SICUREZZA IN RETE

Versione leggera

A cura di:
M. Ivan Fabris

Progetto grafico e struttura:
Ing. Michele Mordenti

Associazione Culturale
FoLUG
Forlì Linux User Group

Release : Forlì, 2008 10 04

SOMMARIO

- Jungla Selvaggia
- Attacchi illeggittimi e “legittimi”
- Difese legittime e illegittime
- Parental Control

Jungla selvaggia

- La rete e' un territorio senza controllo ?
- E' pericolosa ?
- E quanto, rispetto al mondo “reale” ?
- Puo' essere controllata ?
- Chi lo puo', o vuole fare ? E come ?

Attacchi

I possibili attacchi al nostro computer, ai nostri dati, alla nostra privacy

- Virus, Troian
- Portscan
- Intercettazioni (sniffing)
- Furti
- Circonvenzioni, frodi, raggiri, inganni

Difese

- Antivirus (ClamAV, ClamAV per win)
- Antispyware (SpyBot per win)
- Firewall (SuSEFirewall, ZoneAlarm per win)
- Crittografia (Gnupg, Thunderbird)
- Gestione degli utenti e dei servizi offerti
- Freenet
- Accortezza

Antivirus

- Virus

  software maligno in ambiente Windows

- Antidoto:

1) ClamAV software libero

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

2) Antivir: gratuito per uso personale

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

Anti 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:
  sofware a bassa pericolosità che degradano le prestazioni della macchina

Phishing

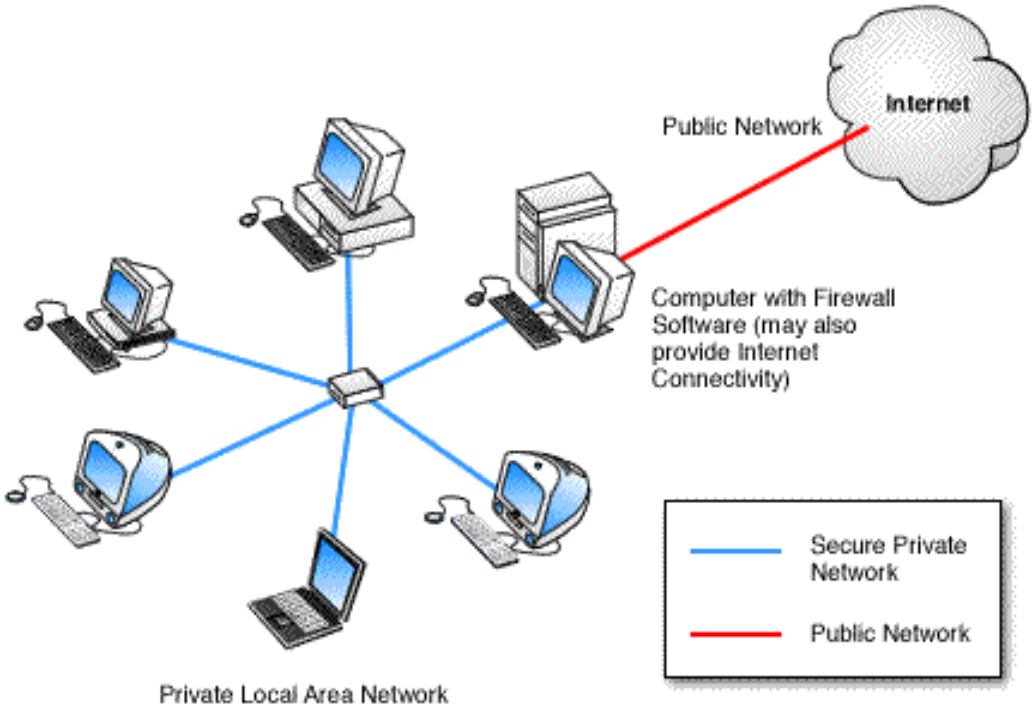
Tecnica di inganno
tramite la quale l' utente di un account finanziario (poste, banca) o meno (accesso alla casella email, servizi web, eccetera) viene convinto ad inserire le proprie credenziali in un sito all' apparenza legittimo ma in effetti fraudolento

esempio: www.posste.it

Firewall 1

- Dotare di firewall il proprio calcolatore

proteggere le porte di comunicazione esterne



Firewall 2

Linux

- iptables
- SuSE Firewall (interfaccia iptables)
- Ipcop
- SmoothWall

Windows

- Integrato da XP SP 3 in avanti, decente
- Zone Alarm, gratuito per uso domestico

Firewall 3

Controllare non solo il traffico

in INGRESSO

ma anche quello

in USCITA

ed, eventualmente, quello

in TRANSITO

SNIFFING / SPOOFING

- SNIFFING:
  Tecnica di ascolto passivo della rete per intercettare dati sensibili (tipicamente password)

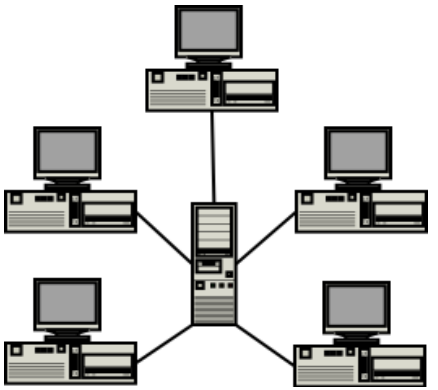
- SPOOFING:
  Tecnica di attacco consistente nel cammuffare le proprie credenziali di rete (Man in the Middle)

Gestione degli utenti

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

Disattivare servizi inutili

- Lasciare in esecuzione sul proprio elaboratore solo i servizi di rete strettamente necessari.
- Per una utenza casalinga, essi sono molto pochi



Freenet

Un network anonimo e cifrato

che funziona all' interno della Internet normale

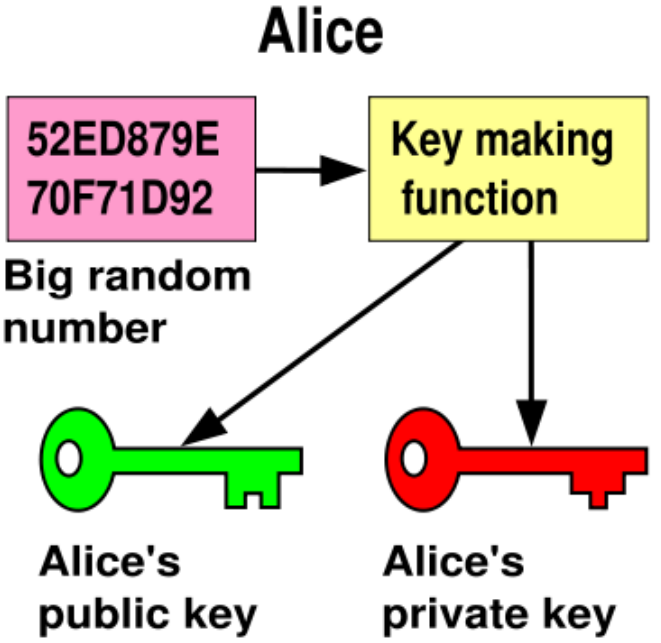
Crittografia

- Email
- Browsing del web
- File
- Interi dischi

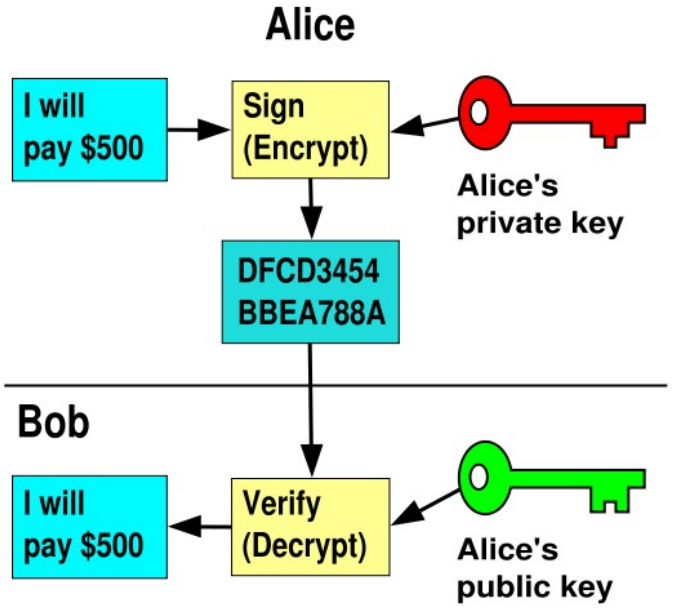
Algoritmi di Protezione

- 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.

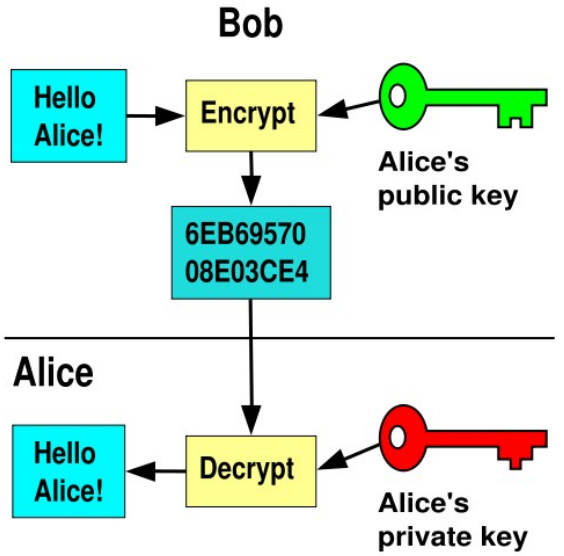
- Algoritmo a chiave asimmetrica
  Ogni soggetto possiede due chiavi, una privata ed una pubblica. La chiave privata non verrà mai compromessa rimanendo sempre in possesso del proprietario, mentre la chiave pubblica può e deve essere fornita a tutti generalmente su server pubblici.



Chiave Asimmetrica

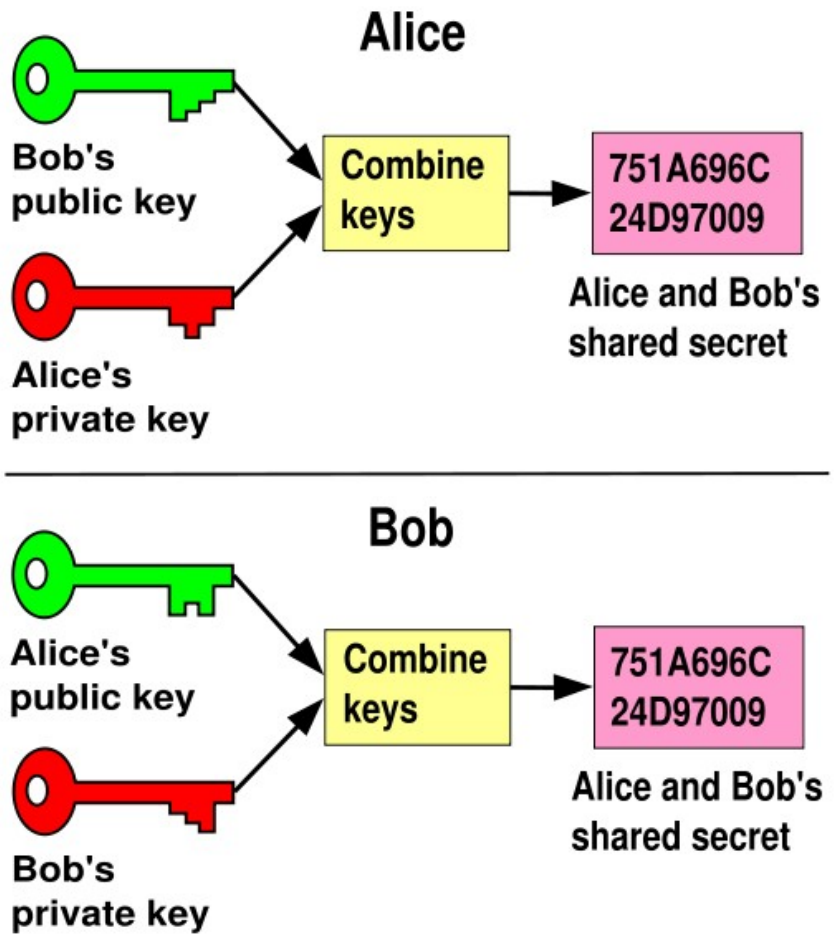


FIRMA DEL MESSAGGIO



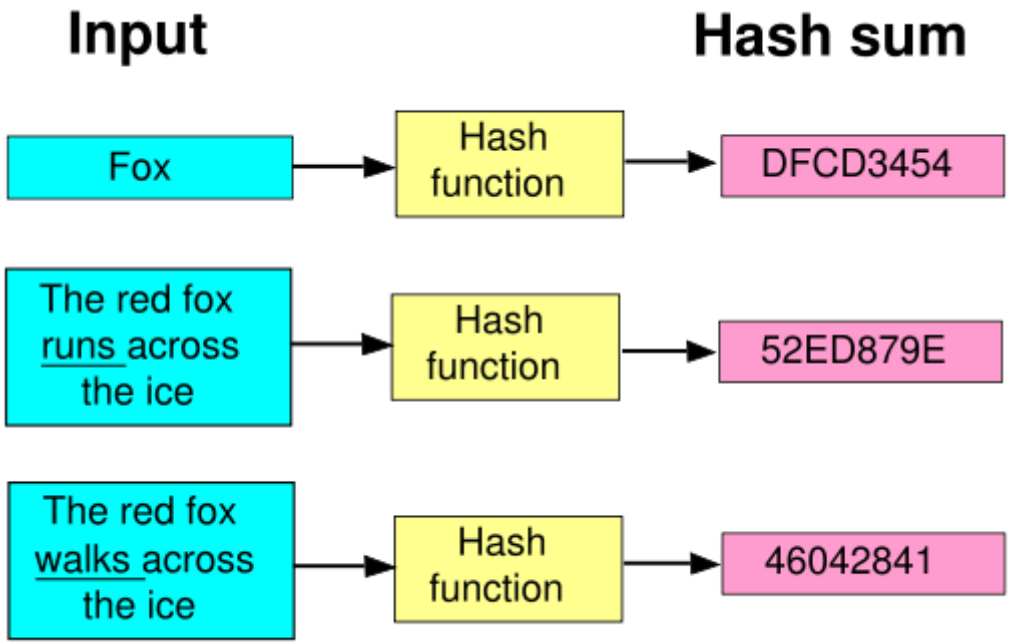
CRITTAZIONE DEL MESSAGGIO

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)

GNUPG

- 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/

Dischi crittografati : 1

- Truecript
- Loop AES
- DM-Crypt
- EncFS

Dischi crittografati : 2

- Truecript
- Loop AES
- DM-Crypt
- EncFS

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

LOG / IDS / Controlli

- Controllare periodicamente i LOG di sistema per scoprire eventuali anomalie
- Intrusion Detecting System: analisi approfondita del sistema per la ricerca di rootkits
- Controllare/cancellare periodicamente cookies dei browser, gli id di sessione, i file temporanei
- Controllare traffico di rete in ingresso e uscita

Varie ed Eventuali

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.

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)

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

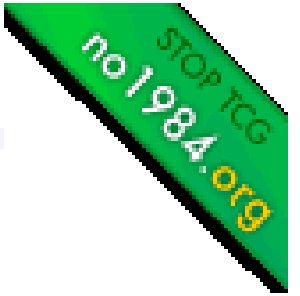
Metodi di filtraggio tramite PROXY

- 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

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

FoLUG: http://www.folug.org