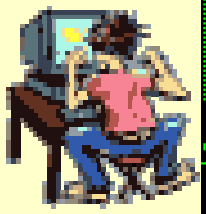


Sicurezza e Internet 04

Alcune statistiche recenti

- For the 13th year, CSI has asked its community how they were affected by network and computer crime in the prior year and what steps they've taken to secure their organizations.
- 522 security professionals responded.

CSI COMPUTER SECURITY INSTITUTE http://www.gocsi.com/

2008

CSI Computer Crime & Security Survey

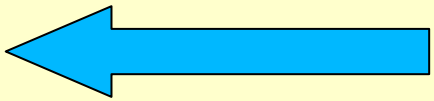
The latest results from the longest-running project of its kind

By Robert Richardson, CSI Director

For the 13th year, CSI has asked its community how they were affected by network and computer crime in the prior year and what steps they've taken to secure their organizations. Over 500 security professionals responded. Their answers are inside…

La Sicurezza

Gli argomenti inerenti la sicurezza sono generalmente raggruppabili all'interno delle seguenti aree:

1. Sicurezza Fisica
2. Sicurezza Logica 
3. Sicurezza Organizzativa
4. Piano di Continuità Operativa

Servizi di Sicurezza

- sono le funzioni di sicurezza che il sistema dovrà garantire su tutte le piattaforme ed a tutti i livelli di elaborazione.
- ISO(*) individua i seguenti servizi di sicurezza:
  A. Autenticazione (reciproca)
  B. Controllo accessi
  C. Confidenzialità (riservatezza)
  D. Integrità
  E. Non ripudio

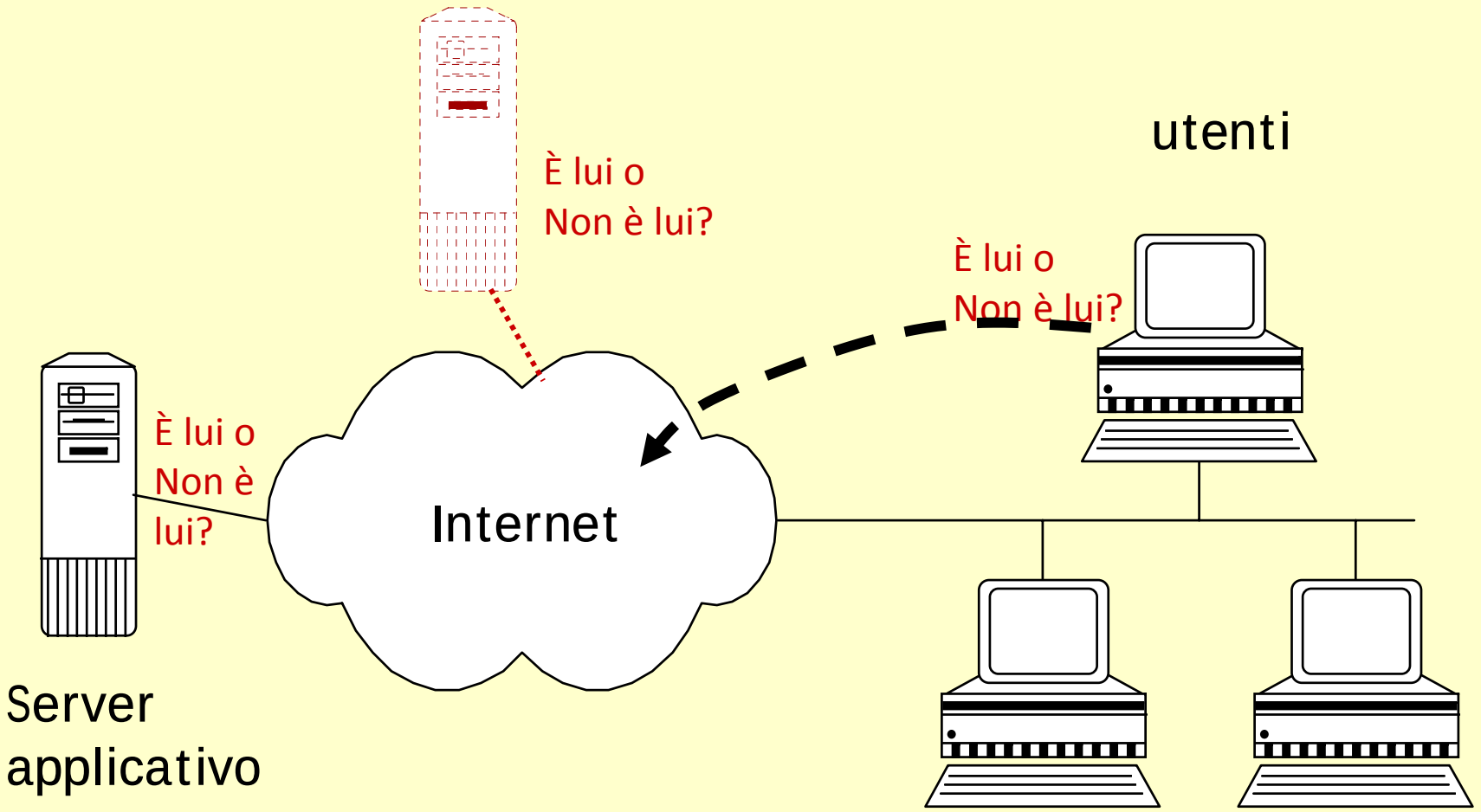
(*) ISO - *International Organization for Standardization*

Table 1.2 Security Services (X.800)

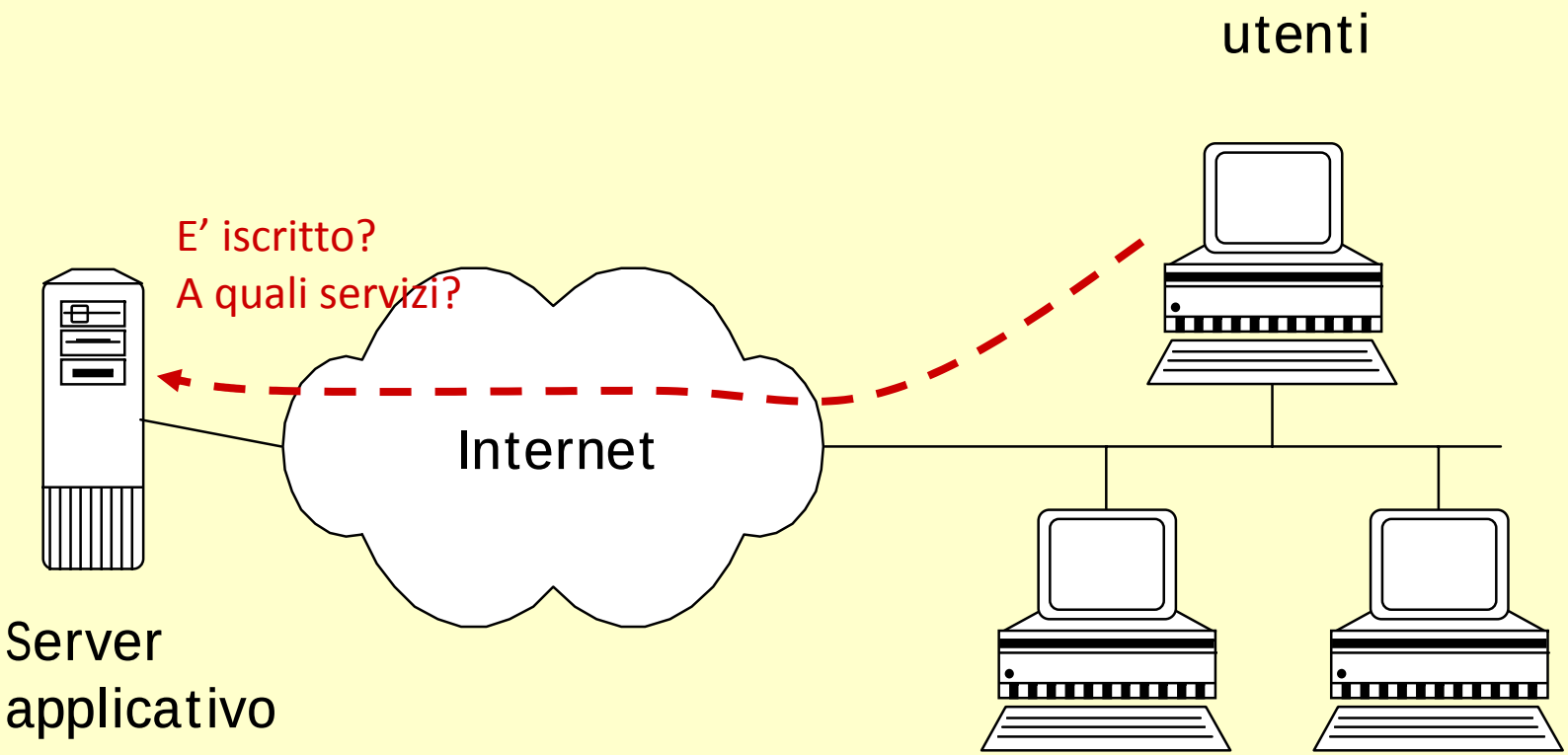
AUTHENTICATION The assurance that the communicating entity is the one that it claims to be. **Peer Entity Authentication** Used in association with a logical connection to provide confidence in the identity of the entities connected. **Data-origin Authentication** In a connectionless transfer, provides assurance that the source of received data is as claimed. **ACCESS CONTROL** The prevention of unauthorized use of a resource (i.e., this service controls who can have access to a resource, under what conditions access can occur, and what those accessing the resource are allowed to do). **DATA CONFIDENTIALITY** The protection of data from unauthorized disclosure. **Connection Confidentiality** The protection of all user data on a connection. **Connectionless Confidentiality** The protection of all user data in a single data block **Selective-Field Confidentiality** The confidentiality of selected fields within the user data on a connection or in a single data block. **Traffic-flow Confidentiality** The protection of the information that might be derived from observation of traffic flows.	**DATA INTEGRITY** The assurance that data received are exactly as sent by an authorized entity (i.e., contain no modification, insertion, deletion, or replay). **Connection Integrity with Recovery** Provides for the integrity of all user data on a connection and detects any modification, insertion, deletion, or replay of any data within an entire data sequence, with recovery attempted. **Connection Integrity without Recovery** As above, but provides only detection without recovery. **Selective-Field Connection Integrity** Provides for the integrity of selected fields within the user data of a data block transferred over a connection and takes the form of determination of whether the selected fields have been modified, inserted, deleted, or replayed. **Connectionless Integrity** Provides for the integrity of a single connectionless data block and may take the form of detection of data modification. Additionally, a limited form of replay detection may be provided. **Selective-Field Connectionless Integrity** Provides for the integrity of selected fields within a single connectionless data block; takes the form of determination of whether the selected fields have been modified. **NONREPUDIATION** Provides protection against denial by one of the entities involved in a communication of having participated in all or part of the communication. **Nonrepudiation, Origin** Proof that the message was sent by the specified party. **Nonrepudiation, Destination** Proof that the message was received by the specified party.

Più precisamente

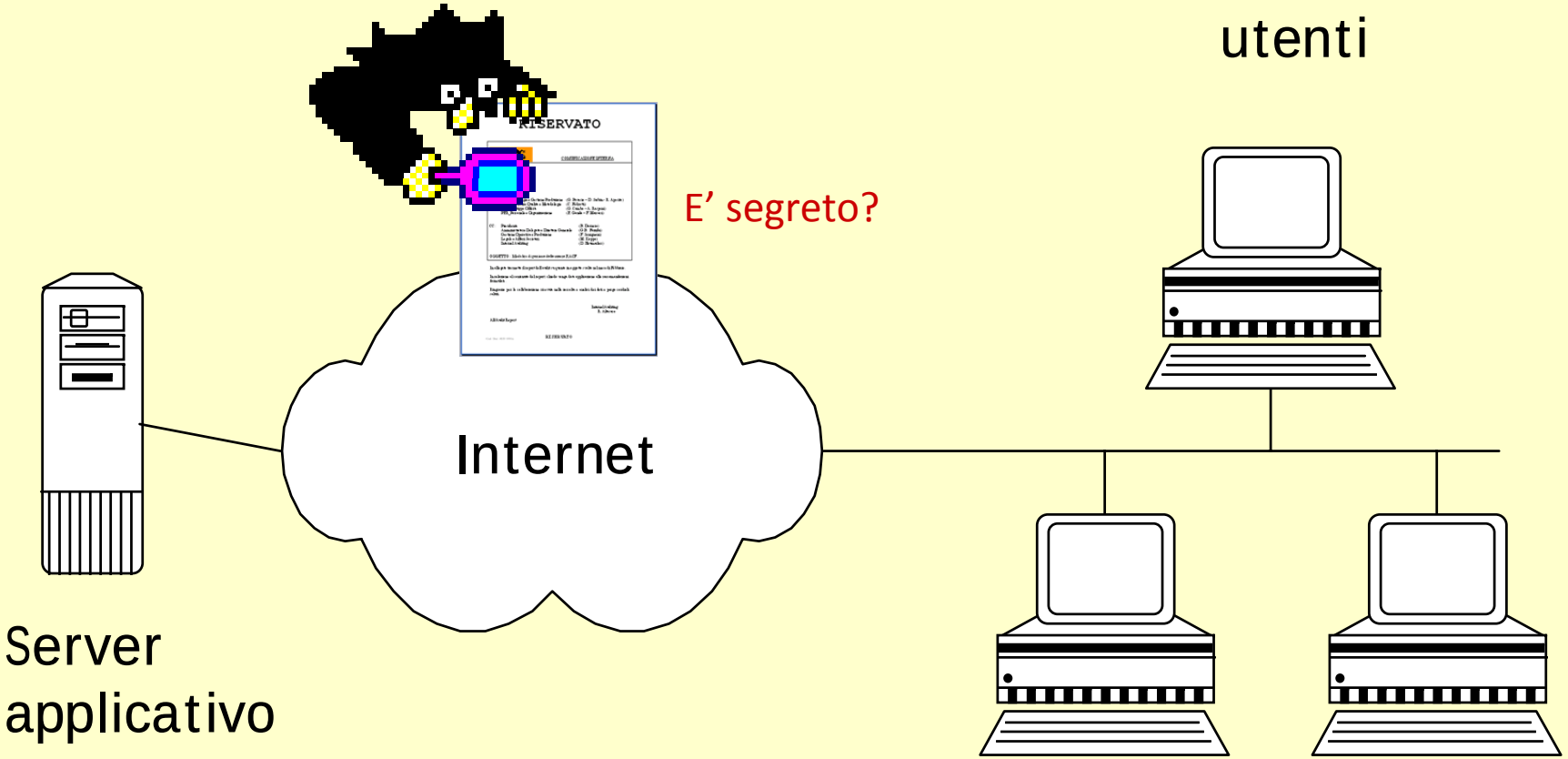
Autenticazione (reciproca)



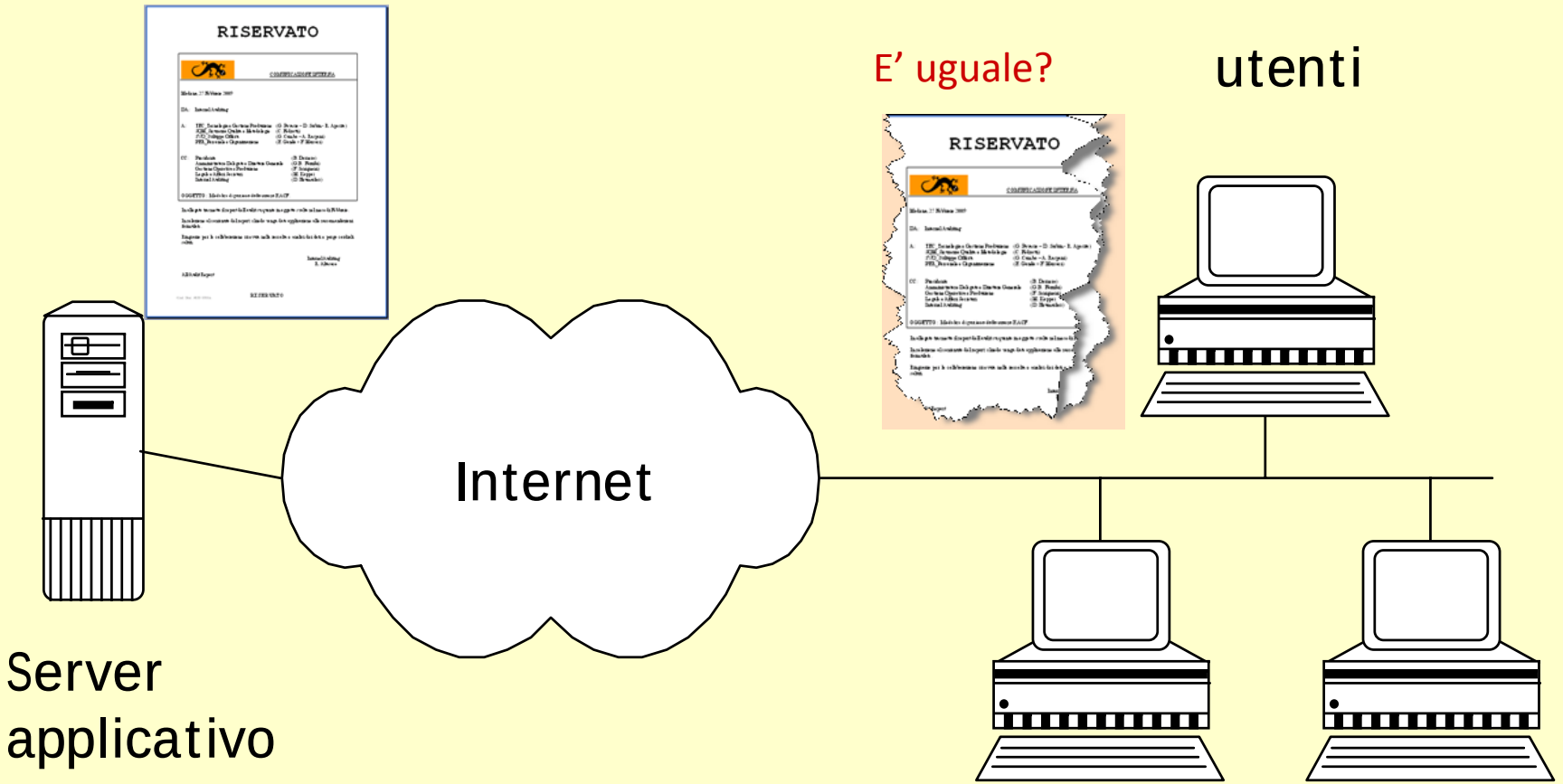
Controllo accessi



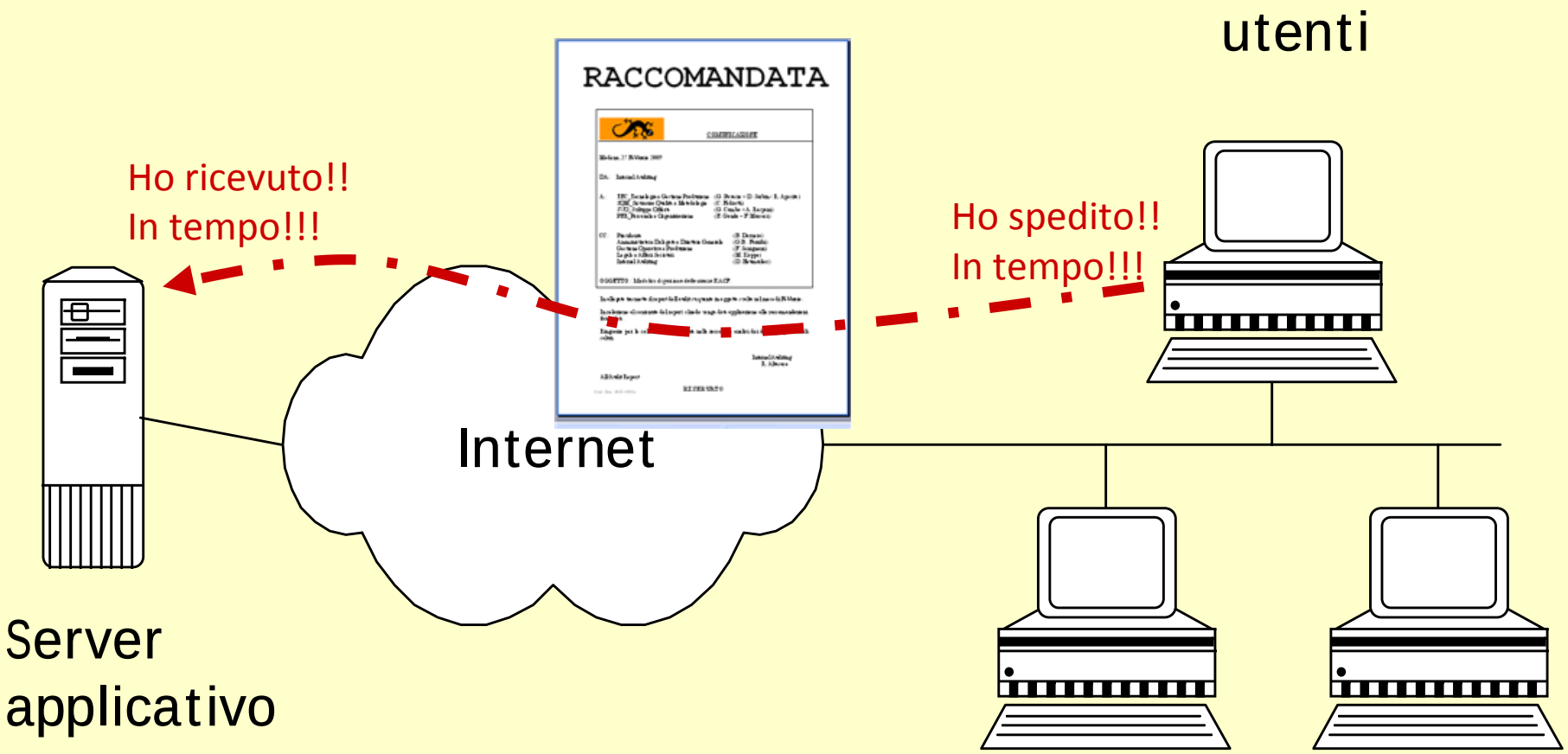
Confidenzialità (riservatezza)



Integrità


RISERVATO
E' uguale?
RISERVATO
utenti
Internet
Server
applicativo

Non ripudio


utenti
RACCOMANDATA
Ho ricevuto!!
In tempo!!!
Ho spedito!!
In tempo!!!
Internet
Server
applicativo

Meccanismi di Sicurezza

- rappresentano le modalità tecniche attraverso le quali è possibile realizzare i servizi di sicurezza.
- ISO individua (tra altri) i seguenti meccanismi di sicurezza:
  - Meccanismi per l'autenticazione (A)
  - Meccanismi per il controllo degli accessi (B)
  - Cifratura (crittografia)(C)
  - Firma digitale (D)
  - Notarizzazione (E)

Le relazioni servizi/meccanismi

Table 1.4 Relationship Between Security Services and Mechanisms

	Mechanism							
Service	**Encipherment**	**Digital signature**	**Access control**	**Data integrity**	**Authentication exchange**	**Traffic padding**	**Routing control**	**Notarization**
Peer entity authentication	Y	Y			Y			
Data origin authentication	Y	Y						
Access control			Y					
Confidentiality	Y						Y	
Traffic flow confidentiality	Y					Y	Y	
Data integrity	Y	Y		Y				
Non-repudiation		Y		Y				Y
Availability				Y	Y			


The 12 Layer Matrix
Building a Cyber Fortress
OCTAVE
Chief Security Officer
Policy Management Software
Proper Systems Administration
Firewall
Authentication
Incident Response Plan
Virus Scanners
Intrusion Detection Systems (IDS)
Cyber Intelligence
Encyrption
Active Content Filtering

Gli strumenti di base

1. Strumenti tecnologici
    1. Antivirus
    2. Adware, spyware, et similia
    3. Firewall
    4. …. Ed altro ancora (wifi)
2. Strumenti basati sulla identità
    1. What you know
    2. What you have
    3. What you are

Il funzionamento degli antivirus

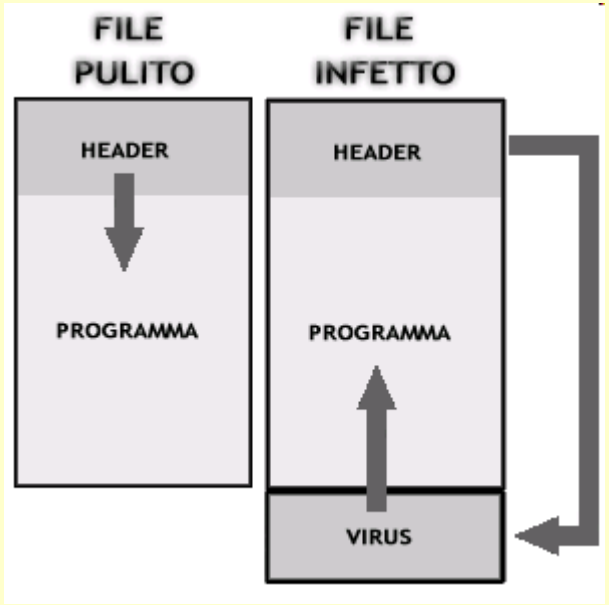
- Per controllarne l'effettiva attività è possibile navigare nel sito www.eicar.org e scaricare il file di prova EICAR.COM. http://www.eicar.org/anti_virus_test_file.htm
- Se il vostro antivirus lancerà un allarme non preoccupatevi, è tutto ok: non è infatti un vero virus, ma solo un file di prova che 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

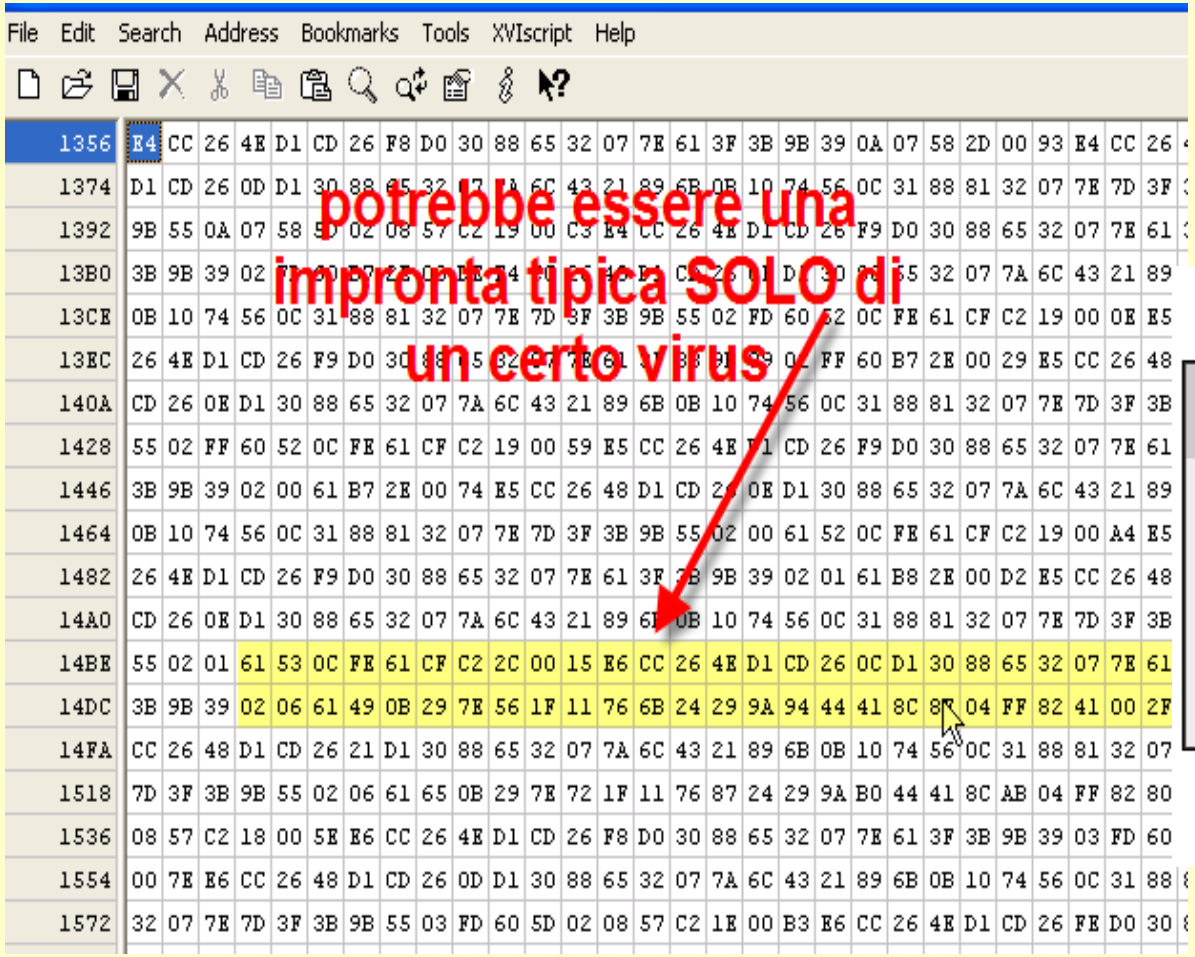
- "impronte" digitali
- tecnologia euristica.

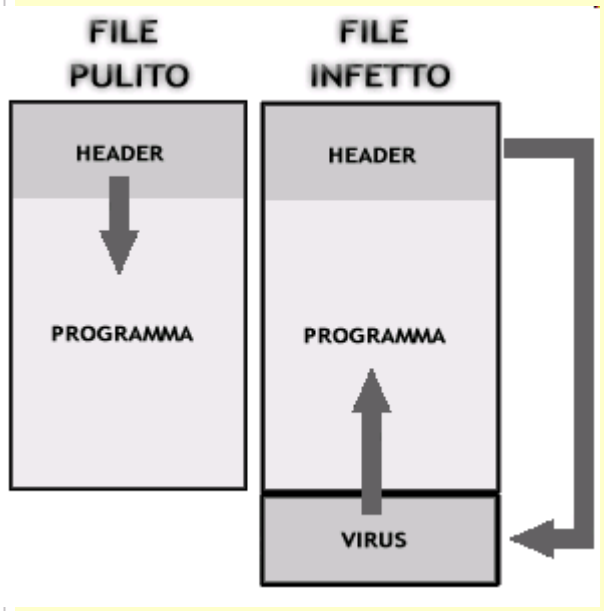
Come è fatto un malware

- 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

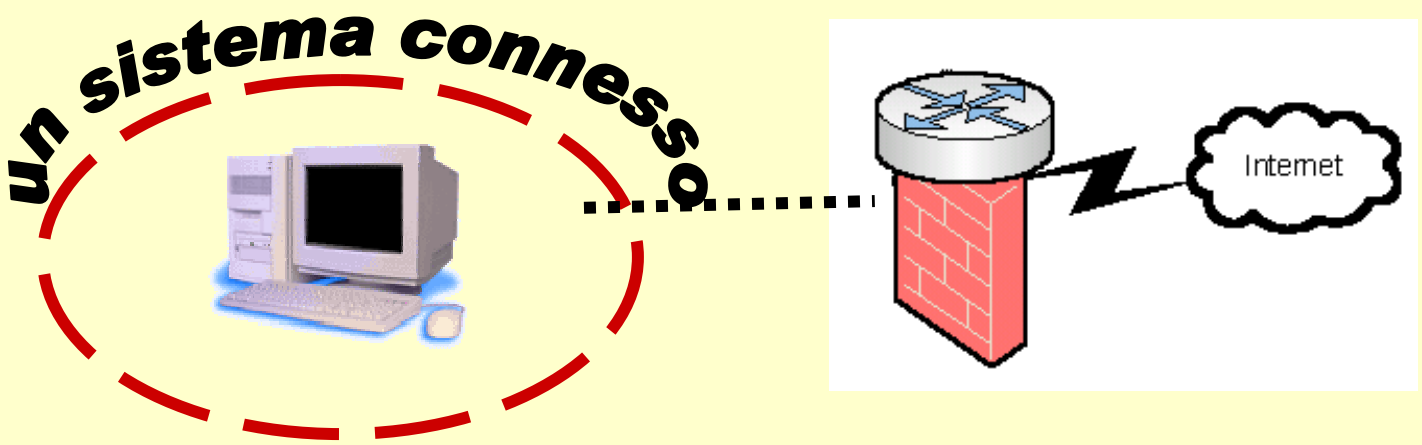
- Adware, che è una forma “innocua” di malware, il cui scopo consiste nel mostrare annunci pubblicitari e simili,
- Spyware, che invece viene scritto con lo scopo di sottrarre informazioni personali in modo illegittimo,
  - Insieme al proprio programma antivirus si raccomanda di usare un programma antispyware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

Il Decalog

Norme di sicurezza
Organizzativa
Enforced by policy

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.

Il Firewall



è un componente passivo di difesa perimetrale che può anche svolgere funzioni di collegamento tra due o più tronconi di rete.

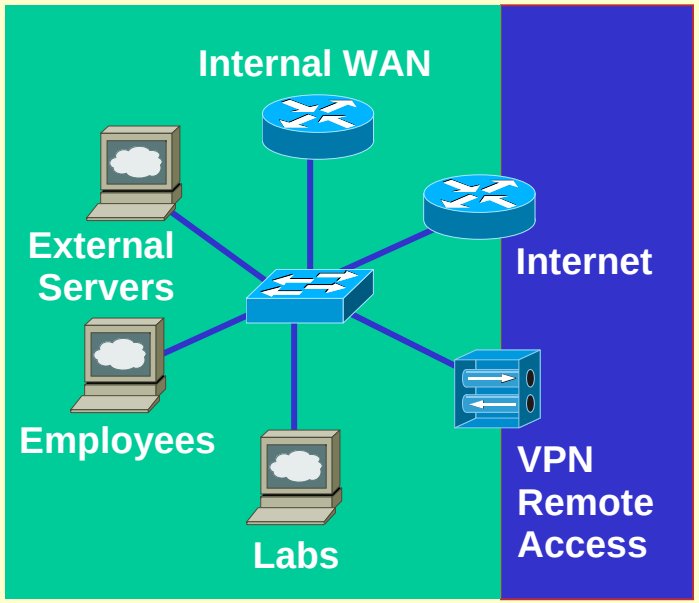
Usualmente la rete viene divisa in due sottoreti:

- una, detta esterna, comprende l'intera Internet (the wilderness)
- l'altra interna, detta LAN (Local Area Network),

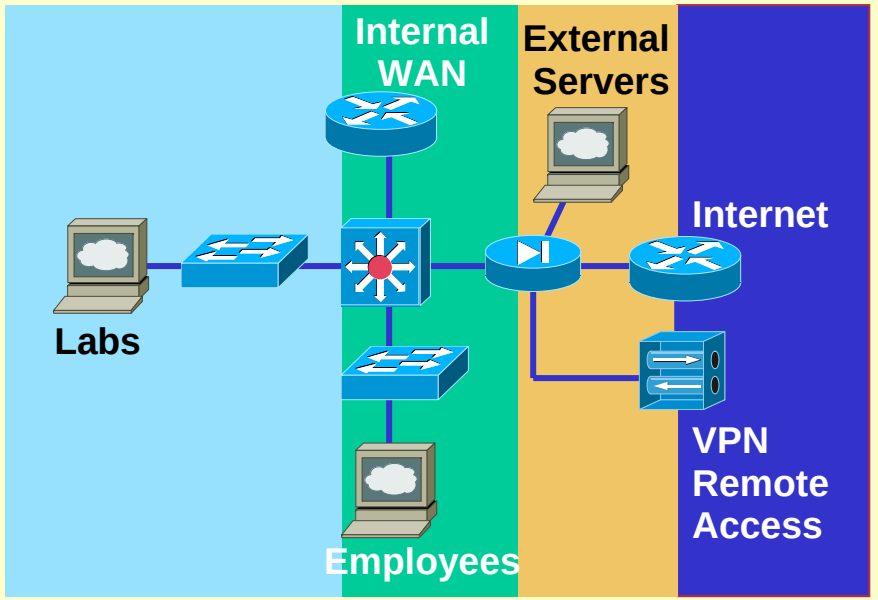
In alcuni casi si crea una terza sottorete detta DMZ (o zona demilitarizzata) atta a contenere quei sistemi che devono essere isolati dalla rete interna ma devono comunque essere protetti dal firewall

Domains of Trust (Zones)

1stcase.com



2ndcase.com

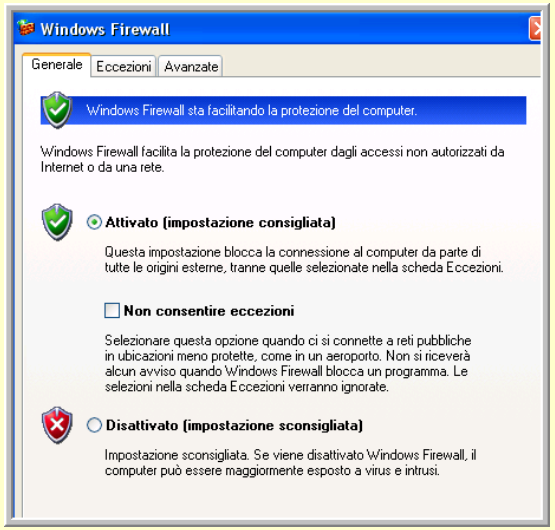


Domains of Trust segment communities by policy

Il Firewall

Oltre al firewall a protezione perimetrale ne esiste un secondo tipo, definito "Personal Firewall", che si installa direttamente sui sistemi da proteggere (per questo motivo è chiamato anche Firewall Software).

Windows è dotato in modo standard del firewall Microsoft, ma ne esistono molti altri anche gratuiti.



Il firewall è solo uno dei componenti di una strategia di sicurezza informatica, e non può in generale essere considerato sufficiente.
La sua configurazione è un compromesso tra usabilità della rete, sicurezza e risorse disponibili per la manutenzione della configurazione stessa (le esigenze di una rete cambiano rapidamente)

Tipologie di Firewall

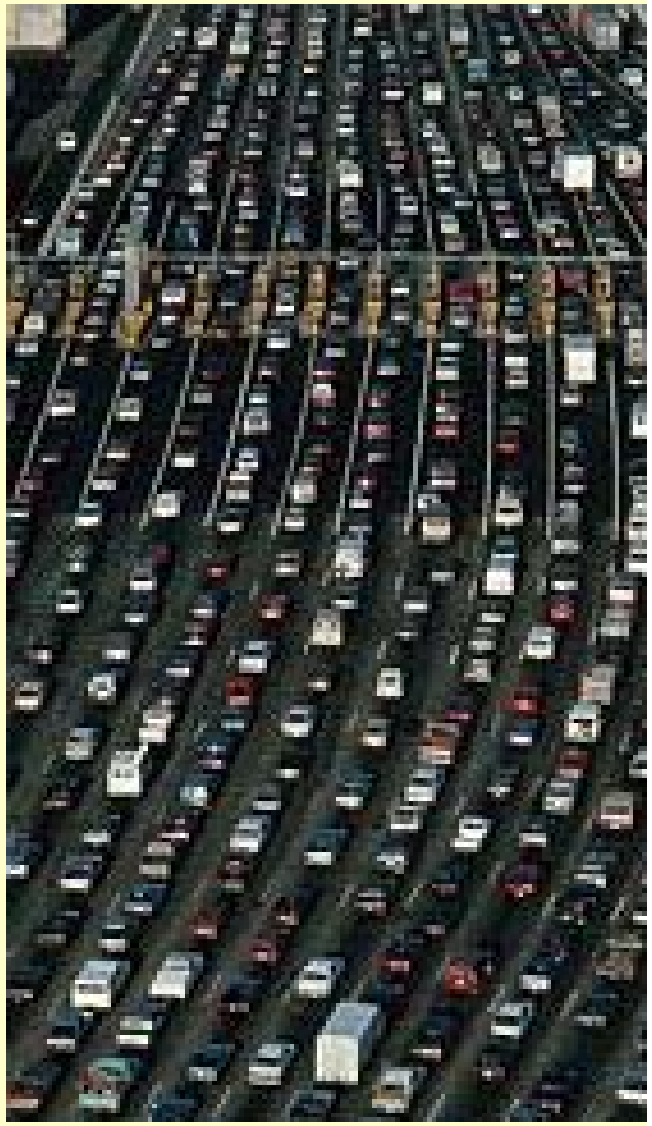
I. Il più semplice è il **packet filter**, che si limita a valutare gli header di ciascun pacchetto, decidendo quali far passare e quali no sulla base delle regole configurate. Ciascun pacchetto viene valutato solamente sulla base delle regole configurate, e per questo un firewall di questo tipo è detto anche **stateless**. "
II. Un firewall di tipo **stateful inspection**, tiene traccia di alcune relazioni tra i pacchetti che lo attraversano, ad esempio ricostruisce lo stato delle connessioni TCP. Questo permette ad esempio di riconoscere pacchetti TCP malevoli che non fanno parte di alcuna connessione.
III. I firewall di tipo **deep inspection** effettuano controlli fino al livello 7 della pila ISO/OSI, ovvero valutano anche il contenuto applicativo dei pacchetti, ad esempio riconoscendo e bloccando i dati appartenenti a virus o worm noti in una sessione HTTP o SMTP.
IV. I cosiddetti **Application Layer Firewall** sono apparati che intercettano le connessioni a livello applicativo. A questa categoria appartengono i proxy. In tali casi, la configurazione della rete privata non consente connessioni dirette verso l'esterno, ma il proxy è connesso sia alla rete privata che alla rete pubblica, e permette alcune connessioni in modo selettivo, e solo per i protocolli che supporta.

Filtering Network Traffic

Examining the flow of data (traffic) across a network

Types of flows:

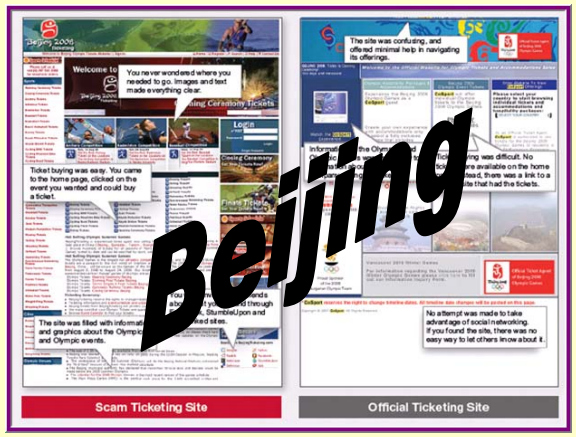
- Packets
- Connections
- State



Identity Services

I dubbi sulla identità

1. Mi collego ad un server, ma sono davvero collegato con il server che volevo?
2. Un utente si collega al mio server e si qualifica, ma è proprio lui oppure semplicemente ha indovinato la password?



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**

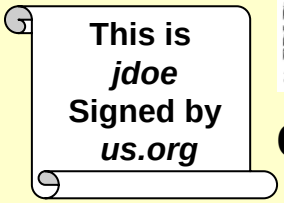
Both **people and devices** can be authenticated

Three authentication attributes:

Something you know

Something you have

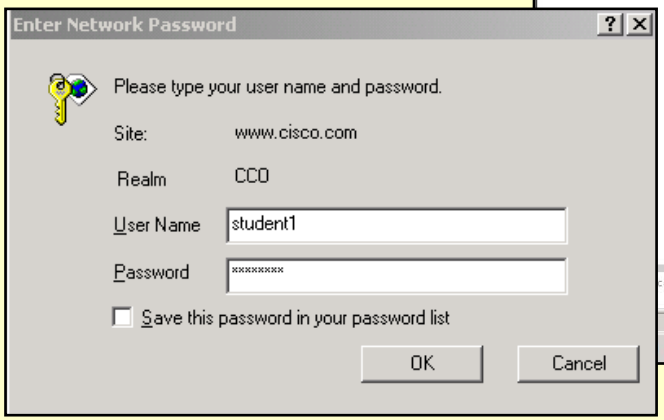
Something you are

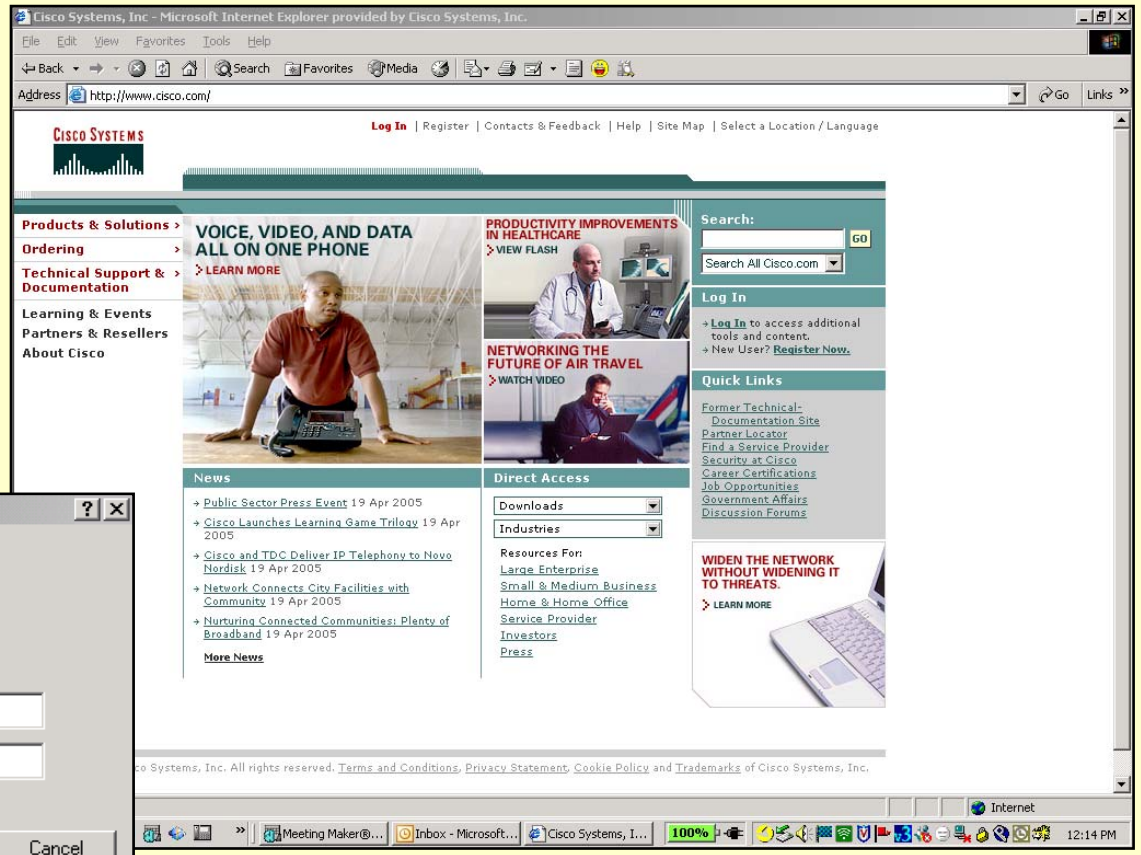


Certificate

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)

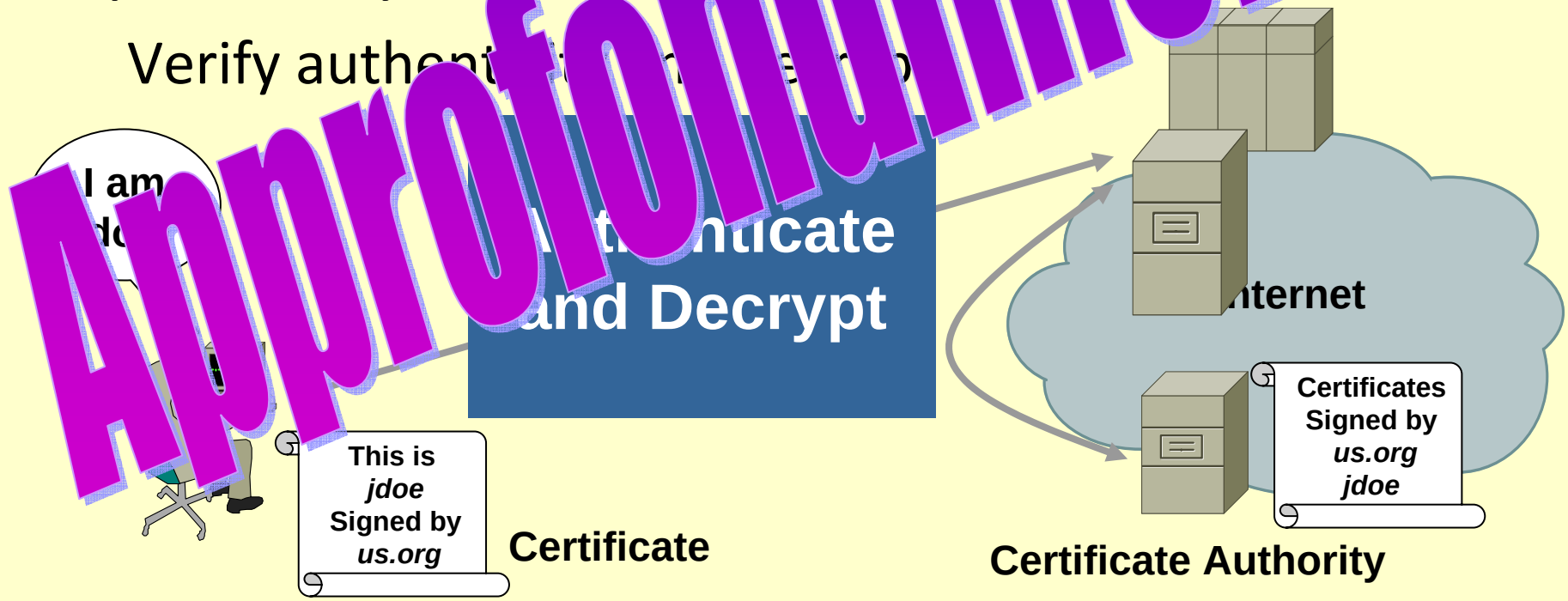
Relies on a Two Key System

J Doe signs a document with his privat

Person who receives that doc s L Doe's public key to:

Verify authent

Approfondimento

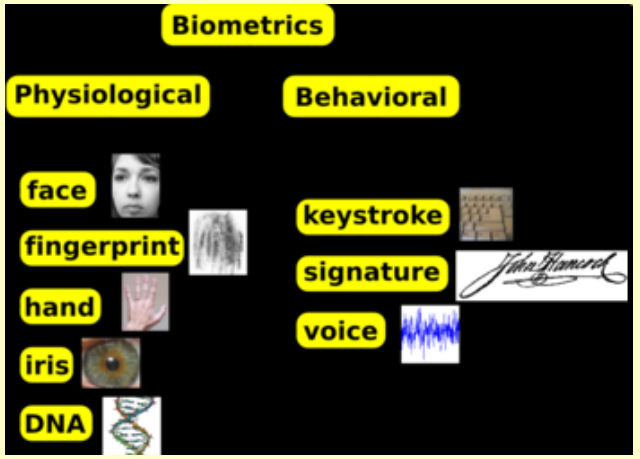


Biometrics

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.

Si riprende dal 4°