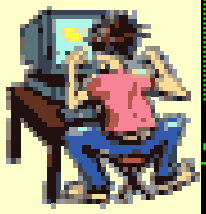
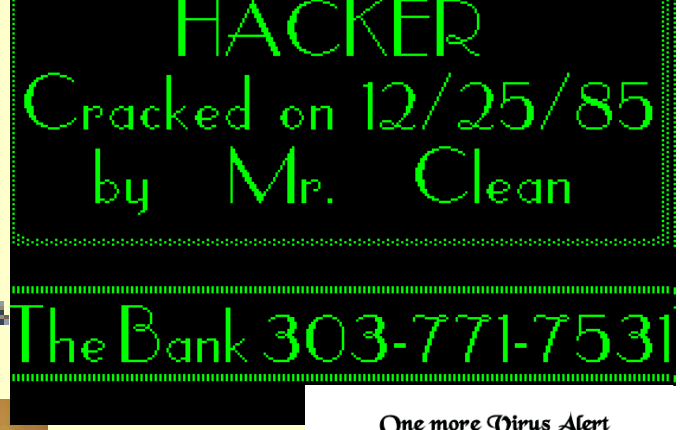




Sicurezza e Internet 03

Gli strumenti di base

1. Strumenti tecnologici
    1. Antivirus
    2. Adware, spyware, et similia
    3. Firewall
2. Strumenti basati sulla identità
    1. What you know
    2. What you have
    3. What you are

Gli Antivirus

- Un antivirus è un programma specificatamente studiato per prevenire, individuare e rimuovere i virus dal proprio pc.
- Quando negli anni 80 iniziano a nascere i virus informatici, i più curiosi esperti e "smanettoni" non rimasero a guardare e un paio di anni dopo la comparsa di Brain, nel 1988 comparvero i primi tool di rimozione del virus.
- Nello stesso anno a risposta per l'attacco del worm di Morris, venne fondato il CERT/CC - Computer Emergency Response Team/Coordination Center - una sorta di associazione che fornisce assistenza in caso di emergenze o epidemie.
- Negli anni a seguire vengono rilasciati i primi software antivirus, tra i quali Dr.Solomon Antivirus.

Gli Antivirus

- Norton, Kaspersky, McAfee, PCCillin, Nod32, Avast, F-Secure...di nomi ce ne sono tanti e di pareri sull'efficienza altrettanti, ma spesso si ignora come veramente i software antivirus funzionino e perché ci sia bisogno di aggiornarli spesso, o addirittura si ignora il perché abbiano bisogno di aggiornarsi.
- Scomponiamo dunque un software antivirus.
  - Le parti fondamentali sono sostanzialmente due,
    1. il modulo di scansione on-access
    2. il modulo di scansione on-demand.
  - Il primo è il modulo che controlla in tempo reale cosa avviene sul pc, il secondo invece è il modulo che si occupa della scansione manuale del sistema, solo quando l'utente richiede una scansione.

Il funzionamento degli antivirus

- Per controllarne l'effettiva attività è possibile navigare nel sito www.eicar.org e scaricare il file di prova EICAR.COM. http://www.eicar.org/anti_virus_test_file.htm
- Se il vostro antivirus lancerà un allarme non preoccupatevi, è tutto ok: non è infatti un vero virus, ma solo un file di prova che i software antivirus riconoscono come virus. Ciò vi servirà per verificare le funzionalità e l'efficienza di individuazione del vostro antivirus.

scansione per mezzo di

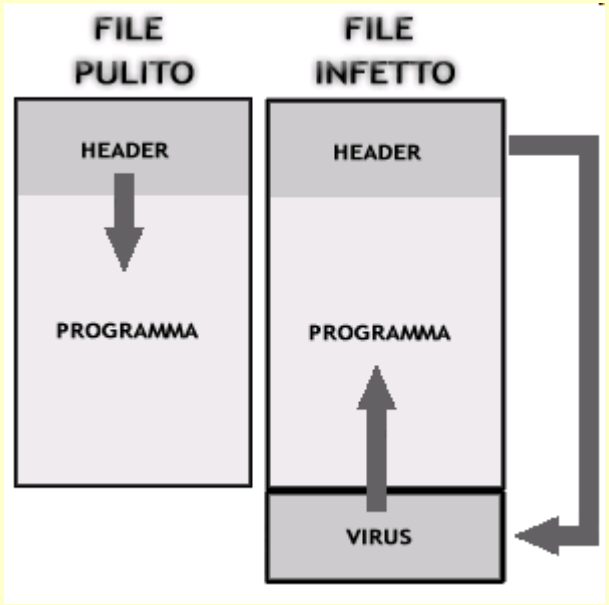
- "impronte" digitali
- tecnologia euristica.

“Impronte” Digit

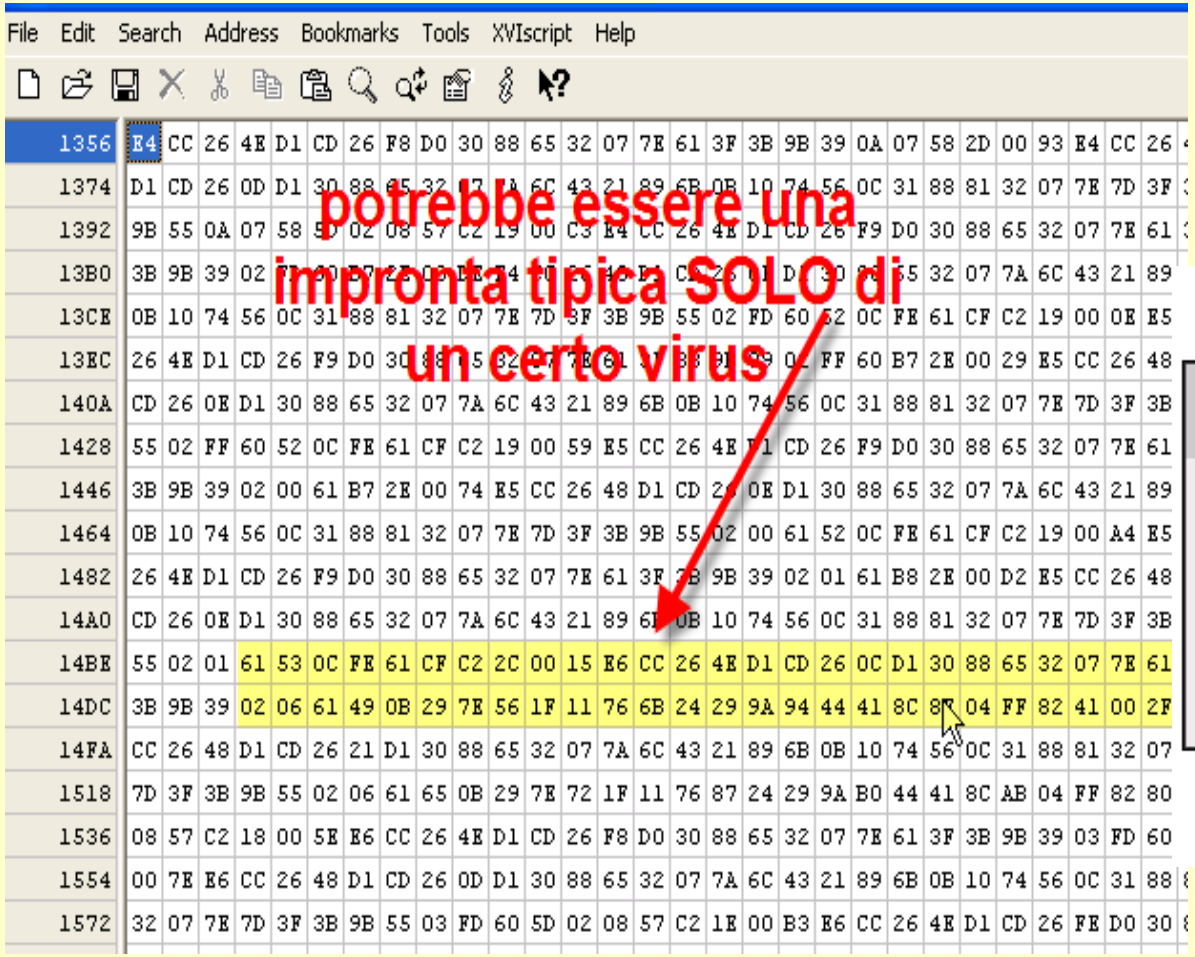
- Un virus non è nient'altro che un software come lo sono tanti altri, quindi un insieme di righe di codice che, compilato, diviene codice macchina. Per poter identificare un virus si è dunque pensato di cercare all'interno del file infetto una serie di bytes riconducibili con certezza la presenza di quel determinato virus.
- Quindi un ricercatore di una società di antivirus deve prendere il file infetto dal virus, disassemblarlo (cioè leggerne il codice macchina interpretato, per una seppure lieve facilitazione nella comprensione) e cercare all'interno una **sequenza di bytes** che sia propria del virus, cioè che solo quel virus ha e nessun altro programma esistente al mondo.
- Un software antivirus non controlla esclusivamente la presenza della sequenza di bytes all'interno dei file, ma prende in considerazione molti altri parametri, tipo la locazione di dove dovrebbe trovarsi la specifica sequenza.
- Per avere una certezza assoluta che il file sia infetto, alcuni ricercatori ricorrono a più di una sequenza per identificare un preciso malware, prese in zone differenti del file.

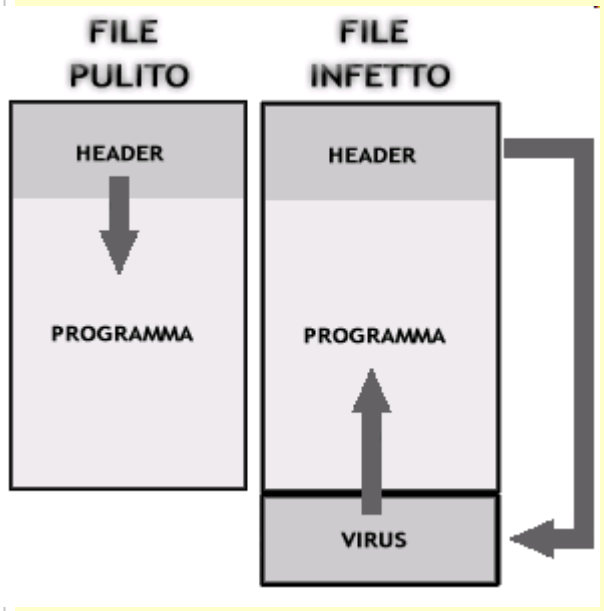
Come è fatto un malware

- Un file eseguibile tipico è composto all'interno da varie sezioni:
- un header - una sorta di presentazione del file - e le varie sezioni che contengono il codice eseguibile del programma.
- Un esempio di file infector può essere il virus Vienna: il virus inserisce subito dopo l'ultima sezione del file da colpire il proprio codice e modifica l'intestazione del file in modo da far eseguire il codice del virus prima e il programma subito dopo. Ecco che il file è stato dunque infettato.



Come è fatto un malware





Antivirus

- il "grosso" limite dei software antivirus:
  - **non è possibile identificare un virus se prima non viene aggiornato il database di firme con la relativa firma digitale**.
- Possono passare pochi minuti dalla diffusione della minaccia come possono passare diverse ore, giorni, senza che il software antivirus riesca a riconoscere un determinato malware.
- Vista la rapidità con la quale nascono ogni giorno nuovi virus, si è sentita la necessità di dover studiare qualche modo per poter prevenire nuovi virus.
- scansione euristica.
- Il termine euristica deriva dal greco "eurískein" che, tradotto, assume il significato di "scoprire". La scansione euristica si prende infatti il compito di scoprire nuovi virus analizzandone esclusivamente alcuni fattori e calcolandone la percentuale di pericolosità.
- raccoglie quante più informazioni possibili sui dettagli di un file sospetto e giudica se ritenerlo sospetto oppure no

Virus, trojan, worm, spyware, adware, dialer, phishing,

Sono diverse forme con cui si manifestano

- i worm sono sempre più spesso usati come vettori di spyware e cavalli di troia (trojan):
- installano proxy e downloader di vario tipo, che spesso notificano il loro stato su canali IRC (Internet Relay Chat) e vengono pilotati in remoto da malintenzionati, trasformando i computer infetti in cosiddetti “zombie”, ovvero sistemi attraverso i quali sia possibile commettere attacchi di vario tipo.
- Insieme allo Spam, questa è una tendenza che negli ultimi mesi è risultata in continuo aumento.

spyware e adware?

Si distingue tra

- Adware, che è una forma “innocua” di malware, il cui scopo consiste nel mostrare annunci pubblicitari e simili,
- Spyware, che invece viene scritto con lo scopo di sottrarre informazioni personali in modo illegittimo,
  - Insieme al proprio programma antivirus si raccomanda di usare un programma antispyware dedicato. Ad esempio, si consiglia l’uso di *Spybot Search & Destroy*. Questo programma è gratuito per uso personale..

Il Decalogo

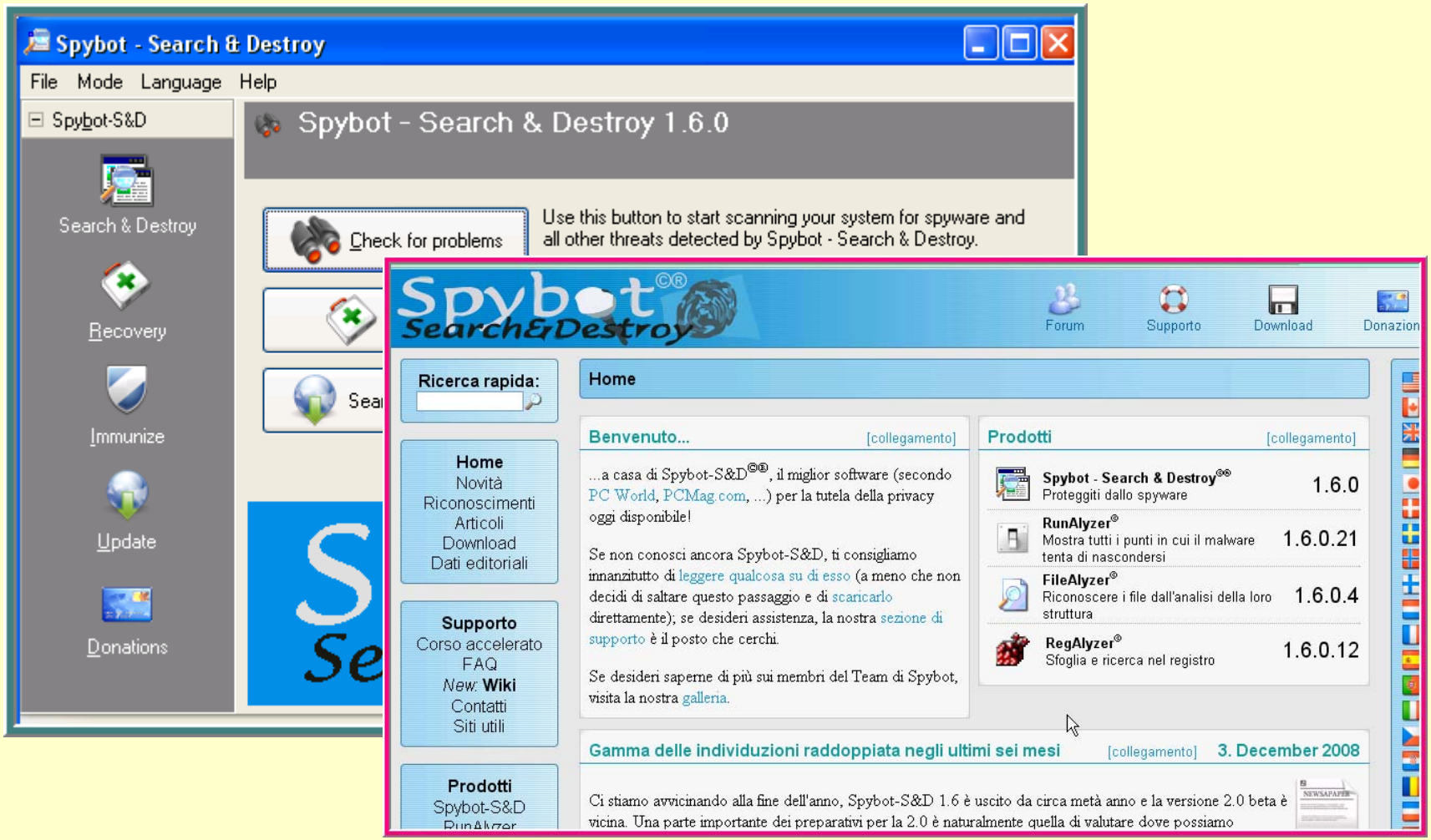
1. **usare un buon antivirus**: qualunque computer connesso alla rete Internet deve esserne munito; inoltre è altrettanto importante provvedere con regolarità all'aggiornamento del file delle firme;
2. **usare un firewall**: può sembrare eccessivo ma l'uso di dispositivi di filtraggio come i firewall, purché opportunamente configurati, è in grado di offrire un discreto grado di protezione contro determinati tipi di attacco e soprattutto contro tutta una serie di attività preparatorie (come ad es. la scansione delle porte TCP/UDP) che un aggressore in genere compie prima di tentare un accesso non autorizzato;
3. **non aprire ingenuamente allegati di posta elettronica**: questa semplice regola vale anche per i messaggi di posta che sembrano originati da un indirizzo conosciuto; in ogni caso è sempre opportuno salvare in un file l'allegato e sottoporlo ad una scansione virale prima di aprirlo;
4. **non eseguire ingenuamente programmi di ogni tipo**: è buona regola accertarsi sempre della genuinità di qualsiasi programma prima di eseguirlo e lo stesso dicasi per tutti quei documenti che possono contenere delle macro;
5. **applicare sempre le più recenti patch**: questo vale non soltanto per il sistema operativo ma anche per il software applicativo;
6. **prestare la massima attenzione al funzionamento anomalo del sistema operativo**: è assolutamente opportuno guardare sempre con sospetto ai funzionamenti apparentemente inspiegabili del sistema operativo e cercare di individuarne le cause per quanto possibile anche con l'uso di strumenti specifici;
7. **disabilitare Java, JavaScript ed ActiveX**: queste tecnologie possono costituire una vera spina nel fianco durante la navigazione su Internet; in alternativa, per non rendere la navigazione su alcuni siti frustrante, è possibile proteggersi, ma entro certi limiti, facendo uso di software specifico che funge da filtro per i contenuti interattivi che vengono normalmente ricevuti o utilizzando forme di navigazione anonime tramite proxy server;
8. **disabilitare le funzionalità di scripting nei client di posta elettronica**: spesso infatti le maggiori vulnerabilità che colpiscono i browser, legate alla presenza di contenuti interattivi, si presentano anche in questo genere di software;
9. **fare un backup regolare di tutti i dati sensibili**: ugualmente importante è tenere in posti sicuri le copie generate;
10. **creare un disco di boot**: ciò può aiutare in un eventuale attività di recovery di un sistema compromesso a patto però che la copia sia assolutamente genuina e sia conservata in un luogo sicuro.

AD-ware

http://www.lavasoft.com/products/ad_aware_free.php

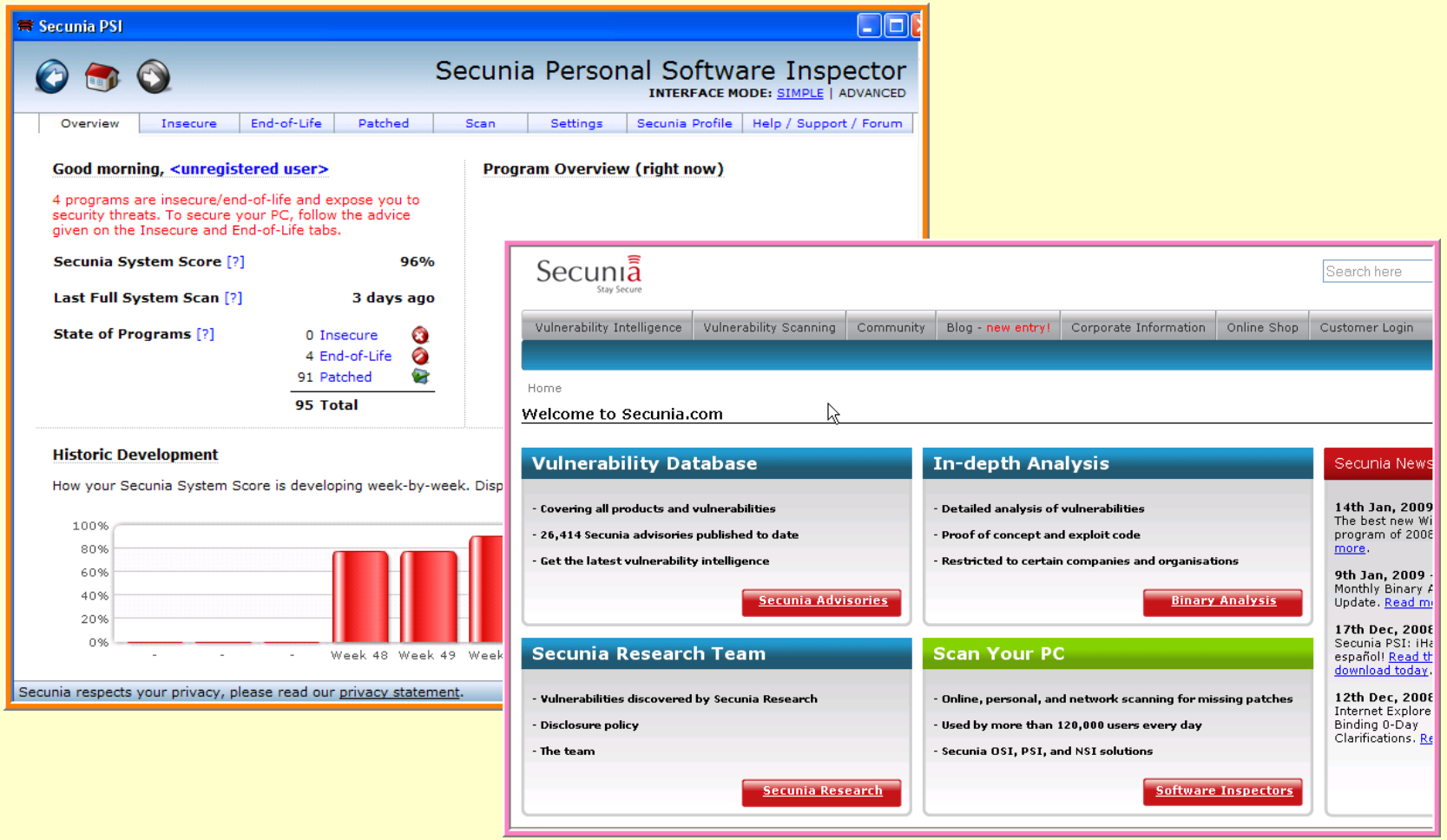
Spy-ware

http://www.safer-networking.org/it/home/index.html

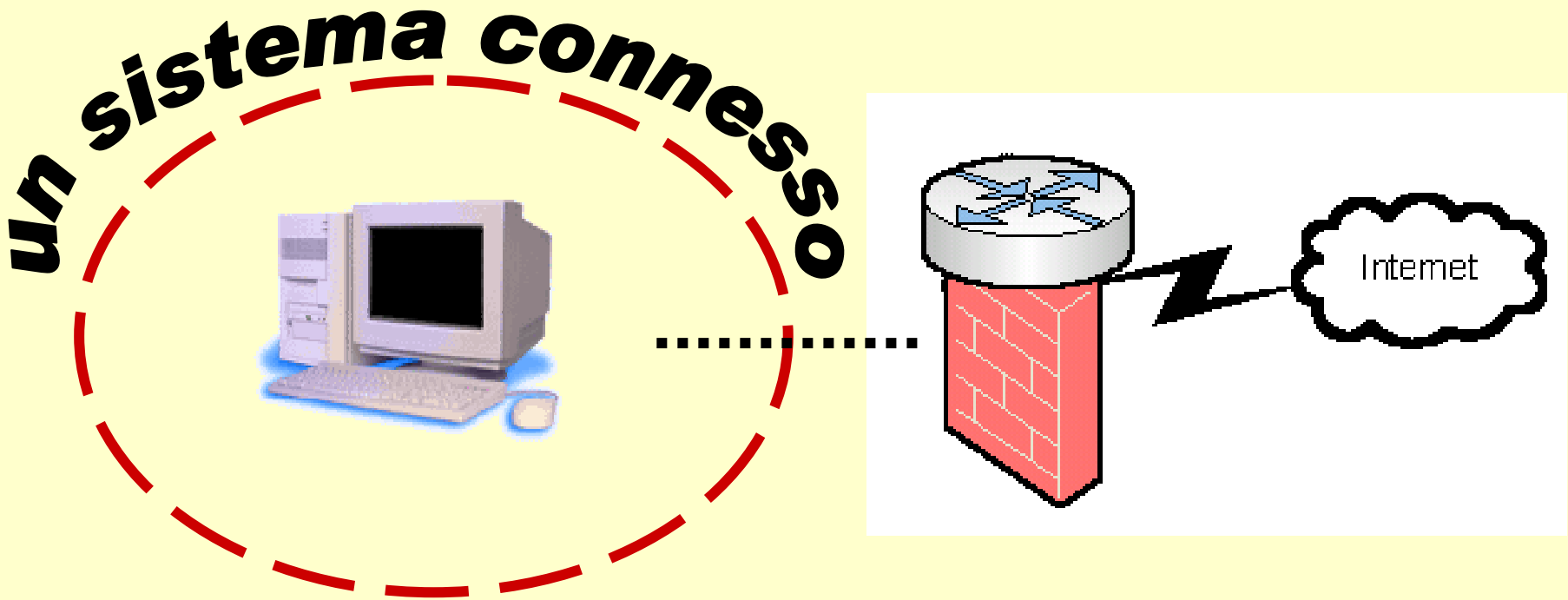


Patch di sicurezza

http://secunia.com/



Il Firewall



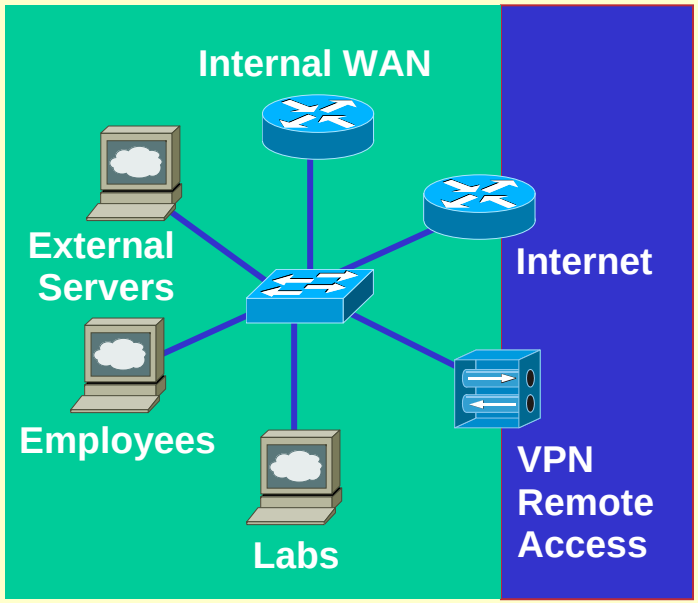
Apparato di rete hardware o software che filtra tutti i pacchetti entranti ed uscenti, da e verso una rete o un computer, applicando regole che contribuiscono alla sicurezza della stessa.
Il programma può girare sul singolo PC (Personal Firewall) oppure in un dispositivo sulla linea di ingresso (il router oppure un dispositivo ad hoc)

Firewall

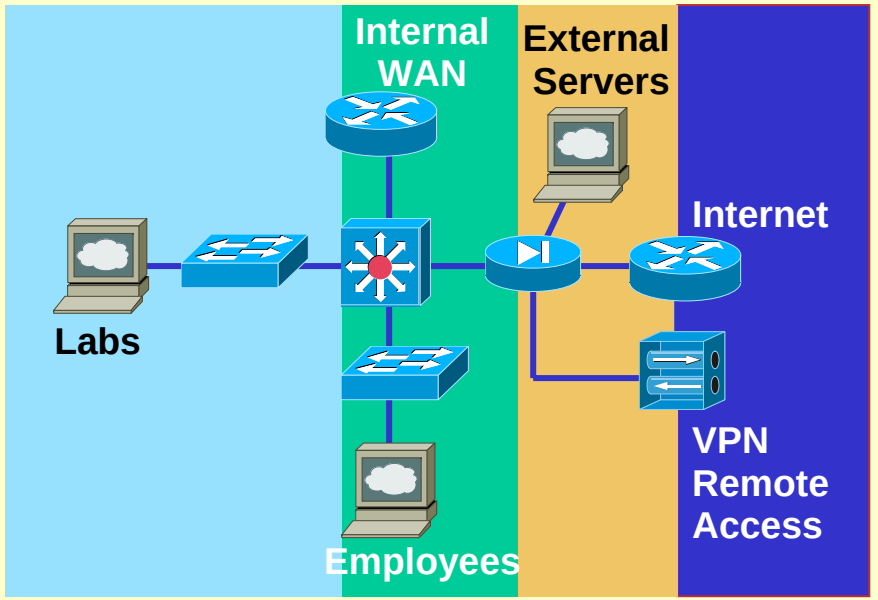
- termine inglese dal significato originario di parete refrattaria, muro tagliafuoco', "muro ignifugo"'; in italiano anche parafuoco o parafiamma
- è un componente passivo di difesa perimetrale che può anche svolgere funzioni di collegamento tra due o più tronconi di rete.
- Usualmente la rete viene divisa in due sottoreti:
  - una, detta esterna, comprende l'intera Internet
  - l'altra interna, detta LAN (Local Area Network), comprende una sezione più o meno grande di un insieme di computer locali.
- In alcuni casi è possibile che si crei l'esigenza di creare una terza sottorete detta DMZ (o zona demilitarizzata) atta a contenere quei sistemi che devono essere isolati dalla rete interna ma devono comunque essere protetti dal firewall.

Domains of Trust (Zones)

1stcase.com

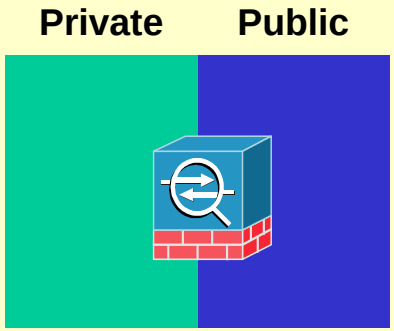


2ndcase.com

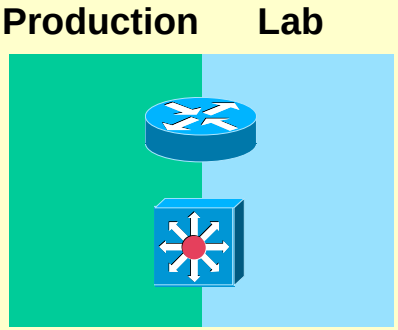


Domains of Trust segment communities by policy

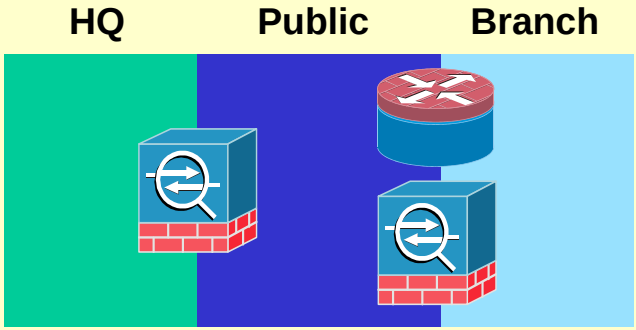
Sample Domains of Trust



- Steep gradient = high risk
- Considerable safeguards
  - –Advanced Firewalling
  - –Flow-based inspection
  - –Misuse detection (IPS)
  - –Constant monitoring

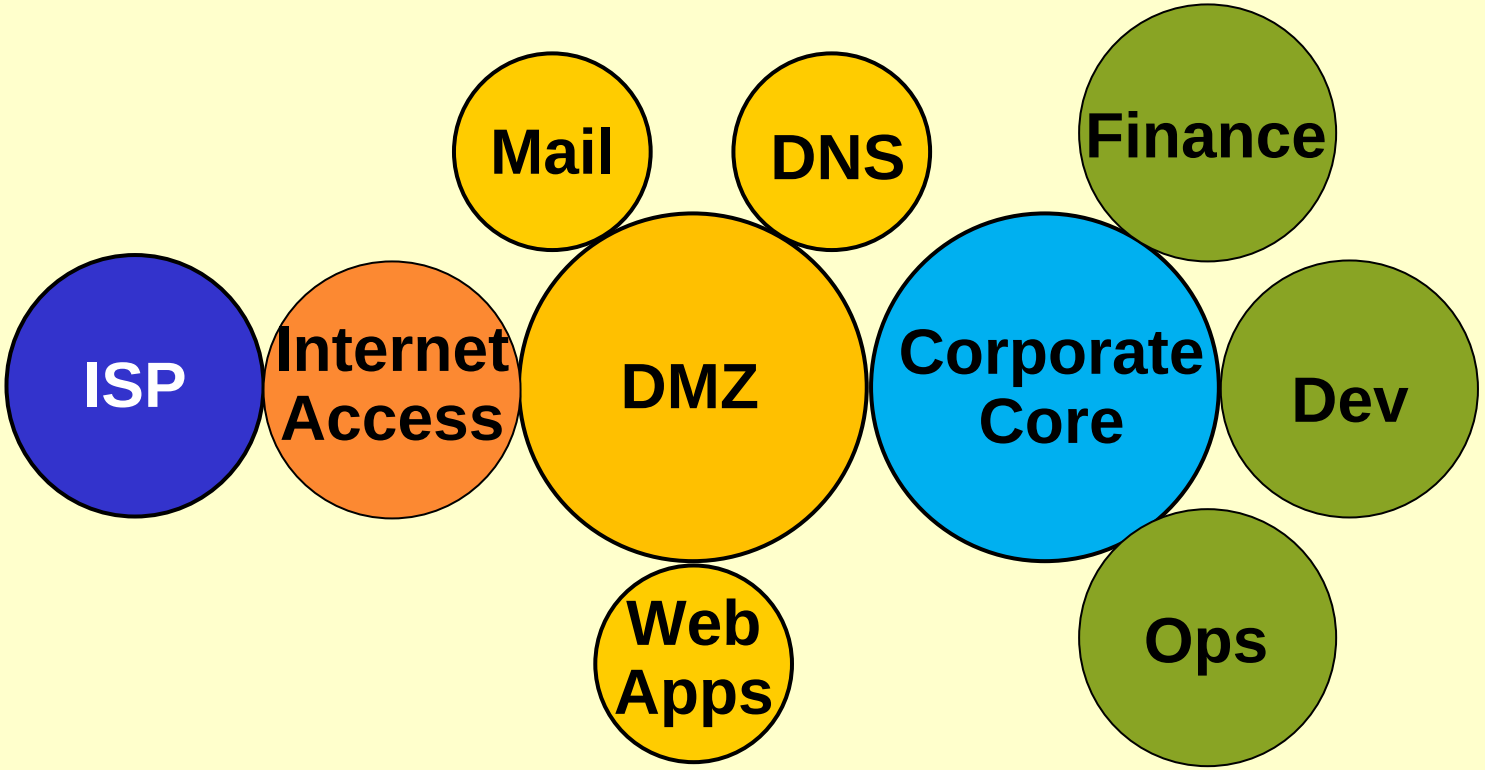


- Lesser gradient = low risk
- Basic safeguards
  - Basic access control
  - Casual monitoring

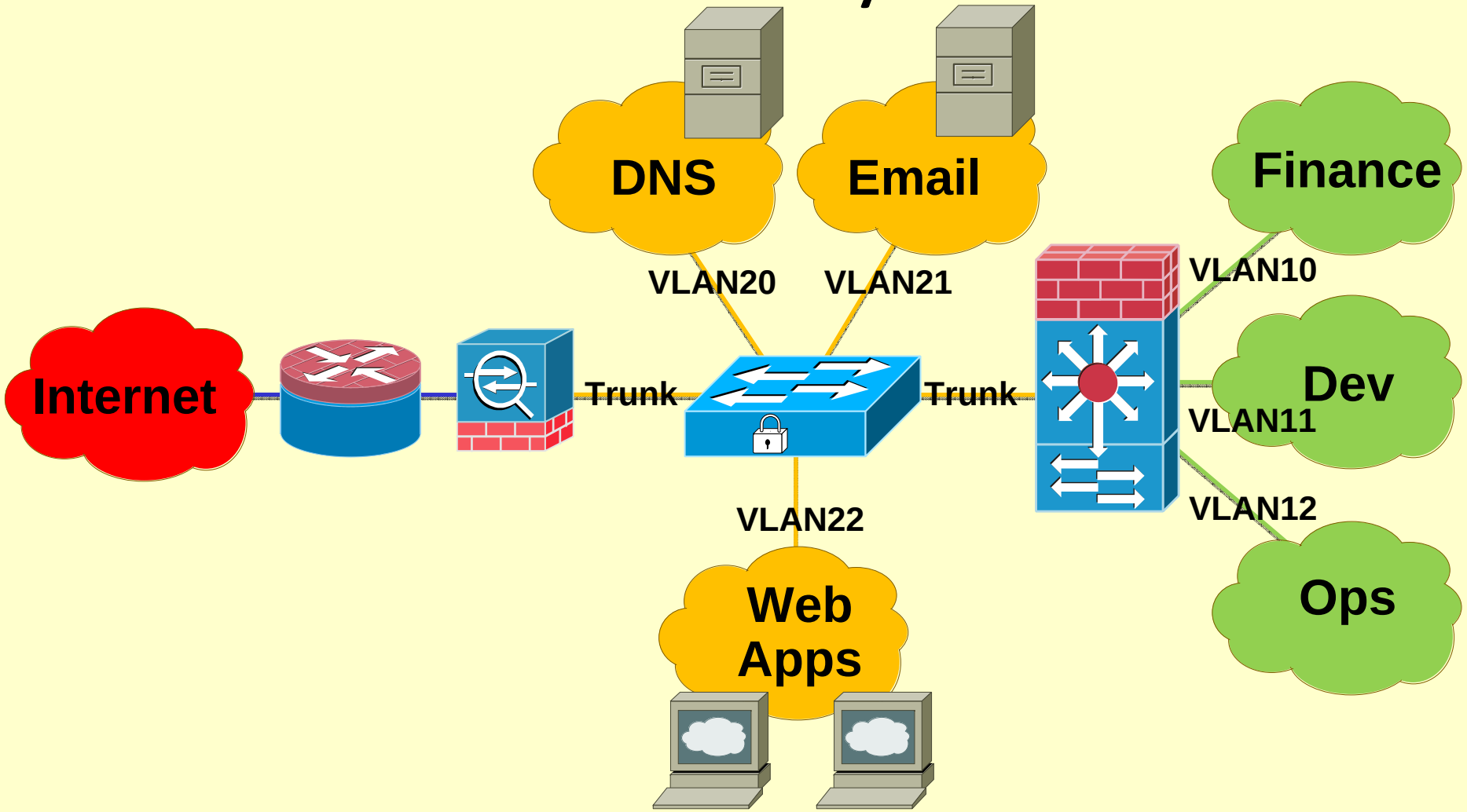


- Considerable safeguards between corporate and public
- Protect data transiting steep gradients
  - Communication security
  - Auth, confidentiality, integrity

Enterprise Security Zones—Logical



Enterprise Security Zones—Physical

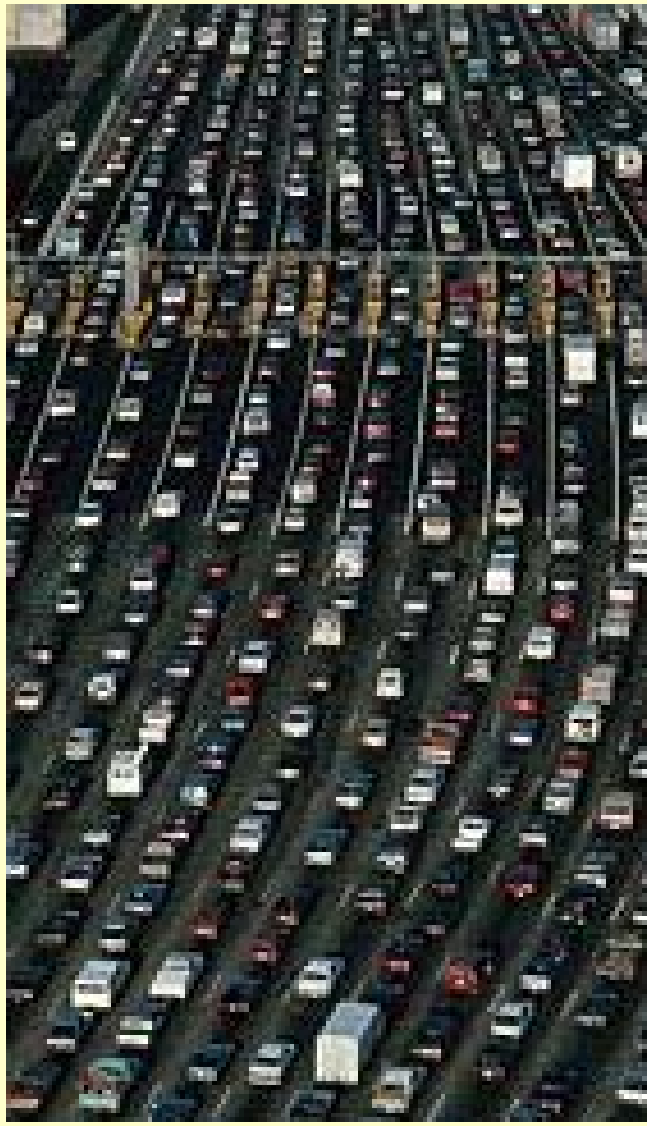


Filtering Network Traffic

Examining the flow of data (traffic) across a network

Types of flows:

- Packets
- Connections
- State



Il Firewall

- Per poter agire come un filtro il firewall ha la necessità di analizzare tutti i pacchetti che lo attraversano in modo da prendere una decisione conforme ad un set di regole definito dall'utente.
- In linea generale queste regole sono specificate in modo da comportare l'accettazione od il blocco dei pacchetti in transito sulla base di quelli che sono i loro elementi distintivi, vale a dire indirizzo IP e porta della sorgente nonché indirizzo IP e porta della destinazione.
- Tuttavia dal punto di vista del funzionamento interno i firewall possono essere ulteriormente distinti in due gruppi separati:
  1. firewall a filtraggio di pacchetti;
  2. firewall a livello di circuito;
- I primi sono i più comuni ed anche i meno costosi: essi esaminano le informazioni contenute nella intestazione del pacchetto relativa al protocollo IP e le confrontano con il loro set di regole interno permettendone o bloccandone il transito.
- Al contrario i firewall a livello di circuito, molto più costosi, forniscono un livello di protezione più elevato poiché esaminano non soltanto l'intestazione ma anche il contenuto dei pacchetti in transito.
  - Questo meccanismo di funzionamento viene anche detto "**stateful packet inspection**" proprio perché l'esame del contenuto del datagramma è diretto a verificare lo stato della comunicazione in corso e, quindi, ad assicurare che il sistema di destinazione abbia effettivamente richiesto la comunicazione stessa.
  - In questo modo c'è la garanzia che tutte le comunicazioni si svolgano soltanto con indirizzi sorgente effettivamente conosciuti per effetto di precedenti interazioni.

Il Firewall

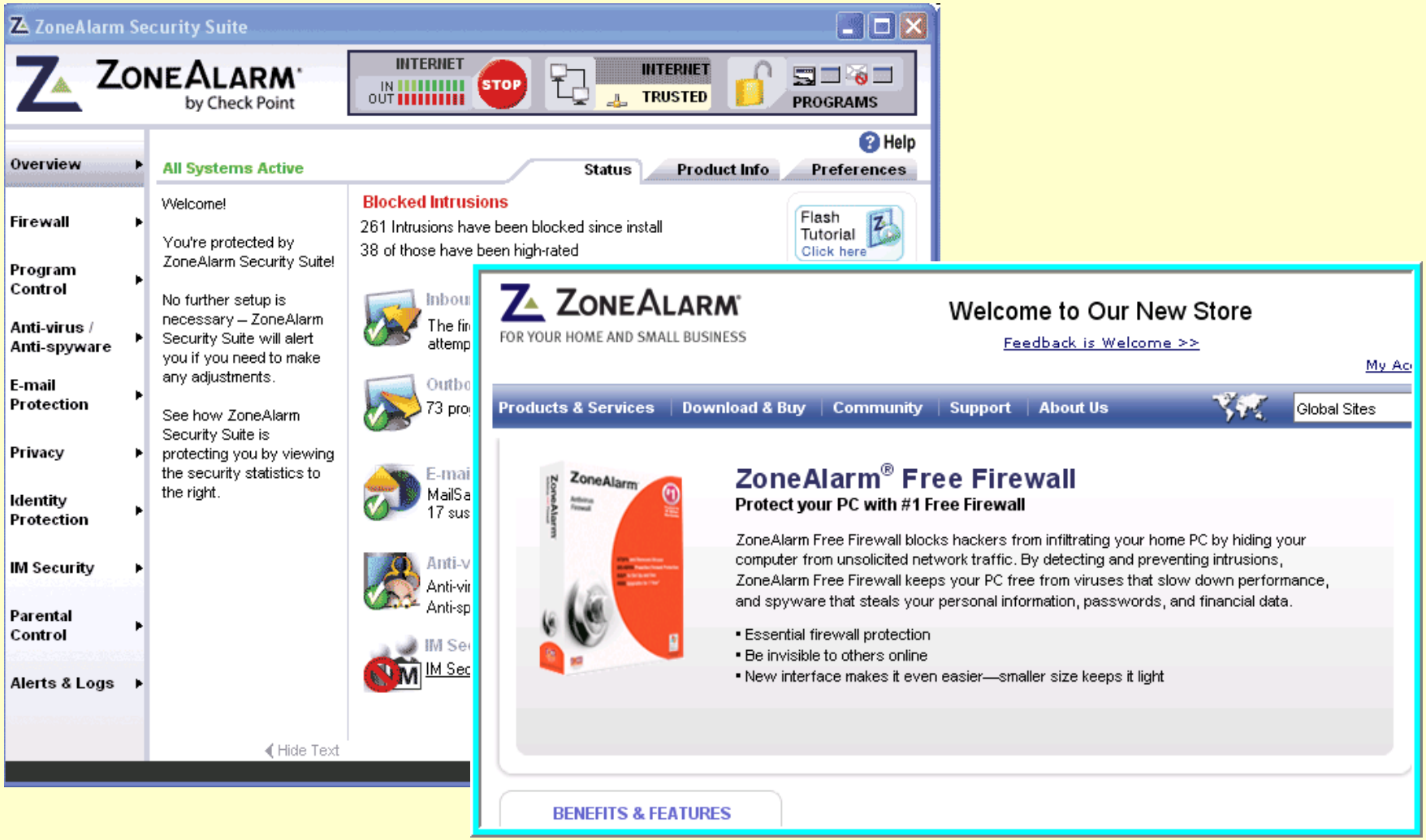
- I firewall non sono dispositivi "autonomi" nel senso che devono essere **istruiti** nel prendere decisioni in merito alla ammissibilità del traffico in transito attraverso delle regole ben precise definite dall'utente.
- La predisposizione di questo set di regole può richiedere una fase di **studio ed implementazione** più o meno lunga e laboriosa a seconda di quali siano effettivamente le esigenze di difesa che si pongono nel caso specifico ma, in ogni caso, il fulcro dell'intero funzionamento di questi dispositivi sta proprio nella loro corretta configurazione.
- Essere in possesso del prodotto software più evoluto sul mercato non è di alcuna utilità se lo stesso prodotto non può essere utilizzato nella pienezza delle sue funzionalità proprio a causa di una cattiva configurazione.
- In questi casi anzi è molto meglio rinunciare all'utilizzo di un firewall perché lo stesso può ingenerare un falso senso di sicurezza in chi lo utilizza.

Il Firewall

http://www.pctools.com/it/firewall/

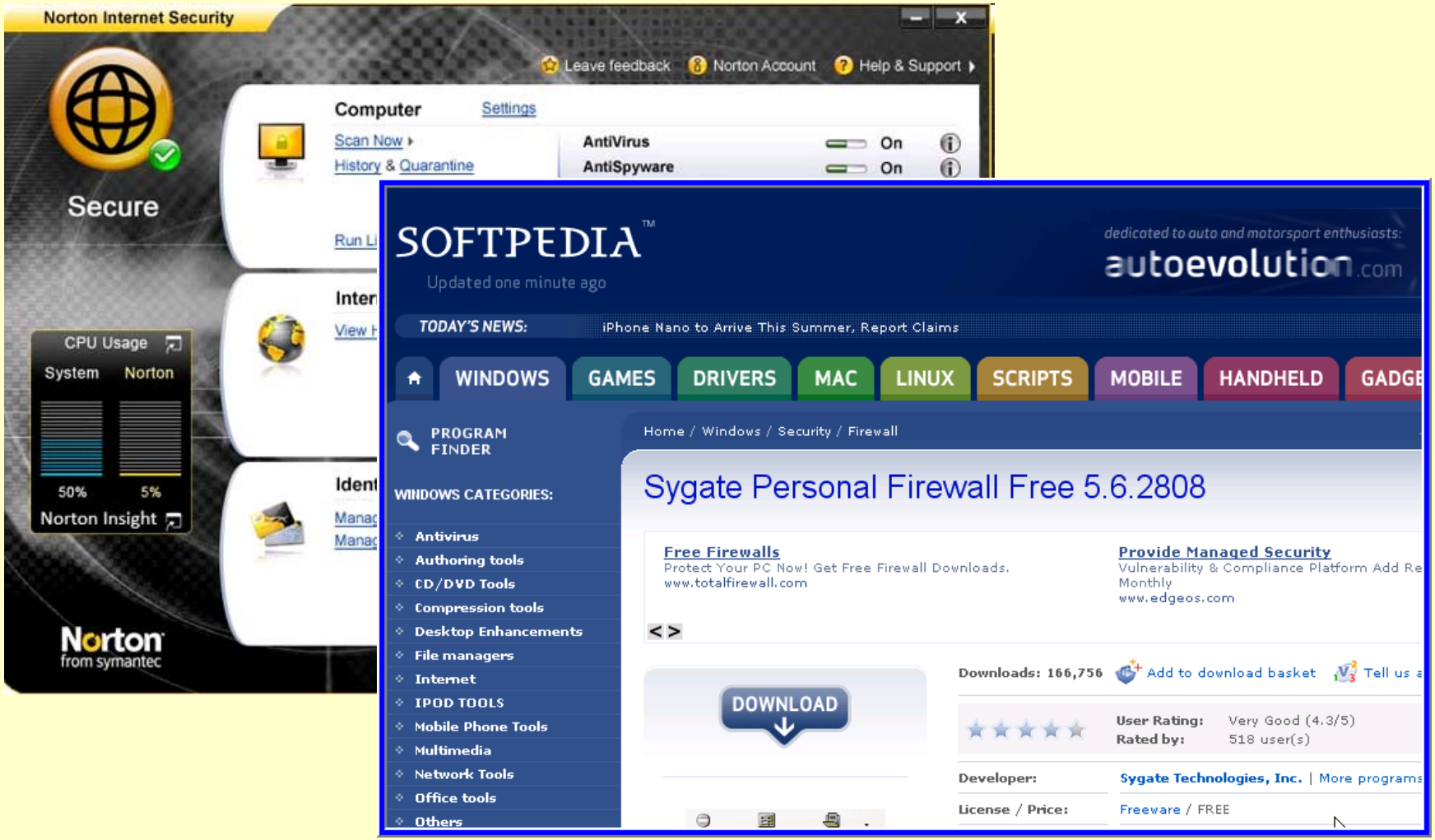
Il Firewall

http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm



Il Firewall

http://www.softpedia.com/get/Security/Firewall/Sygate-Personal-Firewall-Free.shtml



Identity Services

Trust

The Root of Security

Trust: A relationship in which two (or more) network entities are allowed to communicate

Trust forms the root of all security policy decisions

Trust and risk are opposites; security is based on enforcing limitations to trust relationships

Trust relationships:

- Can be explicit or implied
- Can be inherited
- Can be abused

Identity

Users and Organizations

Identity: The “who” of a trust relationship

Can be individuals, machines, organizations, or all three

Credentials: Pieces of information used to verify the identity of a network entity

Most common identity credential: Passwords

Identity and Authentication … Are Important?

User Identity

Mechanisms for proving who you are

- Both people and devices can be authenticated

Three authentication attributes:

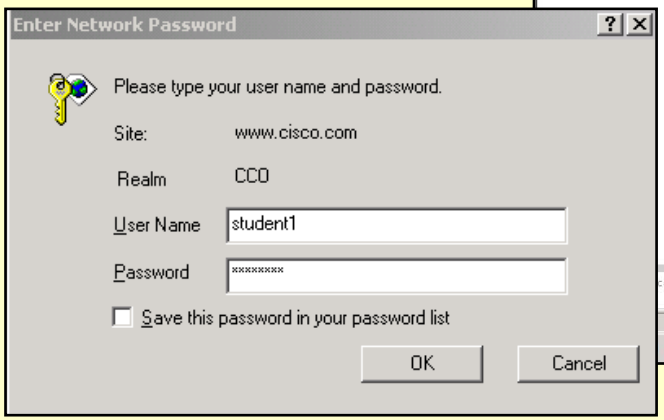
- **Something you know**
- **Something you have**
- **Something you are**

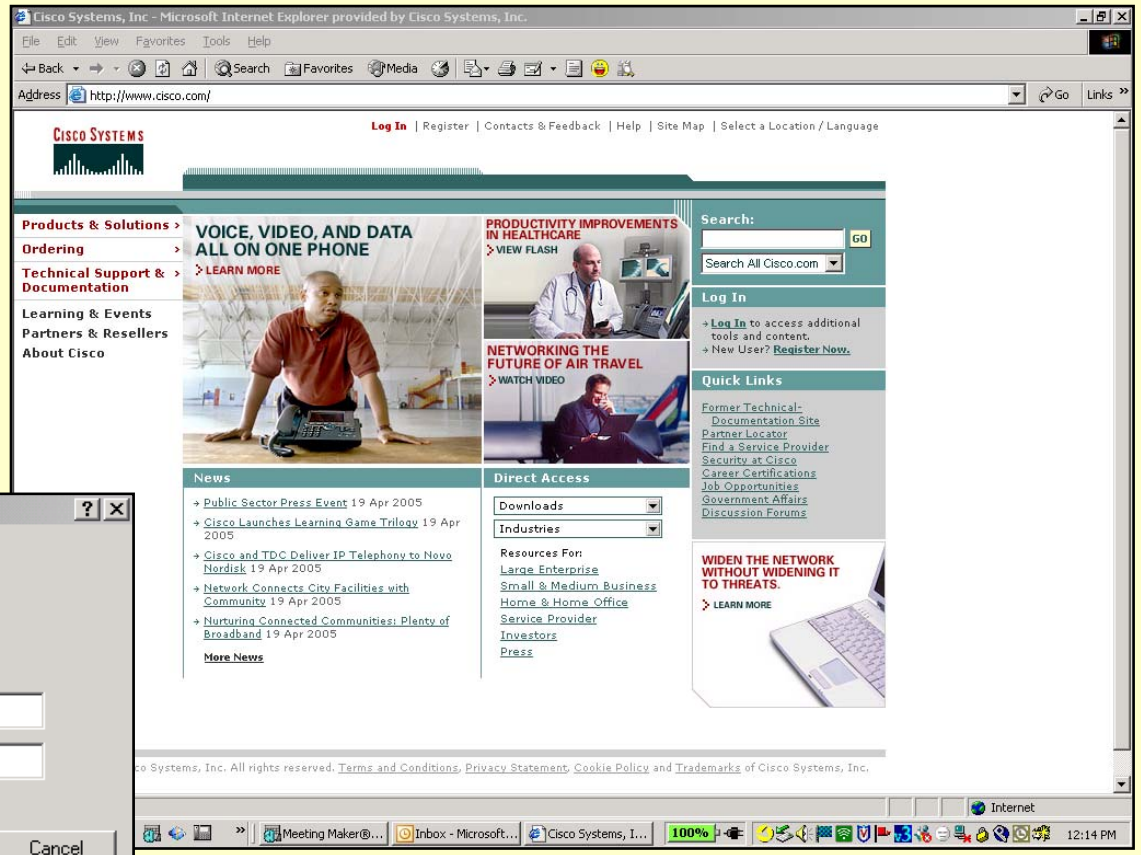
Common approaches to identity:

- Passwords
- Tokens
- Certificates (bio)

Passwords

Correlates an authorized user with network resources





Passwords

Passwords have long been, and will continue to be a problem

People will do what is easiest

Create and enforce good password procedures

- Non-dictionary passwords
- Changed often (90–120 days)

Passwords are like underwear—they should be changed often, never shared and neither hung from your monitor or hidden under your keyboard

Tokens

Strong (two-factor) authentication based on “something you know” and “something you have”

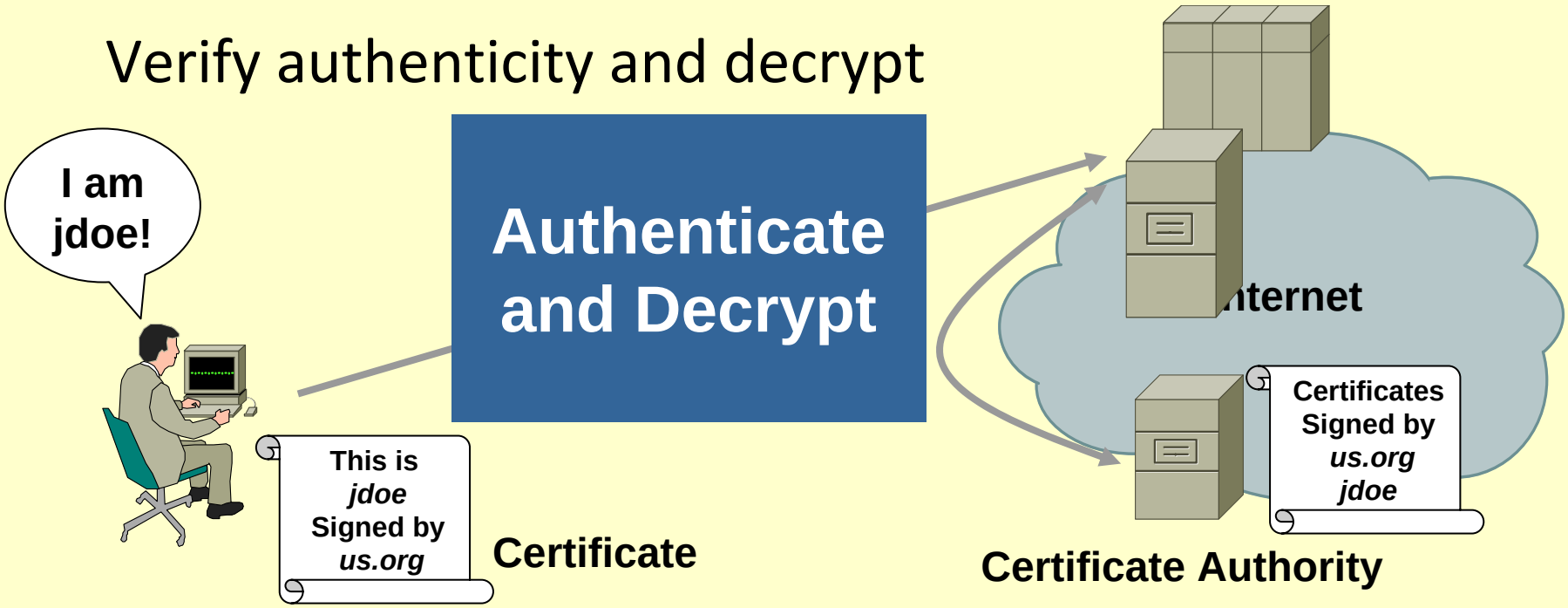
Public Key Infrastructure (PKI)

Relies on a Two Key System

J Doe signs a document with his private key

Person who receives that document uses JDoe's public key to:

Verify authenticity and decrypt

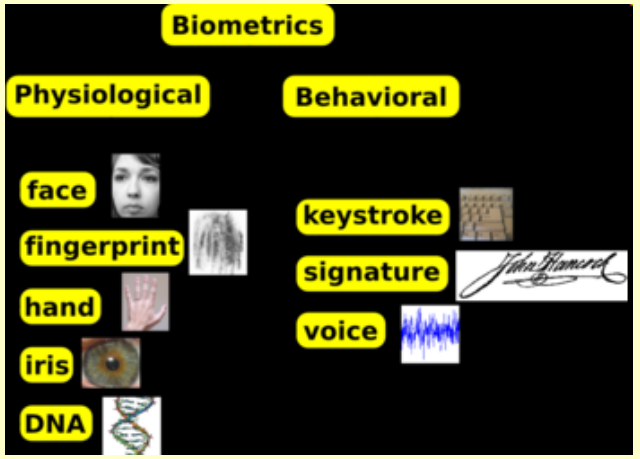


Biometrics

Authentication based on physiological or behavioral characteristics

Features can be based on:

- Face
- Fingerprint
- Eye
- Hand geometry
- Handwriting
- Voice



Becoming more accepted and widely used

Already used in government, military, retail, law enforcement, health and social services, etc.