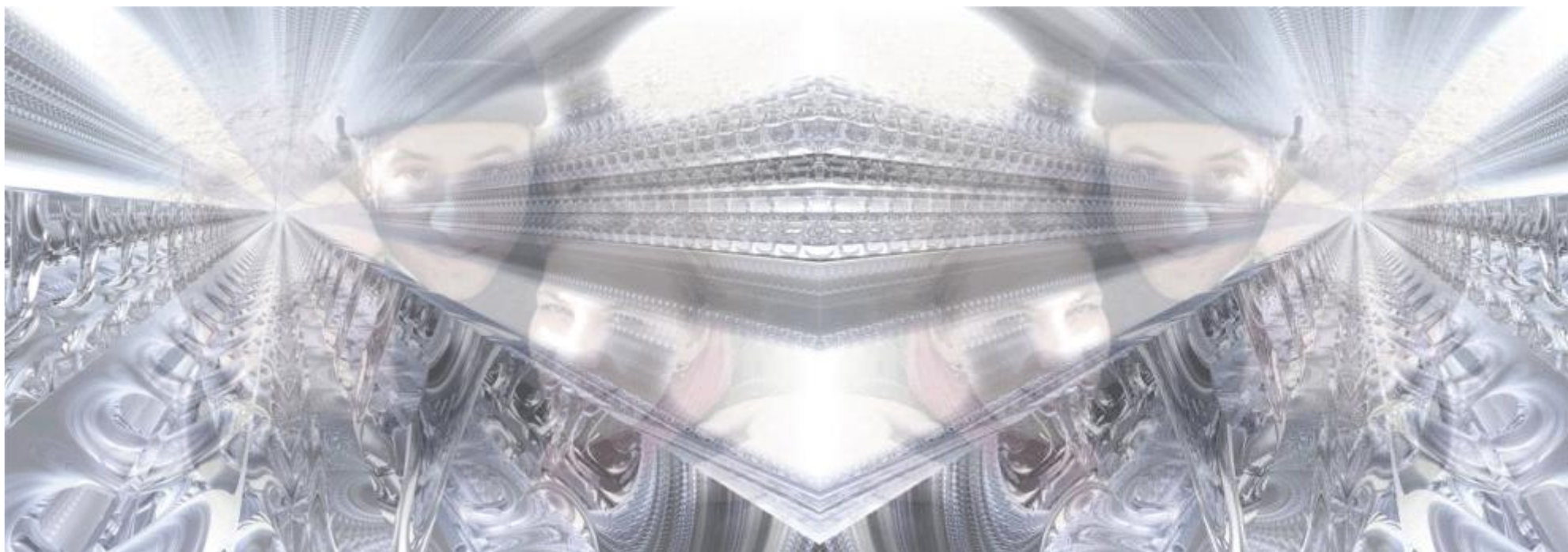


VULNERABILITA' INFORMATICHE E POSSIBILI RIMEDI



Vulnerabilità informatiche e possibili rimedi

PARTE I

Personal Computer

Perchè il personal Computer è vulnerabile

Il sistema operativo

Il personal computer

Autenticazione

Crittografia

Hashing MD5

Attacchi alla password

Sicurezza fisica

Codici malefici (malware)

Tecniche d'attacco sofisticate

Ingegneria sociale

Fishing

Spamming

Keylogging

Danni

Prevenzione

Prevedere l'imprevedibile

PARTE II

Le Reti

Rete LAN (local area network)

Peer to peer

Internet

Intranet

VPN

Vulnerabilità delle reti

Sniffing

Man in the middle

Keylogging

Stack tcp/ip

Dettaglio stack

HTTPS

Firewall

65535 porte

Limite del firewall

IDS

Vulnerabilità di internet

Caratteristiche

Presupposto

Comunicazione e porte

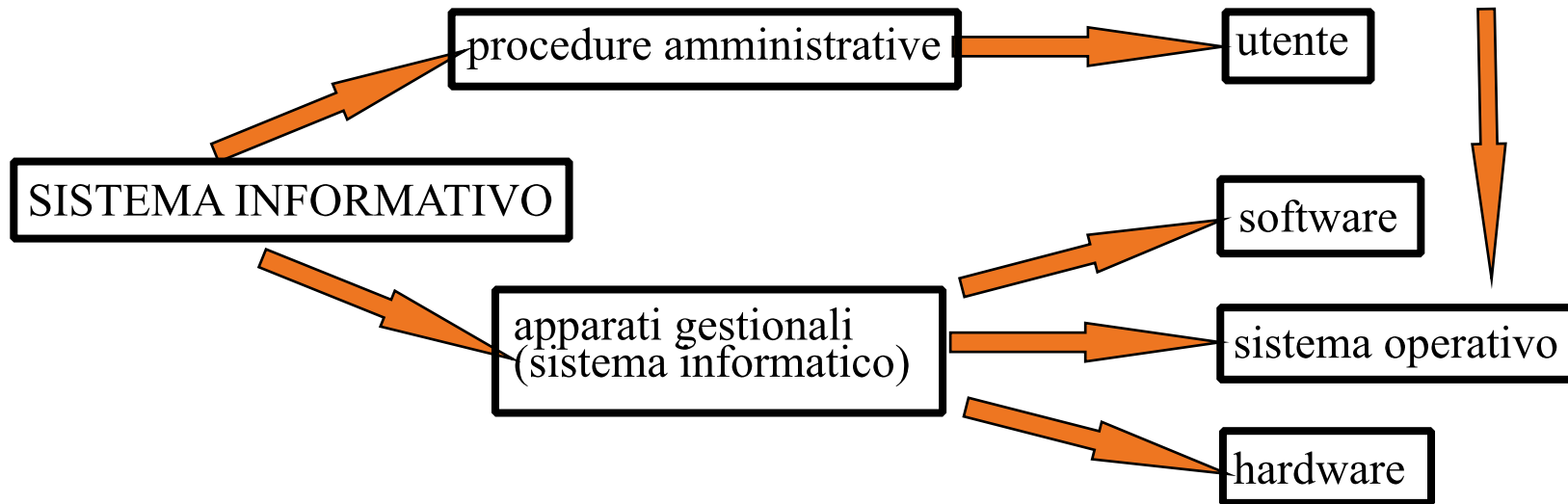
Contromisure

PRIMA PARTE

PERSONAL COMPUTER



PERCHE' IL PERSONAL COMPUTER E' VULNERABILE ?

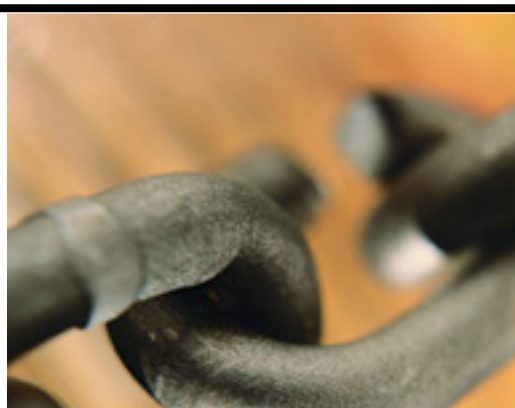


Il SISTEMA OPERATIVO ha il compito di nascondere l'hardware al software e quindi all'utente, permette l'autenticazione di più utenti (da Win2K in poi), ha permesso la diffusione elettronica di massa tramite il Personal Computer perchè l'utente può usare il software senza conoscere l'hardware.

Il Personal Computer, con il suo sistema operativo, è un sistema complesso perchè deve fare tante (troppe) cose : videoscrittura, grafica, CAD, multimedia, DataBase, internet, ecc. Questa capacità di agire a 360 gradi è la prima causa di fragilità. A differenza dei primi calcolatori che erano specializzati e dedicati ad uno o pochissimi compiti .

La prima causa della vulnerabilità del Personal Computer è la complessità

Il Sistema Operativo è l'anello debole del Sistema Informatico e quindi facilmente attaccabile. Il suo carattere "multifunzione" rende il suo codice oggettivamente pieno di falle. Questo è dovuto alla difficoltà che incontrano i programmatori nel prevedere particolari combinazioni di programmi e ad un uso improprio del software.



POSSIBILE RIMEDIO -

Separare fisicamente i dati dal sistema operativo, su un'altra partizione del disco o meglio ancora su un disco separato. In questo modo il Sistema Operativo diventa sacrificabile.

Nel caso del software "chiuso" proprietario (leggi Windows) il problema si accentua ancora di più rispetto a quello "aperto" Open Source (leggi Linux) perchè la correzione delle falle è delegata ad un numero ristretto di programmatori mentre nel secondo caso sono intere comunità che cooperano per risolvere i problemi.



POSSIBILE RIMEDIO -

Configurare due utenti, uno semplice (con poteri limitati) per utilizzare normalmente il PC e l'altro come Amministratore della macchina da utilizzare in casi eccezionali.

POSSIBILE RIMEDIO -

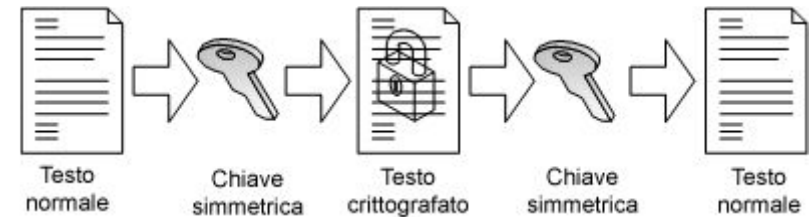
Non scaricare e non installare programmi gratuiti non certificati/verificati



Infatti, mentre il rilascio di aggiornamenti (patch e hotfix) da parte di Microsoft è mensile, gli aggiornamenti del software Open Source possono essere anche quotidiani.

Il Sistema Operativo, oggi, è di tipo multiutente ovvero deve saper distinguere tra diversi profili: l'amministratore della macchina dall'utente semplice e l'utente A dall'utente B. Questa distinzione avviene tramite il processo dell'autenticazione. L'autenticazione è il riconoscimento, per confronto, dell'impronta crittografica della password associata ad un determinato utente con le impronte crittografiche precedentemente archiviate sulla macchina. L'impronta crittografica della password si calcola con algoritmi di HASHING (MD5 o SHA1)

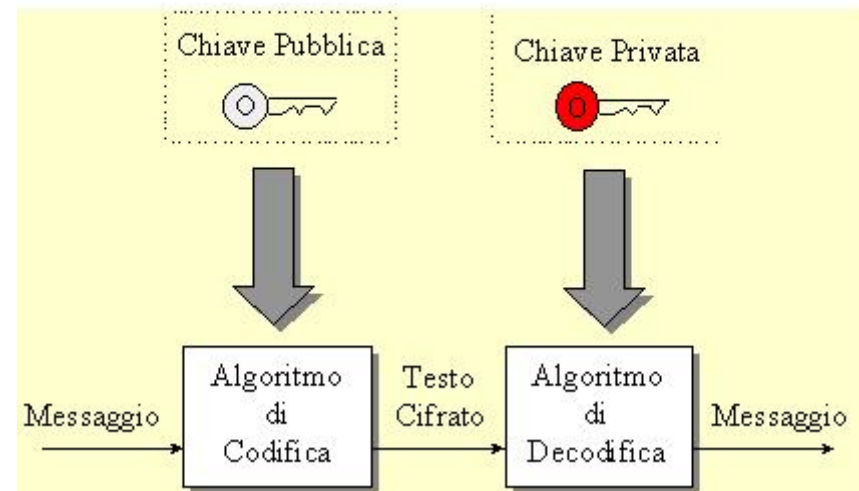
MD51bc29b
82d6622 ENCODER



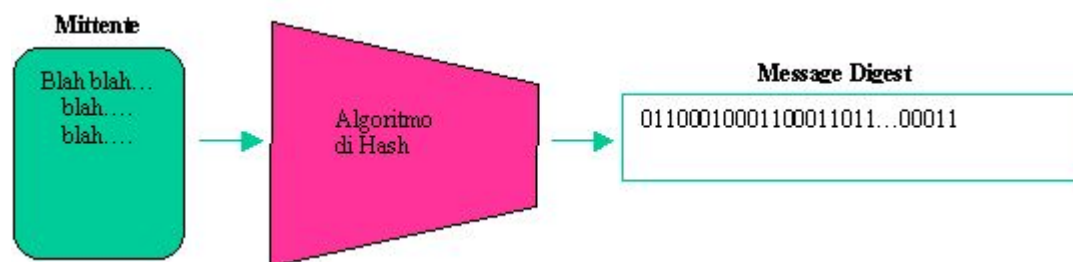
CRITTOGRAFIA



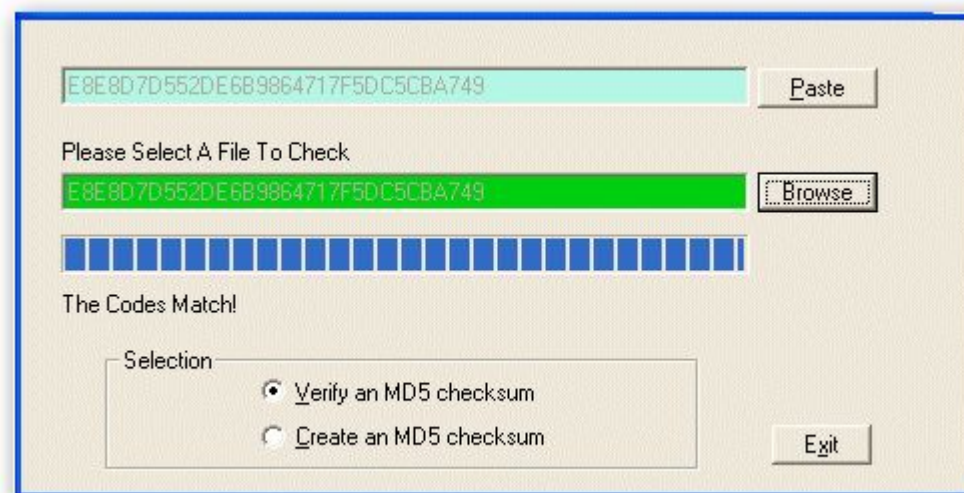
Crittografia a chiave pubblica e privata



Hashing è una cifratura irreversibile, ovvero da un testo (password) o da un file si calcola l'MD5. Partendo dall'MD5 non è possibile (sembra) ricavare la password o il file. Non c'è collisione, ovvero non ci sono due password o due file diversi che producono lo stesso MD5.



Infatti un altro uso dell'Hashing è quello di verificare l'integrità di un file. Quando un sito mette a disposizione il download di un file, di solito, mette a disposizione anche l'MD5. L'utente scarica entrambi e ricalcolando l'MD5 del file scaricato può verificarne l'integrità/originalità.



ATTACCHI ALLA PASSWORD

Attacco a "Forza bruta" = è un attacco per tentativi casuali con strumenti automatici

Attacco a "Dizionario" = è un attacco per tentativi utilizzando automaticamente un dizionario

Possibili rimedi - il file delle impronte non deve essere accessibile/copiabile - la password deve soddisfare specifiche caratteristiche di sicurezza (min 8 caratteri,.....) - Prevedere la chiusura della sessione dopo un certo numero di tentativi infruttuosi



SICUREZZA FISICA

Accesso alle macchine solo a personale autorizzato e munito di credenziali di autenticazione

Password sul BIOS per evitare la possibilità di alterare la sequenza di Boot (deve essere solo HD)

Sigillare lo Chassis per evitare la manomissione del BIOS e/o il furto del disco

"Qualunque computer può essere violato da chi abbia sufficienti risorse, tempo, motivazioni e denaro"

CODICI MALEFICI (MALWARE)



VIRUS - si replicano e danneggiano il software (a volte anche l'hardware, per es. alterando la frequenza del processore)

VIRUS POLIMORFO - è capace di mutare per sfuggire agli antivirus

WORM - si moltiplica fino a saturazione del disco e della rete LAN

TROJAN - programma indesiderato che si camuffa da programma innocuo (praticamente si incollano i due programmi con applicazione exe binder). L'installazione del Trojan si basa sulla complicità inconsapevole dell'utente.

MISTO - combinazione di più malware (un trojan che diffonde un worm che attiva un virus)

TIPO 0-DAY - distribuiti immediatamente dopo la scoperta di una vulnerabilità (sfutta il periodo finestra degli antivirus)

BOMBE LOGICHE/TEMPO - asintomatici su una macchina portatrice sana



TECNICHE D'ATTACCO SOFISTICATE

INGEGNERIA SOCIALE - è lo studio del comportamento individuale di una persona al fine di carpirne informazioni. Un ingegnere sociale può indurre un utente a compromettere il proprio sistema per esempio aprendo una e-mail o scaricando un gioco o cliccando su un link

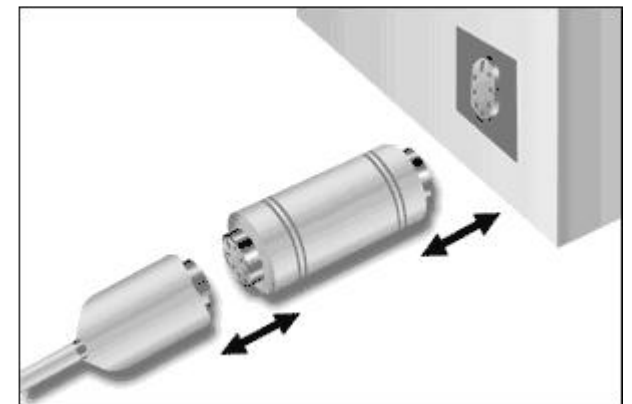
FISHING - l'utente riceve un messaggio apparentemente dalla propria banca, che lo invita a collegarsi ad un link, accedendo al quale si apre un sito simile a quello della banca, per rubare password, numero di carta di credito,.....



SPAMMING - si concretizza in e-mail che hanno in comune il mittente e che si indirizzano ad un numero molto alto di destinatari

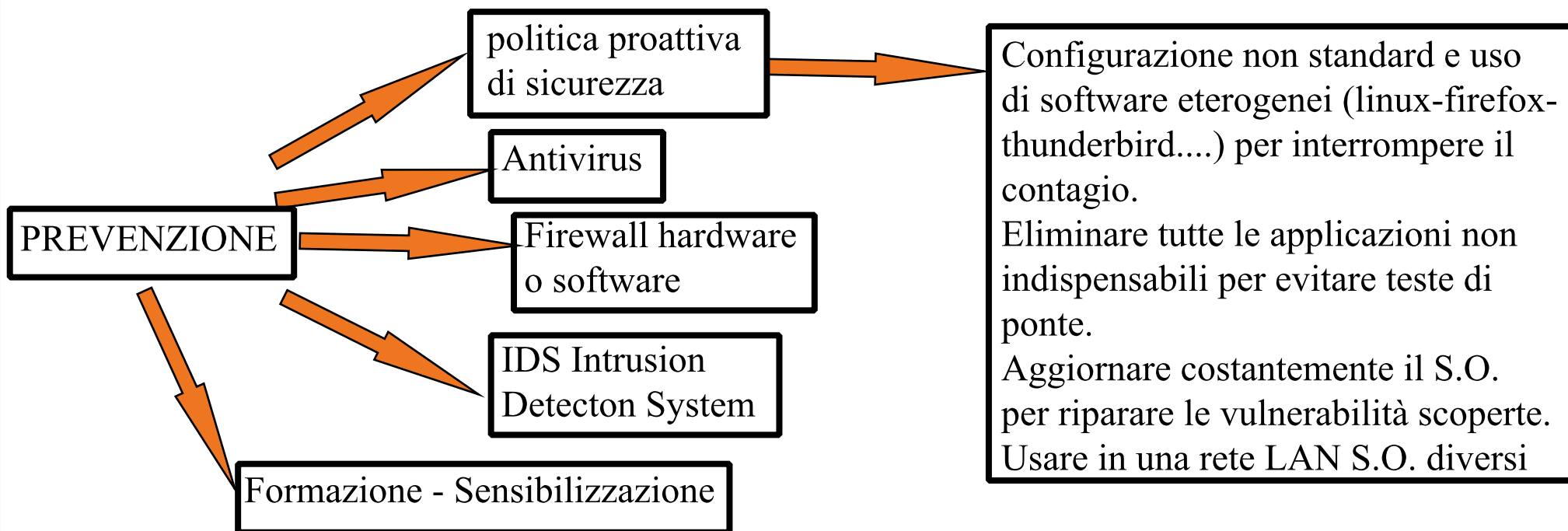


KEYLOGGING - si tratta di hardware o di uno spyware che installa sul PC un codice spia che consente di "vedere" i tasti premuti dall'ignaro utente.....



DANNI

distruzione dei dati, furto dei dati, inattendibilità dei dati, corruzione dei dati e interruzione del servizio,



PREVEDERE L'IMPREVISTO : - uso improprio di PC portatili - apparati bluetooth, cellulari con modem incorporati - modem seriali/USB - Live CD - Floppy di Boot - sequenza di Boot - blocco dello shassis - aparati USB e telefonini collegabili al PC.

Anche una semplice immagine può contenere un codice malefico, quindi ci si può infettare con la semplice navigazione su internet o aprendo una semplice e-mail con codice formattato in HTML

SECONDA PARTE

LE RETI

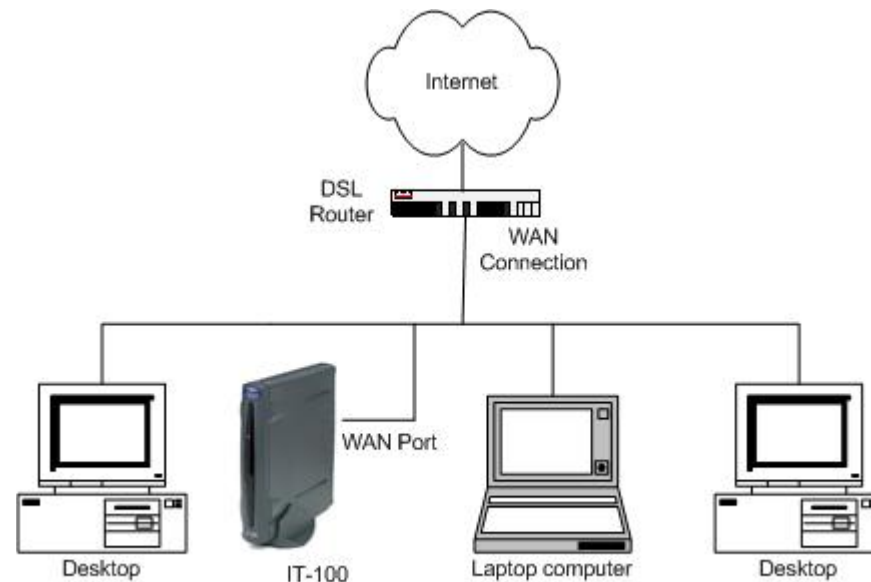
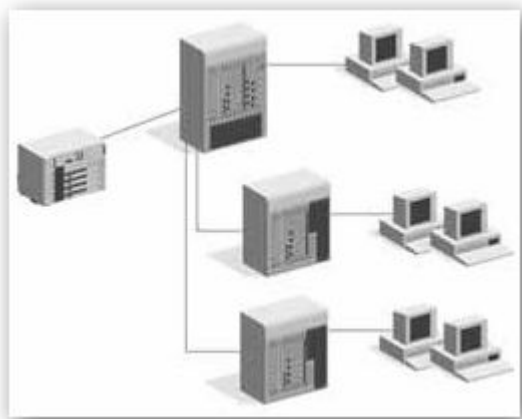


Diagram B

RETE LAN (Local Area Network)



Ogni Pc nella rete ha un nome univoco, un mac address (scheda di rete) univoco e un indirizzo IP (privato o pubblico), fisso o variabile in caso di DHCP), es. 192.168.0.10. Scopo della rete è quello di poter raggiungere risorse condivise (sui Server, su Active Directory o su cartelle condivise da singoli PC)

Attivabile tramite specifici programmi come emule, kaza o winmx, mette in comunicazione via internet n PC distribuiti geograficamente che mettono in condivisione il contenuto di una cartella. * Nessuno può garantire la bontà dei file.



RETE PEER TO PEER

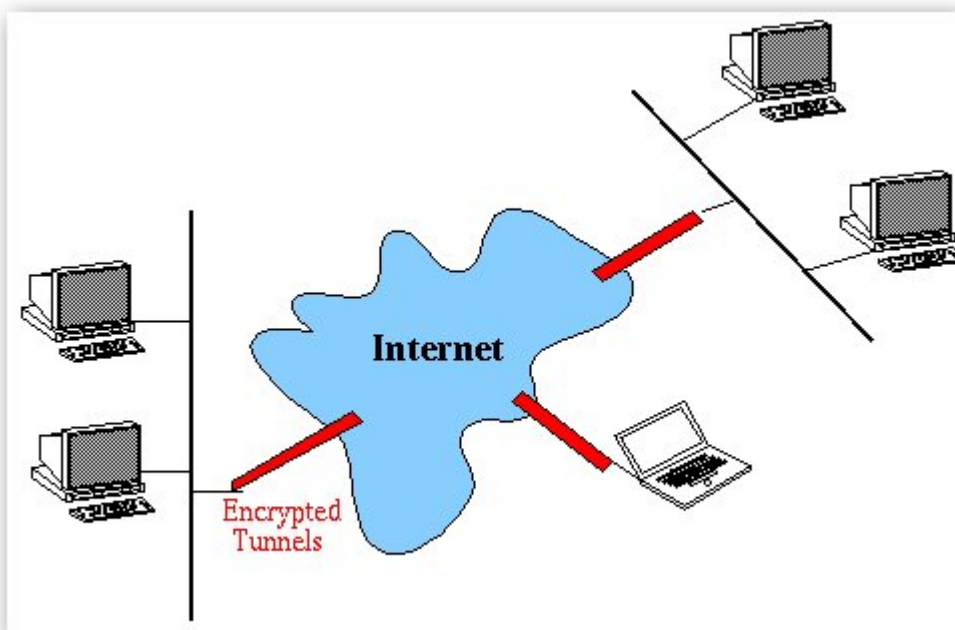
INTERNET



è una rete di reti LAN. Un PC, tramite un programma client (browser) chiede una pagina web ad un computer Server che tramite un programma Server permette di scaricare e visualizzare la pagina web richiesta. Oltre al web, internet permette altri servizi come POP, FTP, TELNET ecc. (ogni servizio ha un suo protocollo) es. TCP/IP

VPN

Virtual Private Network - canale sicuro (tunnel crittografato) su internet tra due reti LAN

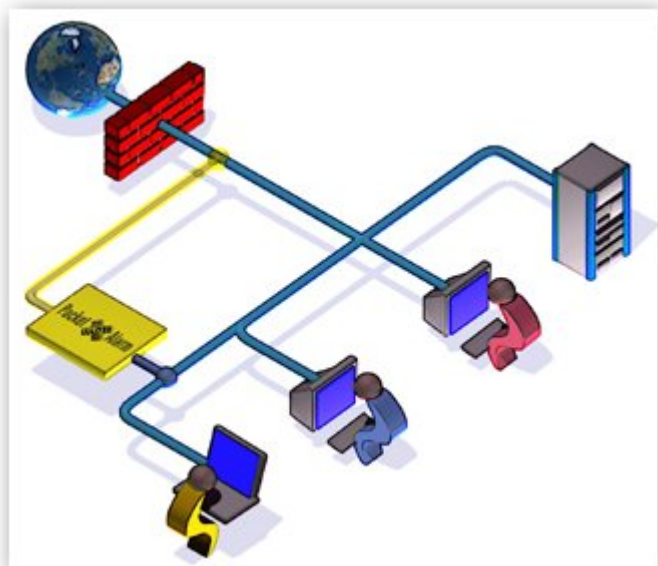


INTRANET

è lo stesso servizio web che da internet, ma è applicato all'interno della stessa rete LAN (Web Server Interno)



VULNERABILITA' DELLE RETI

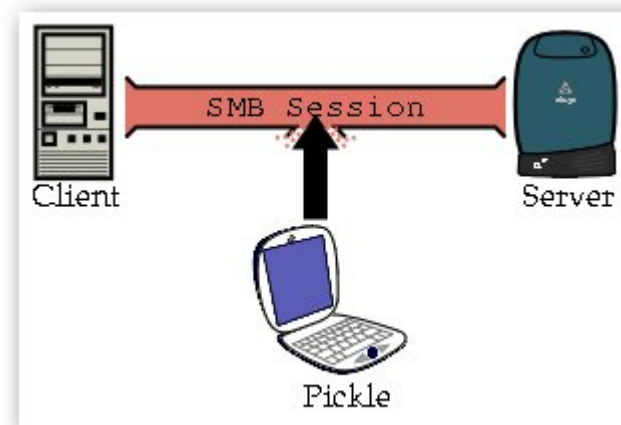


Sniffing del TCP/IP per es. ettercap

un trojan installato su una macchina della rete LAN, con accesso a internet, può sniffare (catturare) i pacchetti in transito e spedirli fuori su internet all'attaccante (i pacchetti trasmessi tramite HTTP, POP, SMT e TELNET sono in chiaro)

Man in the middle

si possono cifrare i dati con il protocollo HTTPS ma questo necessita di 1 o più comunicazioni in HTTP e quindi un attaccante può mettersi in mezzo alla comunicazione e sostituire il certificato digitale. praticamente l'attaccante si sostituisce al gateway tramite un trojan, backdoor, ecc



Keylogging

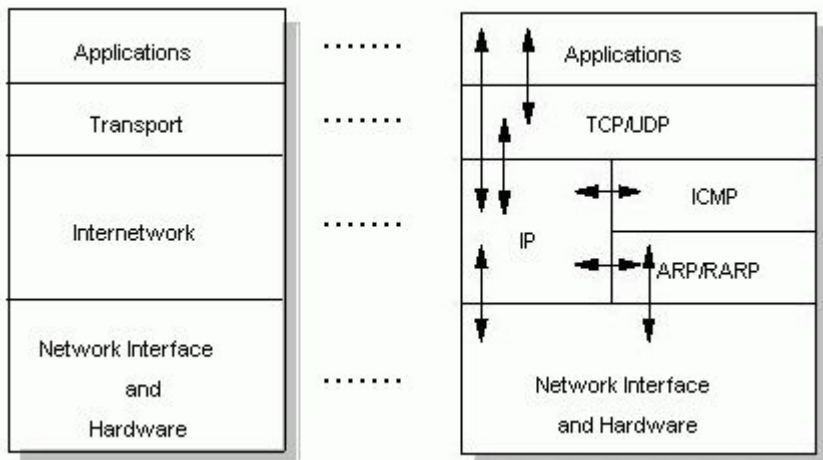
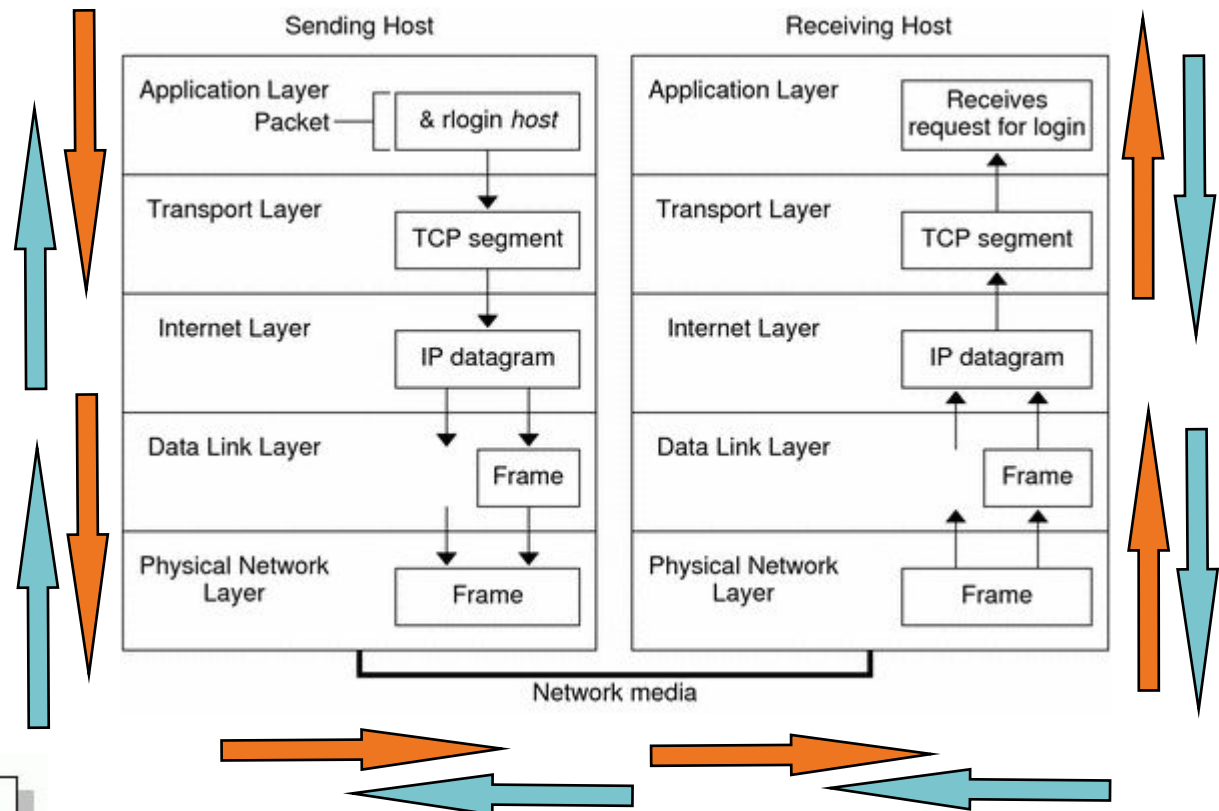
registra ogni battuta sulla tastiera, poi si può salvare il file che viene spedito fuori (è a prova di crittografia perchè avviene prima)

l'unico controllo possibile è analizzare la cache ARP (un altro protocollo) che associa univocamente ogni indirizzo IP della rete con il MAC address della scheda di rete dell'utente che utilizza quel IP.

"L'ingegnere sociale cerca informazioni anche tra i rifiuti, e le trova!"

- Stack del TCP/IP -

Livelli di comunicazione (protocolli) che devono essere attraversati dall'alto verso il basso dal richiedente (sending) e dal basso verso l'alto dal lato del ricevente (receiving) e viceversa da ricevente verso il richiedente in senso contrario.



Dettaglio dello STACK

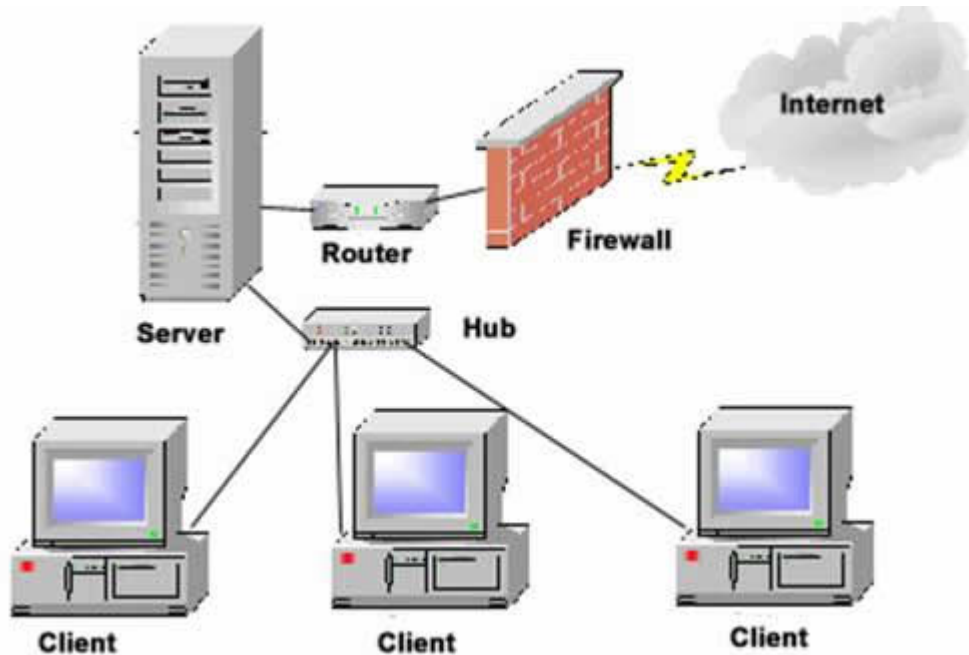
- Livello delle Applicazioni
- Livello TCP/UDP
- Livello rete (IP - ICMP - ARP - RARP)
- Livello fisico (scheda e cavo)



Per rendere sicura la comunicazione istitui come Banche, Catasto, Anagrafe Tributaria, ecc. cifrano i pacchetti che trasmettono da e verso l'utente a livello di trasporto sul protocollo HTTP applicando il Secure Socket Layer (SSL) ovvero uno strato sicuro, ottenendo così il famoso HTTPS

- 1) l'utente fa la richiesta tramite protocollo normale (in chiaro) HTTP di comunicazione sicura al Server
- 2) il Server trasmette tramite protocollo normale (in chiaro) HTTP all'utente un Certificato Digitale (chiave pubblica)
- 3) il browser dell'utente cifra le proprie credenziali di autenticazione con la chiave pubblica ricevuta e le trasmette al server
- 4) il Server decifra le credenziali dell'utente con la propria chiave privata ed eventualmente autentica l'utente mandandogli un cookie per non ripetere tutta la procedura
- 5) l'utente, da questo momento, utilizzando il protocollo sicuro HTTPS trasmette e riceve pacchetti cifrati (crittografati) che anche se intercettati risultano inintelligibili

**** PROBLEMA - Nelle prime fasi della comunicazione il protocollo HTTP trasmette in chiaro e qualcuno potrebbe mettersi in mezzo (Man in the Middle) e spacciarsi per la banca verso l'utente e per l'utente verso la banca**



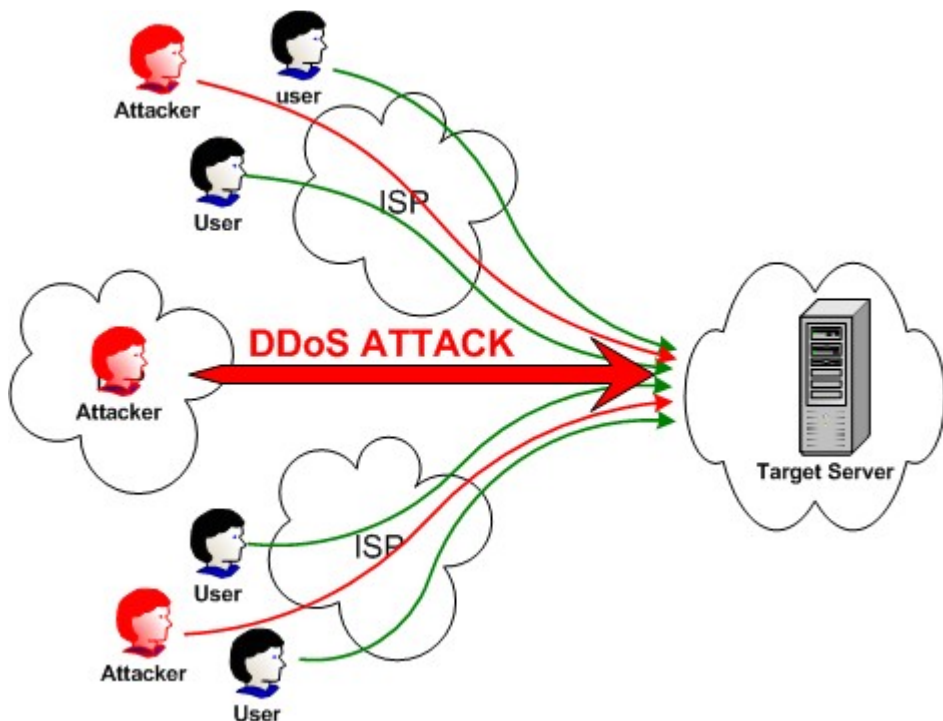
FIREWALL

Può essere hardware (aziendale) o software (personale). Filtra (blocca con una politica sulle porte) la comunicazione in ENTRATA (tramite regole prefissate) e in USCITA (tramite regole prefissate[aziendale] o variabili [personale], in questo caso il firewall va istruito)

PORTE di comunicazione

La comunicazione avviene attraverso 65.535 porte con il protocollo TCP o UDP

```
IPTraf
Proto/Port      Pkts  Bytes  PktsTo  BytesTo  PktsFrom  BytesFrom
TCP/6669:       276   23982   140     6064    136      1791
TCP/8080:       842   307416  360     28707   482      27870
UDP/4000:        6     315    3       168     3        14
TCP/ftp:        16    1165   8       451     8        71
TCP/ftp-data:   9     1354   4       164     5        119
UDP/domain:     22    2825   11      686    11       213
TCP/telnet:     75    4471   40      2353   35       211
TCP/pop-3:      37    2058   18      931    19       112
TCP/smtp:       37    2438   20      1191   17       124
UDP/netbios-dg: 4     948    2       474    2        47
```

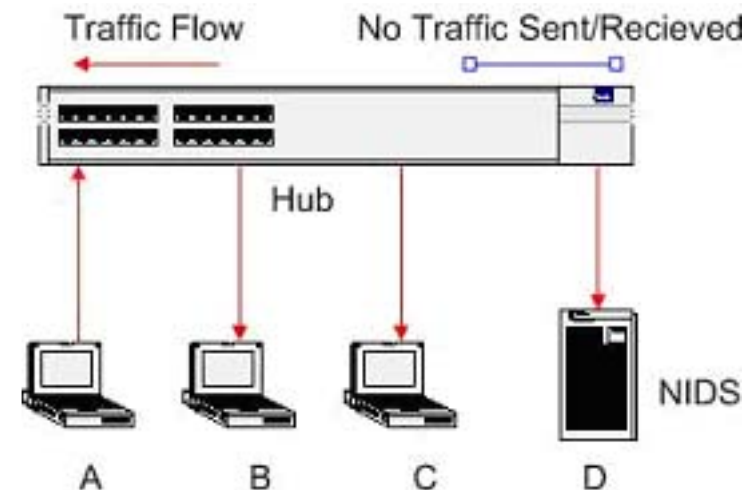


LIMITI del FIREWALL

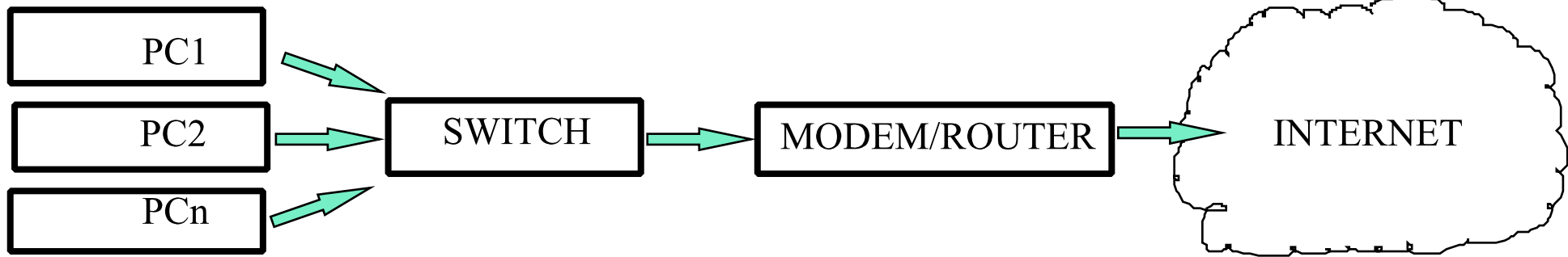
Potrebbe essere attaccato con un sovraccarico (attacco DoS Denial of Service). Comunque il firewall aziendale centralizzato diventa inutile in una LAN dove sono installati/installabili modem seriali o USB. Diventa inutile anche quando l'utente permette la connessione di un programma ad un sito INSICURO che apparentemente sembra sicuro

IDS Intrusion Detection System

E' analogo a uno Sniffer (aziendale) che controlla il traffico e lo confronta con un database. Può essere PASSIVO e cioè avverte l'amministratore per e-mail o ATIVO e cioè attiva l'antivirus o altro (per es. blocca il traffico)



VULNERABILITA' di INTERNET



Caratteristiche

La struttura e la topologia di internet fanno sì che :

(milioni di nodi interconnessi a banda larga)

- i codici malefici si diffondono in tempo reale
- l'autore/attaccante si può nascondere, far perdere le proprie tracce, mantenere l'anonimato
- la propria sicurezza è legata alla sicurezza degli altri
- la soglia critica di trasmissione virale è prossima allo zero
- un attaccante può usare il PC dell'utente A per attaccare l'utente B

Presupposto

quasi tutte le macchine sono configurate in maniera identica e pertanto presentano le stesse vulnerabilità

Quando un PC viene TROJANIZZATO, diventa uno ZOMBIE nelle mani dell'attaccante

Comunicazione e PORTE Schematicamente, la comunicazione su internet avviene tramite 2 protocolli (TCP e UDP) e su 36.535 porte

- i programmi trojan tipo Backorifice o Netbus aprono delle porte in ascolto (Backdoor)
- l'attaccante attiva un servizio su una porta aperta e può eseguire comandi da remoto
- può introdursi su altre macchine della stessa rete o su macchine esterne (su internet)
- la macchina trojanizzata diventa uno zombie e si comporta da testa di ponte per attacchi verso l'interno/esterno garantendo l'anonimato all'attaccante.

Contromisure

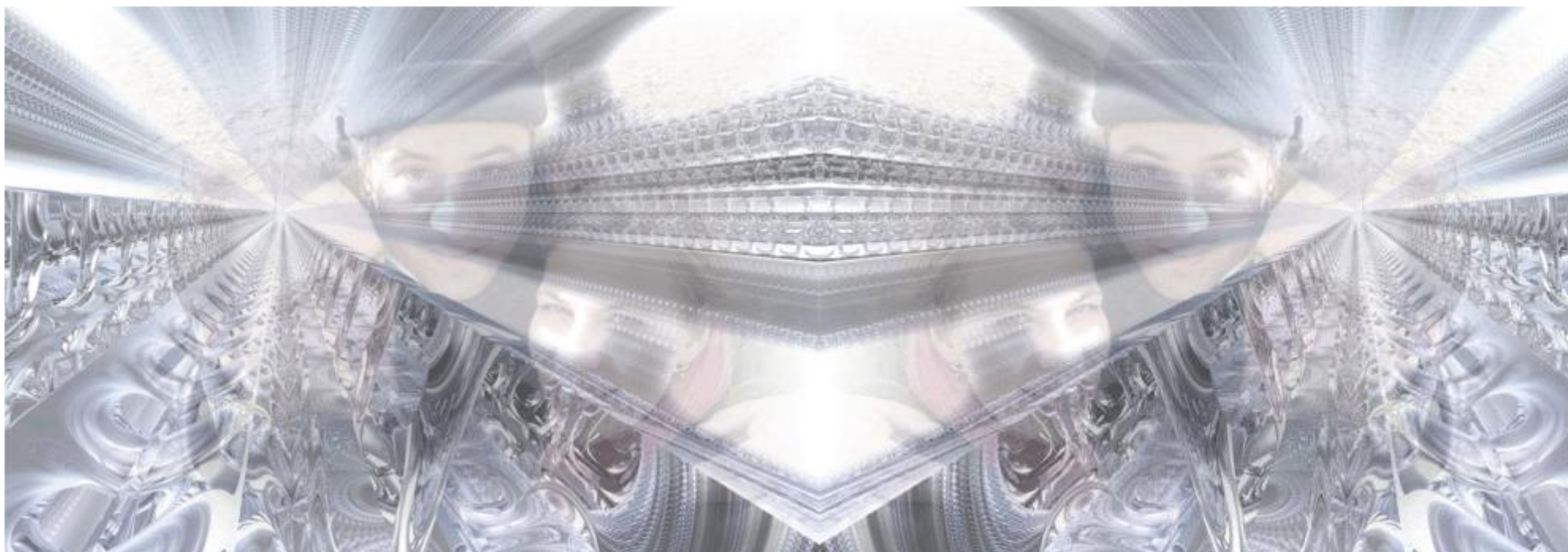
Le macchine, in una rete LAN o singole, dovrebbero essere configurate per quello che devono fare (al minimo)

Si dovrebbero disinstallare tutte le applicazioni INUTILI (giochi, multimedia, USB, Wifire, IRDA, Bluetooth, Chat,

Implementare la sicurezza proattiva (rendere l'attacco diseconomico)

Stabilire chiare e condivise politiche di navigazione internet

VULNERABILITA' INFORMATICHE E POSSIBILI RIMEDI



FINE