

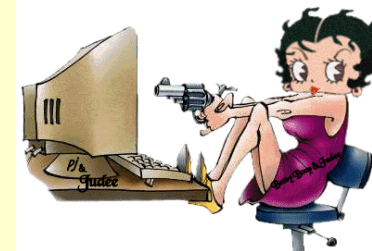


HACKER  
Cracked on 12/25/85  
by Mr. Clean

The Bank 303-771-7531



One more Virus Alert  
or Hacker and  
MySpace Is Gone!



## 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](http://www.eicar.org) e scaricare il file di prova EICAR.COM.  
[http://www.eicar.org/anti\\_virus\\_test\\_file.htm](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.

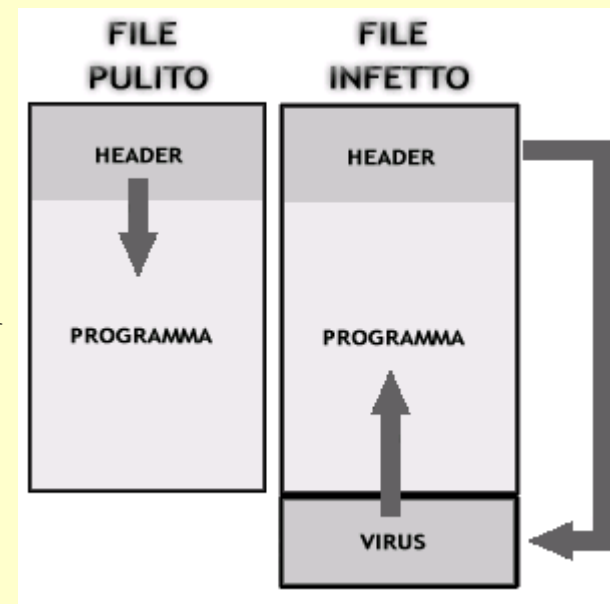
# “Impronte” Digit



- 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 alla 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.







# 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](http://www.lavasoft.com/products/ad_aware_free.php)

The image shows a screenshot of the Ad-Aware 2008 Free software interface. The window title is "Ad-Aware 2008". The interface is in Italian and features a sidebar on the left with navigation buttons: "Stato", "Scansione", "Ad-Watch", "Aggiornamento Web", "Strumenti e plug-in", and "Impostazioni". The main area displays the "Scansione in corso" (Scanning in progress) status. It includes a progress bar for "Avanzamento generale scansione" and "Avanzamento sezione". Below this, it shows the current section being scanned: "Sezione corrente: Scanning Hosts file", "Percorso corrente: 84.252.149.80 southtrus", and "Oggetto corrente: 84.252.149.80 southtrus". A "Dettagli scansione" (Scan details) section lists: "Modalità scansione selezionata: Scans. intelligente", "File delle definizioni: 0143.0012", "Totale oggetti analizzati: 93169", "Totale infezioni rilevate: 0", "Oggetti ignorati: 0", and "Ora scansione: 00:01:24".

Overlaid on the bottom right is a promotional banner for "Ad-Aware 2008 Free". The banner features the text: "The world's most popular anti-spyware!", "Protect yourself against identity theft, online fraud, and other cyber crimes with the world's most popular anti-spyware.", and a large green "Download" button. Below the banner, there are navigation tabs for "Overview", "Features", "Tech Specs", and "Screenshots". A mouse cursor is pointing at the "Features" tab. At the bottom of the banner, it says: "We believe every computer user has the right to protect their private information. We give you that right for free - no strings attached! Safeguard your personal information against cyber threats with the" and a "MOST TRUSTED ANTI-SPYWARE" award seal.

# Spy-ware

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

The image shows the Spybot - Search & Destroy 1.6.0 application window and a screenshot of its website. The application window has a menu bar (File, Mode, Language, Help) and a sidebar with icons for Search & Destroy, Recovery, Immunize, Update, and Donations. The main area features a 'Check for problems' button and a description: 'Use this button to start scanning your system for spyware and all other threats detected by Spybot - Search & Destroy.'

The website screenshot shows the 'Home' page with a search bar, navigation links (Home, Supporto, Prodotti), and a list of products:

Product Name	Version
Spybot - Search & Destroy® Proteggiti dallo spyware	1.6.0
RunAlyzer® Mostra tutti i punti in cui il malware tenta di nascondersi	1.6.0.21
FileAlyzer® Riconoscere i file dall'analisi della loro struttura	1.6.0.4
RegAlyzer® Sfoggia e ricerca nel registro	1.6.0.12

The website also includes a 'Gamma delle individuazioni raddoppiata negli ultimi sei mesi' section dated 3. December 2008, and a 'Prodotti' section with links to 'collegamento'.

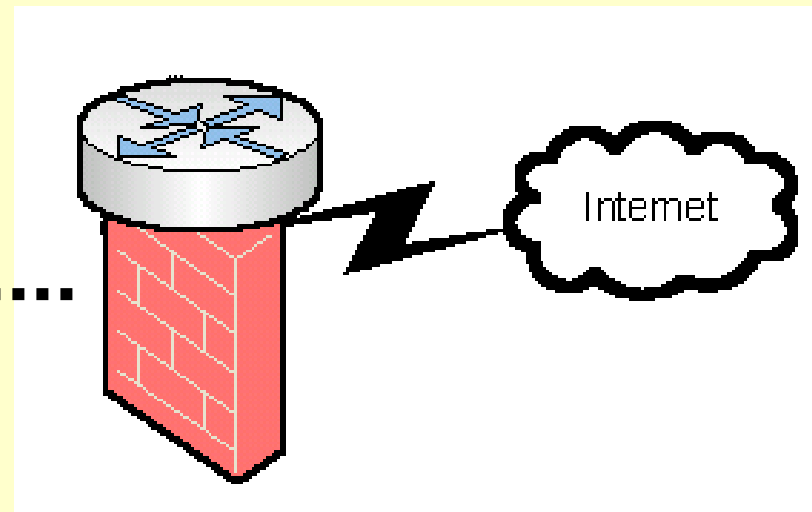
# Patch di sicurezza

<http://secunia.com/>

The screenshot shows the Secunia Personal Software Inspector (PSI) application window. The title bar reads "Secunia PSI". The main window has a blue header with the text "Secunia Personal Software Inspector" and "INTERFACE MODE: SIMPLE | ADVANCED". Below the header is a navigation menu with tabs: Overview, Insecure, End-of-Life, Patched, Scan, Settings, Secunia Profile, and Help / Support / Forum. The main content area is divided into two columns. The left column displays a greeting "Good morning, <unregistered user>" and a warning: "4 programs are insecure/end-of-life and expose you to security threats. To secure your PC, follow the advice given on the Insecure and End-of-Life tabs." Below this, it shows the "Secunia System Score" as 96%, the "Last Full System Scan" as "3 days ago", and the "State of Programs" as: 0 Insecure, 4 End-of-Life, and 91 Patched, with a total of 95. The right column is titled "Program Overview (right now)". At the bottom, there is a "Historic Development" section with a bar chart showing the system score over time (Week 48, Week 49, and Week 50). A footer note states: "Secunia respects your privacy, please read our [privacy statement](#)."

The screenshot shows the Secunia website homepage. The header features the Secunia logo with the tagline "Stay Secure" and a search bar. Below the header is a navigation menu with links: Vulnerability Intelligence, Vulnerability Scanning, Community, Blog - new entry!, Corporate Information, Online Shop, and Customer Login. The main content area is divided into several sections. The "Welcome to Secunia.com" message is at the top. Below it are four main content blocks: "Vulnerability Database" (covering all products and vulnerabilities, 26,414 advisories published to date, and the latest intelligence, with a "Secunia Advisories" button), "In-depth Analysis" (detailed analysis of vulnerabilities, proof of concept and exploit code, and restricted to certain companies and organisations, with a "Binary Analysis" button), "Secunia Research Team" (vulnerabilities discovered by Secunia Research, disclosure policy, and the team, with a "Secunia Research" button), and "Scan Your PC" (online, personal, and network scanning for missing patches, used by more than 120,000 users every day, and Secunia OSI, PSI, and NSI solutions, with a "Software Inspectors" button). On the right side, there is a "Secunia News" section with three news items: "14th Jan, 2009: The best new Wi program of 2008 [more](#).", "9th Jan, 2009: Monthly Binary & Update. [Read m](#)", and "17th Dec, 2008: Secunia PSI: ¡He español! [Read th](#) [download today](#).". At the bottom, there is a "12th Dec, 2008: Internet Explore Binding 0-Day Clarifications. [R](#)".

# 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)

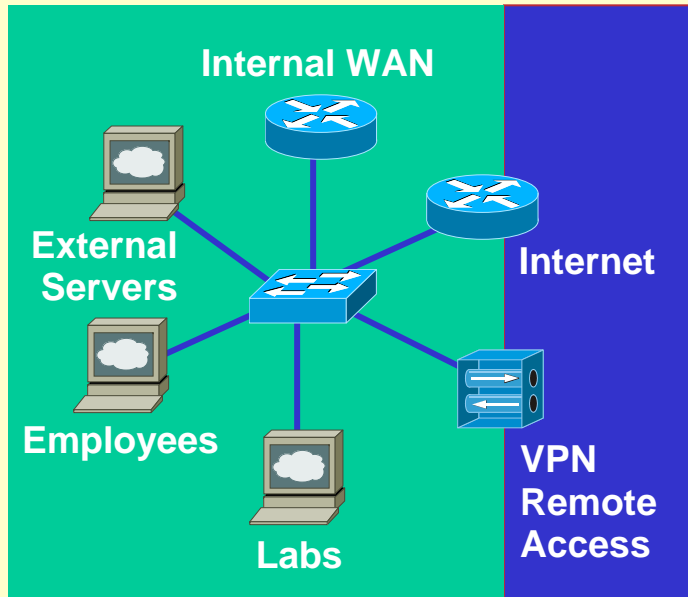


# Firewall

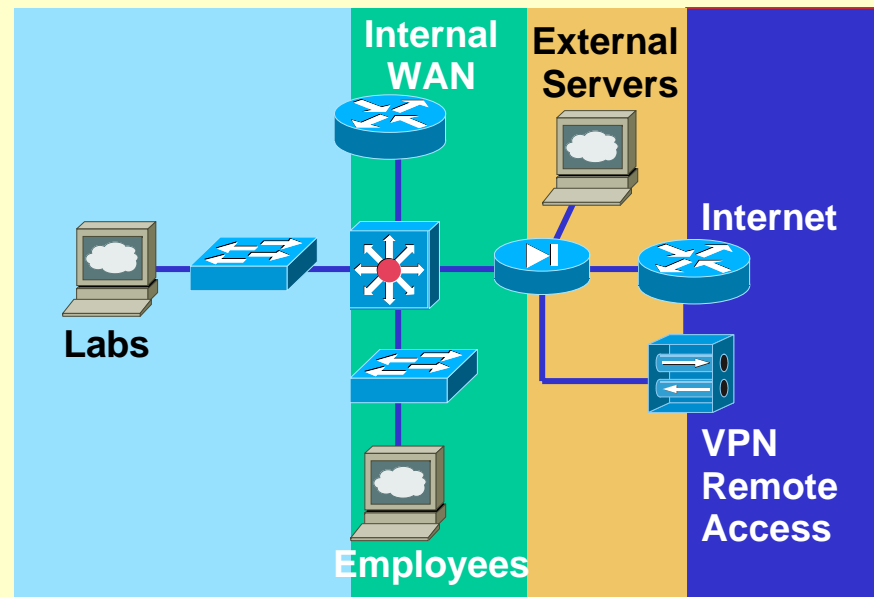
- termine inglese dal significato originario di parete refrattaria, muro tagliafuoco', "muro ignifugo"; in italiano anche parafuoco o parafiamma
- è un componente passivo di difesa perimetrale che può anche svolgere funzioni di collegamento tra due o più tronconi di rete.
- Usualmente la rete viene divisa 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**



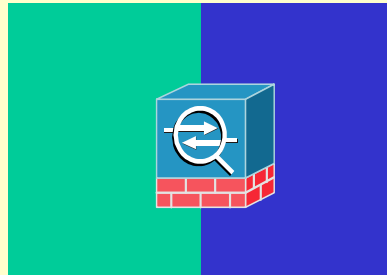
**2ndcase.com**



**Domains of Trust segment communities by policy**

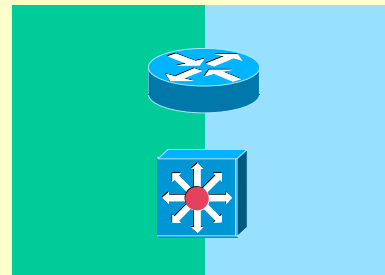
# Sample Domains of Trust

Private    Public



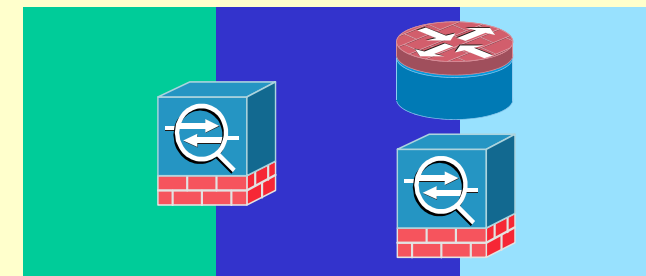
- Steep gradient = high risk
- Considerable safeguards
  - Advanced Firewalling
  - Flow-based inspection
  - Misuse detection (IPS)
  - Constant monitoring

Production    Lab



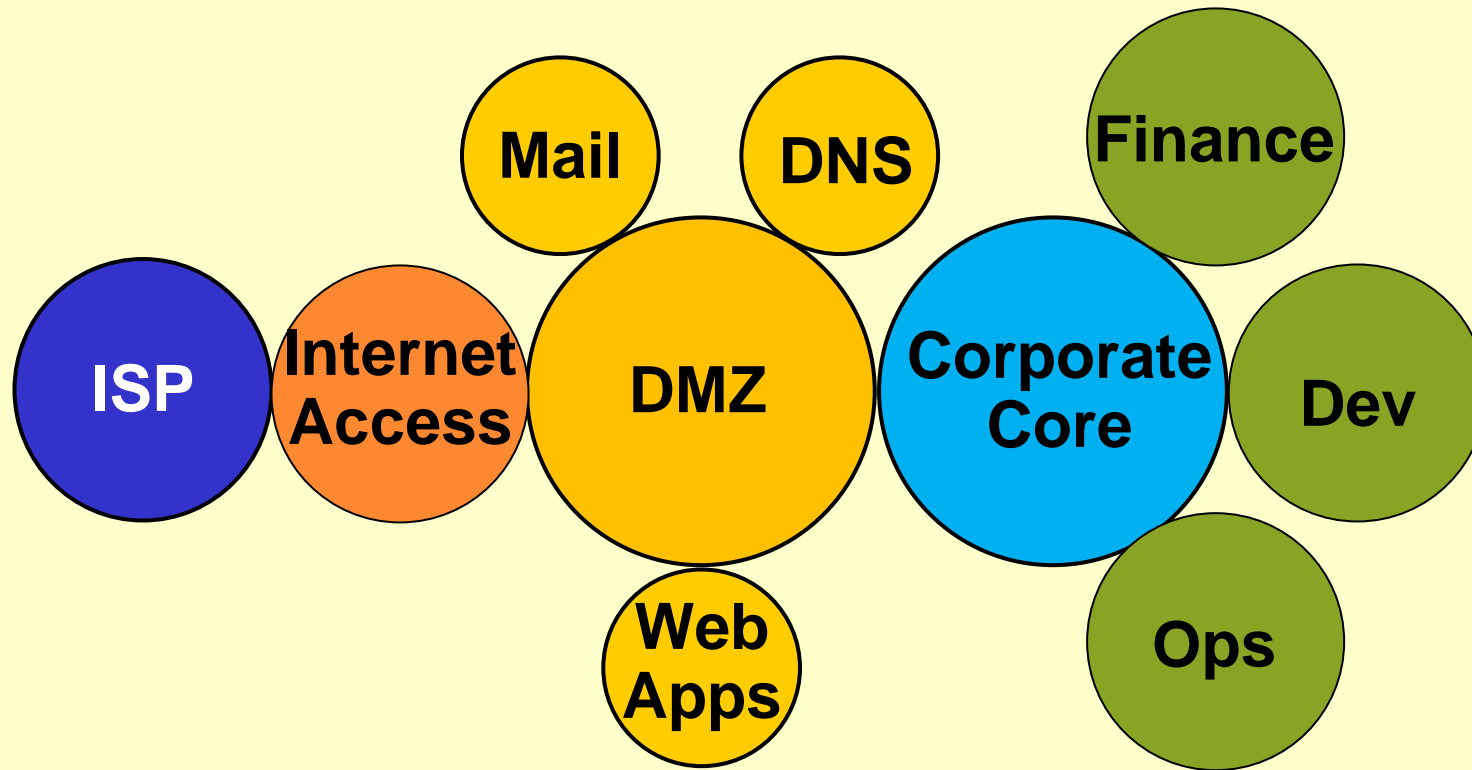
- Lesser gradient = low risk
- Basic safeguards
  - Basic access control
  - Casual monitoring

HQ    Public    Branch

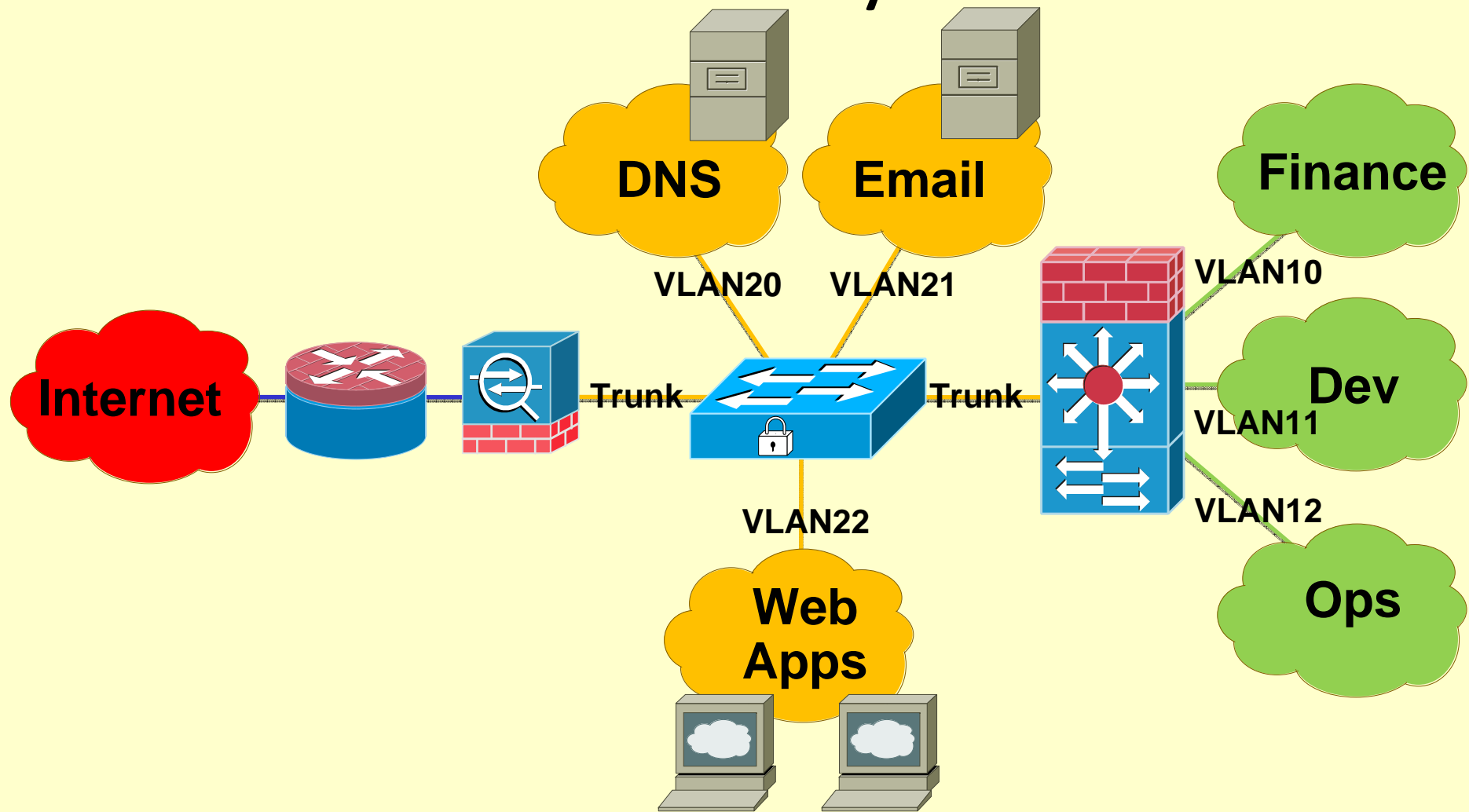


- Considerable safeguards between corporate and public
- Protect data transiting steep gradients
  - Communication security
  - Auth, confidentiality, integrity

# Enterprise Security Zones—Logical



# Enterprise Security Zones— Physical



# Filtering Network Traffic

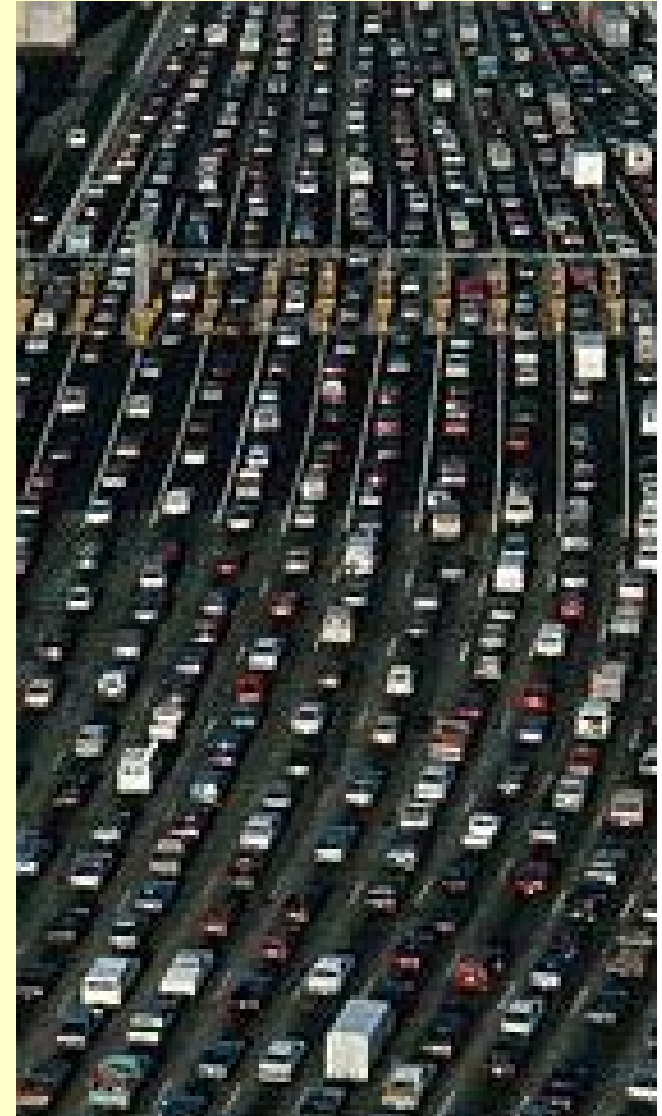
Examining the flow of data  
(traffic) across a network

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/>

The screenshot shows the PC Tools Firewall Plus application window. The title bar reads "PC Tools Firewall Plus" and includes "Smart Update" and "Guida" buttons. The main interface is titled "Seleziona un'azione" and features three primary options: "La protezione del firewall è ON" (Firewall protection is ON), "Blocco applicazione" (Application blocking), and "Regole avanzate" (Advanced rules). A left sidebar contains navigation buttons for "Stato", "Applicazioni", "Regole avanzate", "Cronologia", "Attività", "Impostazioni", and "Aggiorna ora". The "Stato/Riepilogo" section at the bottom left displays product version 4.0.0.44, confirms it is updated, and notes the last update was today. It also mentions a free edition and provides an "aggiorna ora" link.

This is a promotional page for PC Tools Firewall Plus. It features the "pctools" logo at the top left and a navigation menu with "Home", "Download", "Funzionalità", "Registra", and "Supporto". The main heading is "PC Tools Firewall Plus" with a globe icon. Below this, it specifies "PC Tools Firewall Plus™ 5 per Windows®". The text describes it as a "Firewall gratuito e intuitivo che consente di proteggere i PC da intrusioni e traffico di rete dannoso." A prominent green button with a right-pointing arrow says "Avvia il download GRATUITO ora!". At the bottom, it lists compatibility: "Progettato per Windows® Vista™ 32-bit, XP, 2000 e 2003 Server". A small product box image is visible on the left side of the page.

# II Firewall

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

**ZoneAlarm Security Suite**

**ZONEALARM**  
by Check Point

INTERNET IN OUT STOP

INTERNET TRUSTED

PROGRAMS

Overview **All Systems Active** Status Product Info Preferences Help

**Firewall** Welcome!

**Program Control** You're protected by ZoneAlarm Security Suite!

**Anti-virus / Anti-spyware** No further setup is necessary – ZoneAlarm Security Suite will alert you if you need to make any adjustments.

**E-mail Protection** See how ZoneAlarm Security Suite is protecting you by viewing the security statistics to the right.

**Privacy**

**Identity Protection**

**IM Security**

**Parental Control**

**Alerts & Logs**

**Blocked Intrusions**  
261 Intrusions have been blocked since install  
38 of those have been high-rated

Flash Tutorial  
Click here

**ZONEALARM**  
FOR YOUR HOME AND SMALL BUSINESS

Welcome to Our New Store  
[Feedback is Welcome >>](#) [My Account](#)

Products & Services | Download & Buy | Community | Support | About Us | Global Sites

**ZoneAlarm® Free Firewall**  
**Protect your PC with #1 Free Firewall**

ZoneAlarm Free Firewall blocks hackers from infiltrating your home PC by hiding your computer from unsolicited network traffic. By detecting and preventing intrusions, ZoneAlarm Free Firewall keeps your PC free from viruses that slow down performance, and spyware that steals your personal information, passwords, and financial data.

- Essential firewall protection
- Be invisible to others online
- New interface makes it even easier—smaller size keeps it light

**BENEFITS & FEATURES**

# II Firewall

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

The image displays two overlapping screenshots. On the left is the Norton Internet Security software interface, showing a 'Secure' status with a green checkmark, a 'Computer' section with 'AntiVirus' and 'AntiSpyware' both turned 'On', and a 'CPU Usage' widget showing 50% for System and 5% for Norton. On the right is a screenshot of the Softpedia website. The website header includes the Softpedia logo and the text 'dedicated to auto and motorsport enthusiasts: autoevolution.com'. The main content area is titled 'Sygate Personal Firewall Free 5.6.2808' and features a large 'DOWNLOAD' button. Below the button, it shows 'Downloads: 166,756', a star rating of 4.3/5, and the developer 'Sygate Technologies, Inc.'. A sidebar on the left of the website lists various software categories like 'Antivirus', 'Games', and 'Drivers'.

# 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

**Enter Network Password**

Please type your user name and password.

Site: www.cisco.com

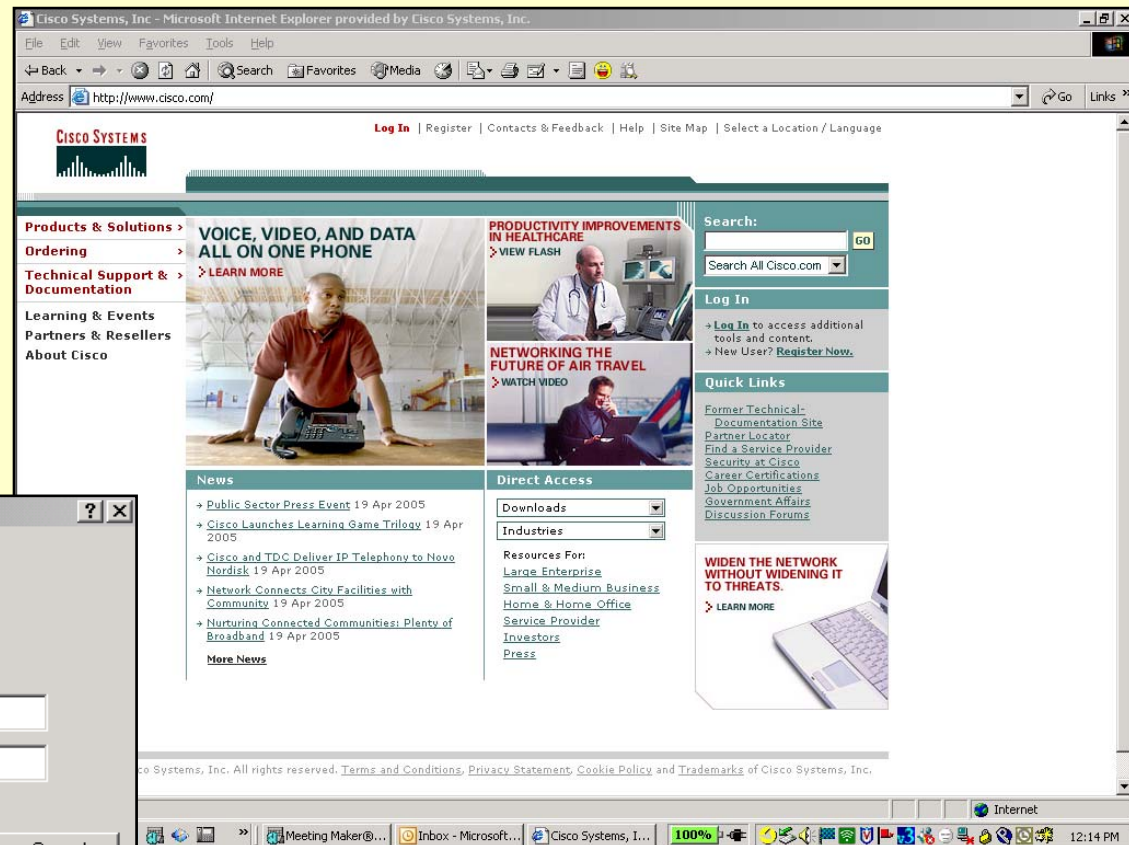
Realm: CCO

User Name: student1

Password: \*\*\*\*\*

Save this password in your password list

OK Cancel



# 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”



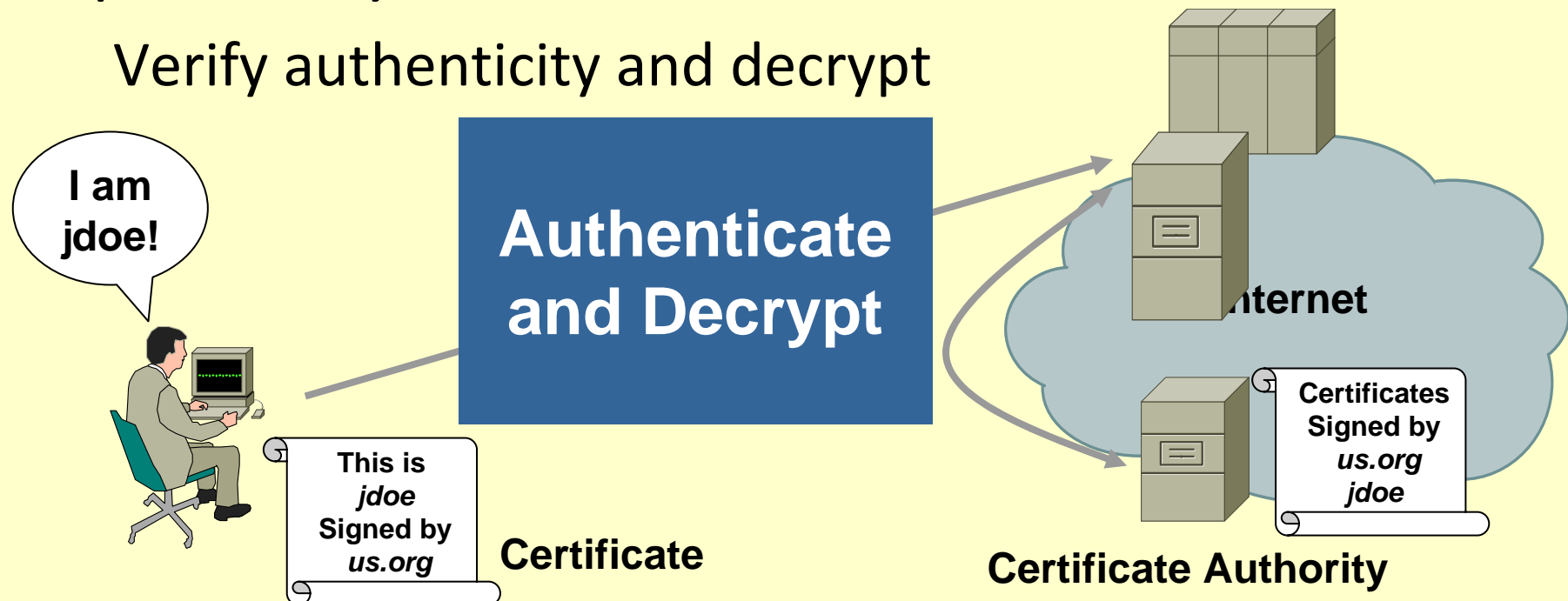
# Public Key Infrastructure (PKI)

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

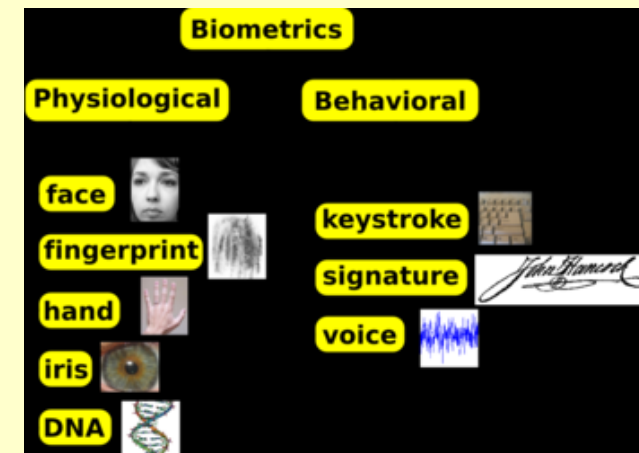
Fingerprint

Eye

Hand geometry

Handwriting

Voice



Becoming more accepted and widely used

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