deve essere fornita a tutti generalmente su server pubblici.



Chiave Asimmetrica

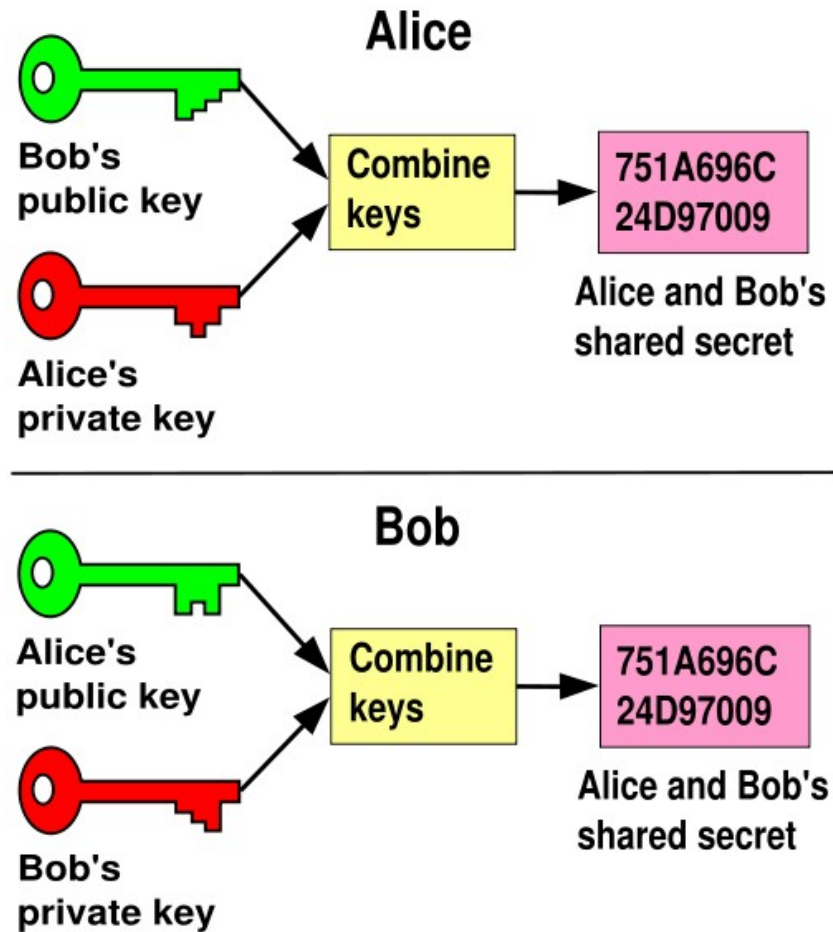


FIRMA DEL MESSAGGIO



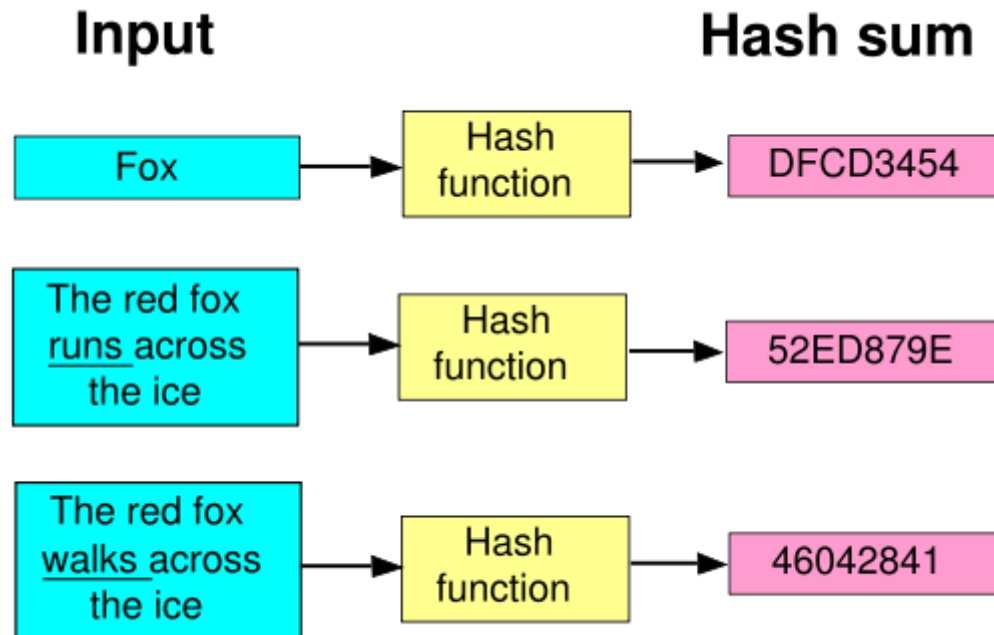
CRITTAZIONE DEL MESSAGGIO

Chiave Asimmetrica



CRITTAZIONE DEL MESSAGGIO - BIUNIVOCA

HASH



- **HASH:**
Particolari algoritmi che restituiscono un numero finito con scarsissima probabilità di collisioni
- Viene utilizzata nella firma digitale
- Utile per verificare l'esattezza dei file scaricati dalla rete (MD5)

SNIFFING / SPOOFING

- **SNIFFING:**
Tecnica di ascolto passivo della rete per intercettare dati sensibili (tipicamente password)
- **SPOOFING:**
Tecnica di attacco consistente nel cammuffare le proprie credenziali di rete (Man in the Middle)

Navigazione sicura

- Protocollo HTTPS

Inserire dati sensibili solo in pagine crittate (https://...)

Utilizzo dei cookies (protocollo http stateless)

- Posta elettronica sicura POP3S

Utilizzare protocolli crittati ove supportati dal proprio internet service provider.

Sconsigliato l'utilizzo dei prodotti Microsoft (fonte NSA)

come alternativa consigliamo:

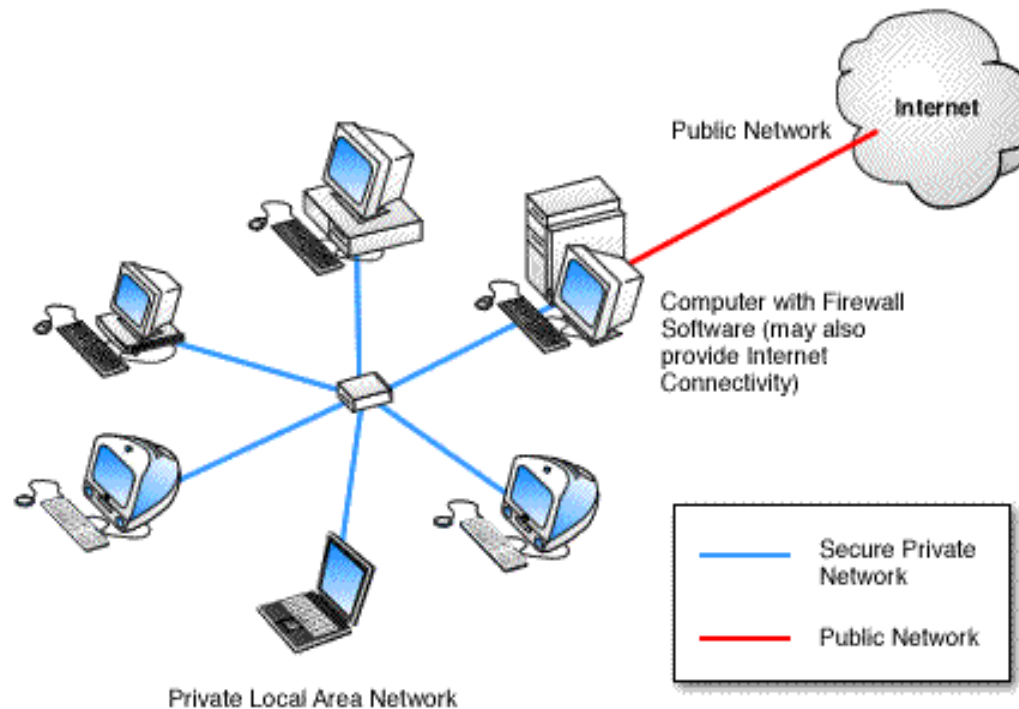
- Browser Web: Mozilla Firefox
- Posta elettronica: Mozilla Thunderbird



Firewall



- Dotare di firewall il proprio calcolatore
proteggere le porte di comunicazione esterne



Reti wireless



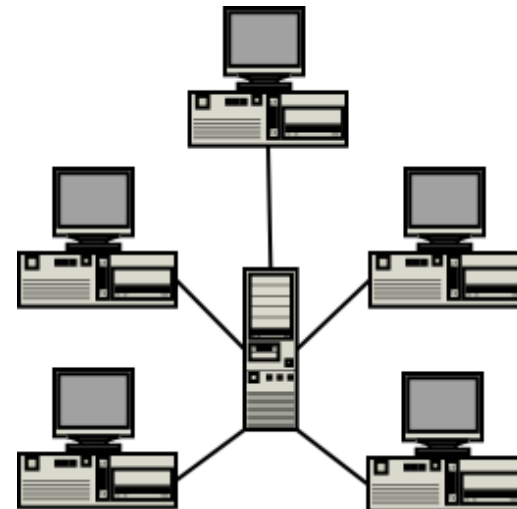
In caso di reti wireless è fondamentale proteggere l'accesso alla propria rete.

Dove non è possibile proteggere i dati fisicamente, si utilizza la crittografia.

- Evitare le reti wireless aperte
- Evitare metodi di protezione facilmente forzabili (WEP - Wireless Equivalent Protocol)
- Utilizzare la protezione WPA (Wireless Protected Access)

Disattivare servizi inutili

- Lasciare in esecuzione sul proprio elaboratore solo i servizi di rete strettamente necessari.



Antivirus



- Dotare di antivirus il proprio calcolatore
proteggere l'esecuzione di software maligno in ambiente
Windows

- Antidoto:

ClamAV (software libero)



<http://www.clamav.net/> - <http://www.clamwin.com/>

in alternativa

Antivir: gratuito per uso personale

<http://www.free-av.com/>

SPYWARE

- Gli spyware sono software che inviano segretamente informazioni sull'utente.

Forma comune di finanziamento del software freeware/shareware (non software libero)

- Antidoto: **spybot** (software libero)

<http://www.safer-networking.org/>

in alternativa

ad-aware: gratuito per uso personale

<http://www.lavasoftusa.com/software/adaware/>

MALWARE

- **TROJAN:**
software apparentemente innocuo che entra in esecuzione sulla macchina per aprire le porte a successivi attacchi. Tipicamente sfruttati da attacchi DDOS attraverso macchine zombie.
- **WORM:**
software a bassa pericolosità che degradano le prestazioni della macchina

LOG / IDS

- Controllare periodicamente i LOG di sistema per scoprire eventuali anomalie
- Intrusion Detecting System: analisi approfondita del sistema per la ricerca di **rootkits**



Parental Control

- Ad oggi non esiste un software al quale delegare l'educazione del minore
- Filtri che agevolano il controllo, ma nessuna garanzia di funzionamento al 100%
- Non esiste la sicurezza assoluta, in base alla valutazione del pericolo si procede di conseguenza

Service Proxy

Server che centralizza le richieste di accesso alla rete internet

- **Acceleratore web** (caching delle pagine)
- **Controllo lato utente:**
limita la navigazione solo su alcuni siti
- **Controllo lato amministratore:**
limita la navigazione solo a determinati utenti e tiene traccia (log) dei siti visitati

Metodi di filtraggio tramite PROXY

- **WHITELIST**

Si imposta il proxy per navigare esclusivamente su siti accreditati (A volte chiamato “*metodo della biblioteca di casa*”)

- **BLACKLIST**

Si imposta il proxy per navigare ovunque tranne che su alcuni siti noti.

Generalmente si implementano soluzioni proxy per reti di calcolatori.

Proxy OpenSource: SquidGuard e DansGuardian



Metodi di filtraggio dinamico

- Esistono software che effettuano il filtraggio dinamico

Problema della accuratezza:

mancato allarme e/o falsi positivi.

ESEMPI: NAOMI (freeware)

<http://www.radiance.m6.net/italian.html>

Notizie utili su:

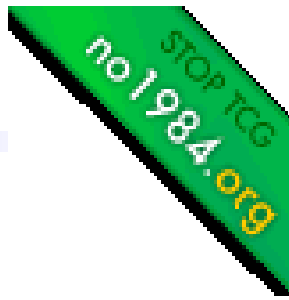
<http://www.ilfiltro.it>

<http://www.davide.it>

Buon Senso

- Ancora una volta: utilizzare sempre il buon senso e non farsi prendere o da paure ingiustificate o da falsi sensi di sicurezza
- Tenere sempre un comportamento sobrio anche in rete
- Non lasciare soli i bambini (davanti al PC, come davanti alla TV come per strada)
- Internet riflette la nostra società, nel bene e nel male. Non demonizzarne l'utilizzo

Trusted Computing



- Consorzio di produttori Hardware/Software per creare una piattaforma sicura

Sicura per chi?

- Non siete voi a decidere quali programmi far eseguire al vostro elaboratore, ma le industrie scelgono per voi
- Il PC non è più sotto il vostro controllo
- Tecnologia inutile per filtrare il contenuto delle pagine web

<http://www.no1984.org>

SICUREZZA IN RETE

...FINE

Contatti: Ing. Michele Mordenti

e-mail: michele.mordenti@gmail.com

web: <http://xoomer.virgilio.it/michele.mordenti>

FoLUG: <http://www.folug.org>

Il materiale presentato è rilasciato su licenza Creative Commons



Attribution



Share-Alike



Non-Commercial