Sicurezza dei sistemi informatici
Firma elettronica
E-commerce

Il contesto applicativo

- Commercio elettronico

collegamenti e transazioni sicure

Il contesto applicativo

- Commercio elettronico

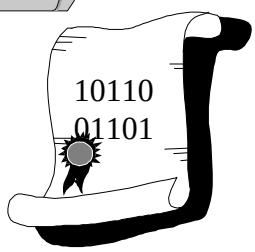
commercio senza identificazione dell'acquirente (net shopping)

commercio con identificazione dell'acquirente (contratto) richiede firma autografa-digitale

Il contesto applicativo

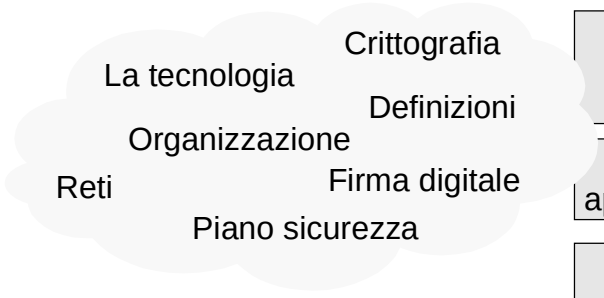
- Commercio elettronico

- Documenti elettronici



sostituzione firma autografa

Sicurezza

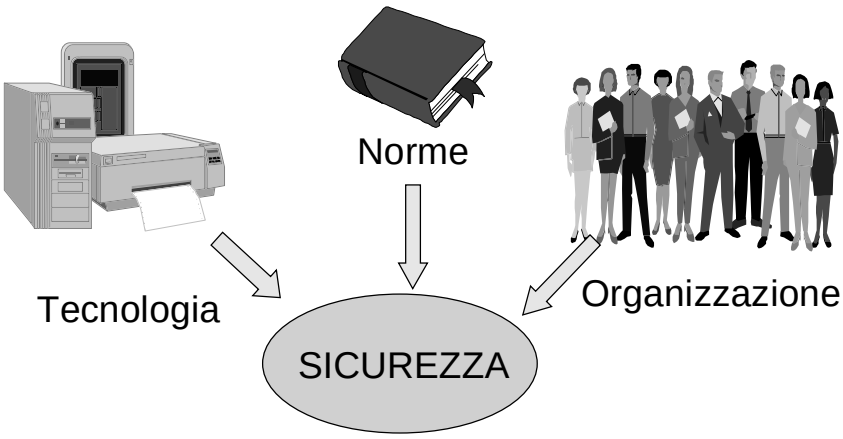


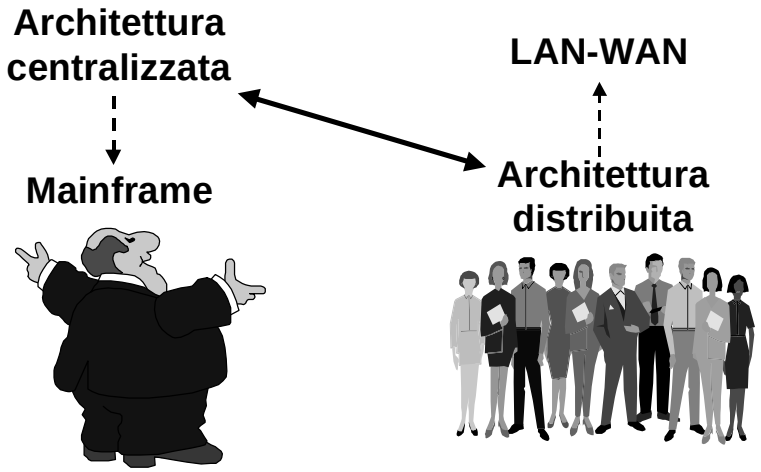
- Virus e worms
- Firewall e reti private virtuali
- Sicurezza delle applicazioni Internet
- Firma digitale e Autorita` di Certificazione
- Smart-card e commercio elettronico

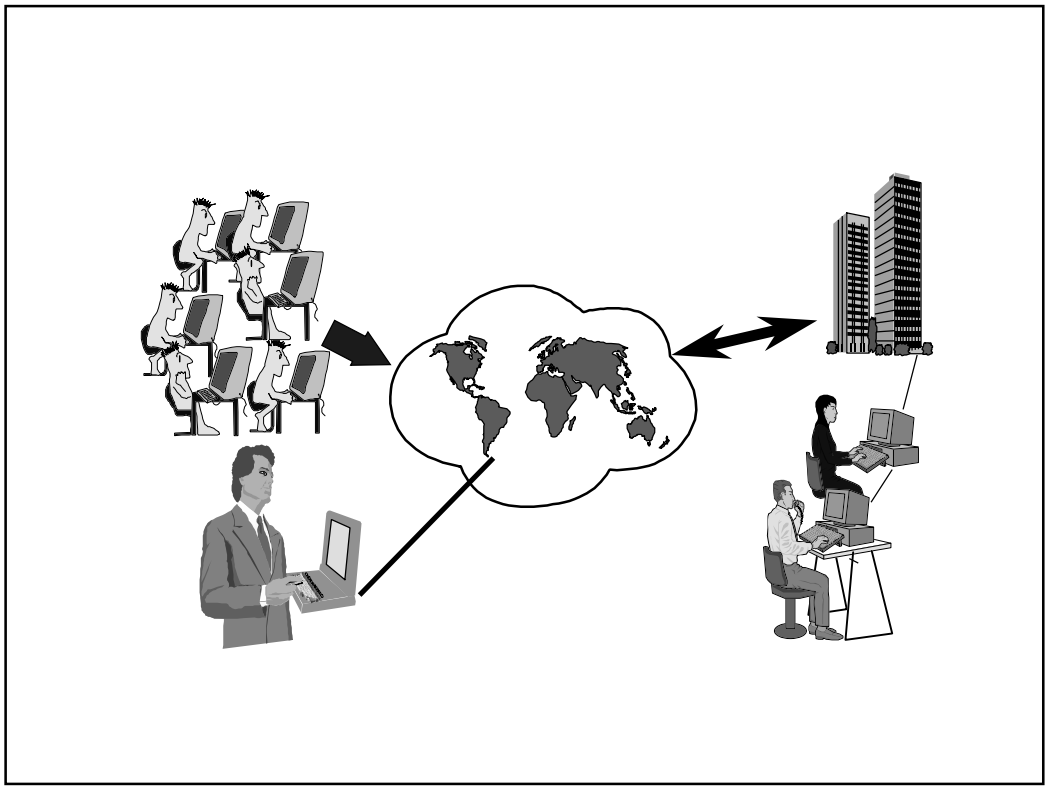
La crescente importanza della sicurezza informatica deriva principalmente da:

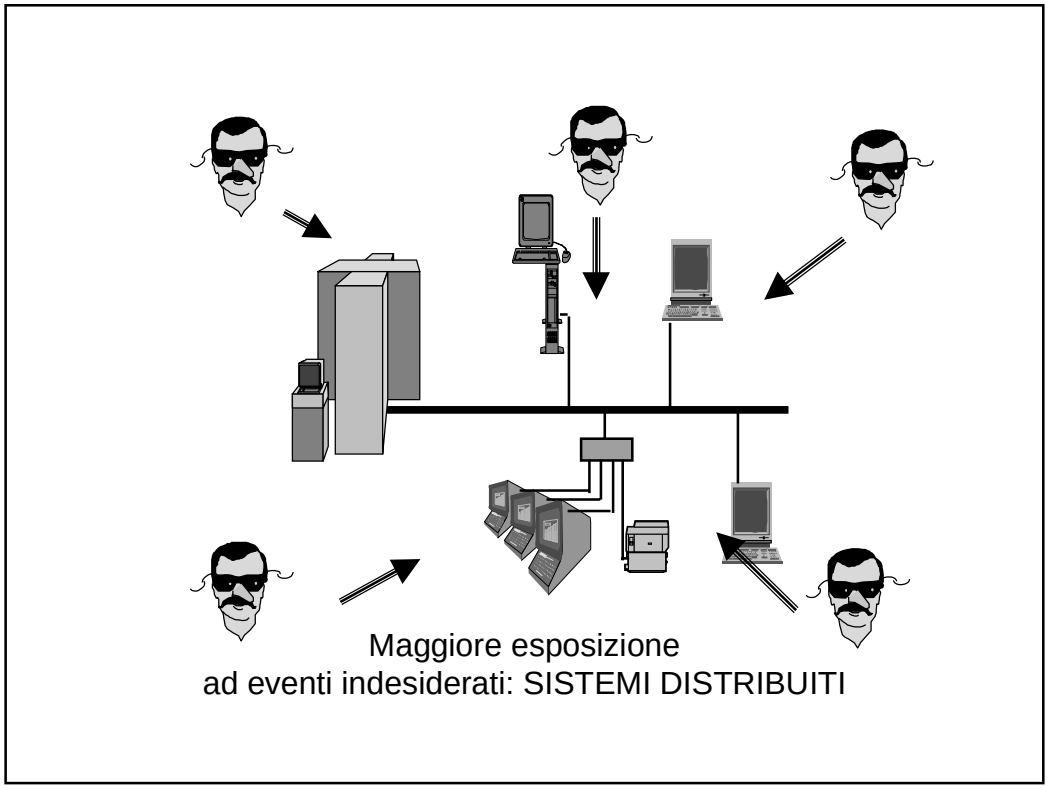
- Maggior informatizzazione dei processi aziendali
- Globalizzazione dei processi
- Nuovi paradigmi tecnologici

Le componenti fondamentali

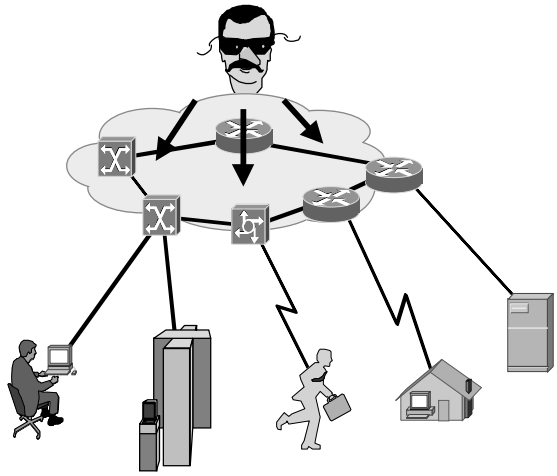








Maggiore esposizione
ad eventi indesiderati: SISTEMI DISTRIBUITI



Maggiore esposizione ad eventi indesiderati: WAN, LAN

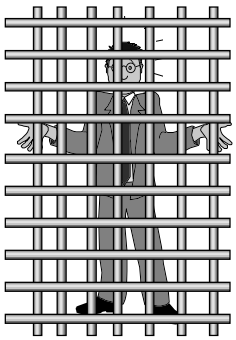
La normativa

Le leggi di riferimento:

- Legge 518/92 (*tutela giuridica sw*)
- Legge 547/93 *(reati informatici)*
- Direttiva UE 97/66/CE del 15 dic. 97 (*trattamento dati a carattere personale e protezione vita privata nel settore tlc*)

Legge 518/92

Legge 547/93

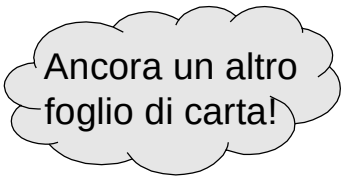


Sancisce come reato penale:

- accesso non autorizzato
- danneggiamento
- sabotaggio
- abusiva acquisizione di programmi e di dati
- diffusione di virus

La normativa

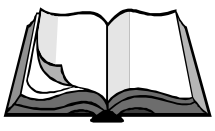
Le leggi di riferimento:



- Legge 675/96 *(privacy)*
- Emanazione schema di regolamento *norme in materia di individuazione delle misure minime per il trattamento dati personali*

La normativa

- Art. 15, comma 2, legge n.59/97:



0110100111010

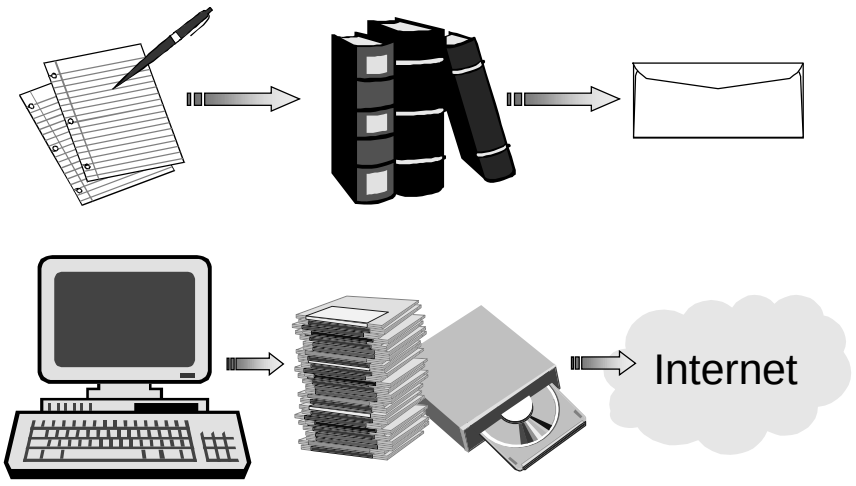
La normativa

- Art. 15, comma 2, legge n.59/97:

  “Gli atti, dati e documenti formati … con strumenti informatici o telematici,… nonché la loro archiviazione trasmissione con documenti informatici, sono validi e rilevanti a tutti gli effetti di legge” (legge Bassanini)

- Legittimazione del documento elettronico

…Il ciclo di vita dalla carta al bit



La normativa

- D.P.R. 513/97 “modalità di applicazione” della legge 59/97
  - introduce la firma digitale
  - regola la costituzione delle CA
- “Regolamento” D.P.C.M. in fase di emanazione

Sicurezza

L’insieme delle misure (di carattere organizzativo e tecnologico) mirate ad assicurare a ciascun utente o processo (e a nessun altro) tutti e soli i servizi previsti per quell’utente o processo, nei tempi e nelle modalità previste.

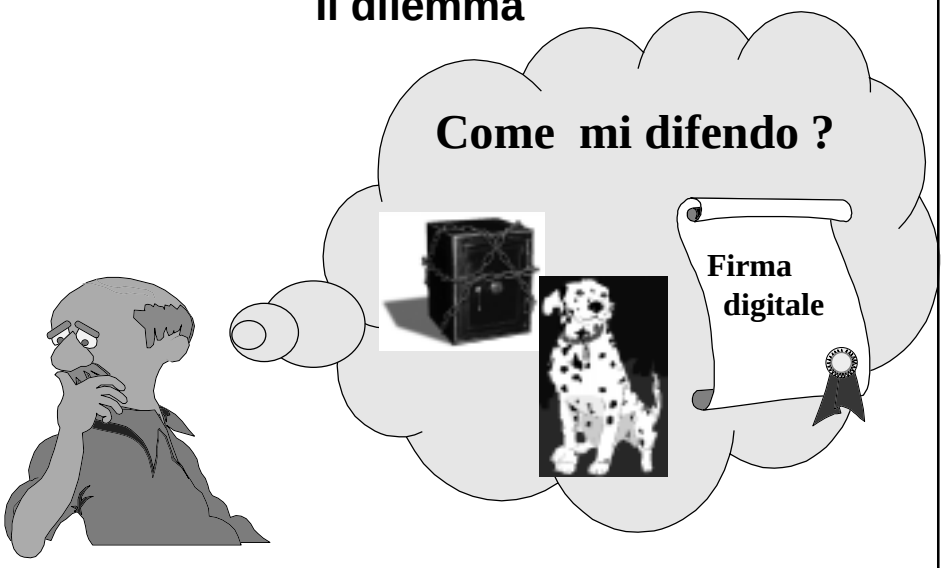
Le tecniche di sicurezza mirano a garantire:

- riservatezza
- integrità
- disponibilità

ma anche:

- autenticazione
- non ripudio

Il dilemma



Le regole per la sicurezza

- Regola n.1:

le informazioni trasmesse o memorizzate devono essere inaccessibili a tutti, tranne a chi le invia e le riceve (riservatezza)

Le regole per la sicurezza

- Regola n.2:

le informazioni trasmesse o memorizzate non devono essere variate durante il tragitto (integrità)

Le regole per la sicurezza

- Regola n.3:

il ricevente deve avere certezza che le informazioni provengano dal vero mittente (autenticità)

Le regole per la sicurezza

- Regola n.4:

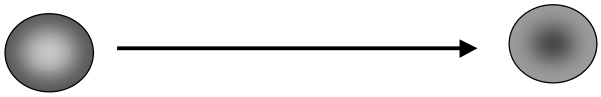
il mittente deve avere certezza che il ricevente sia quello corretto (autenticità)

Le regole per la sicurezza

- Regola n.5:

il ricevente non deve poter negare di aver ricevuto le informazioni e il mittente non deve poter negare di averle inviate (non ripudio)

Categorie di attacco

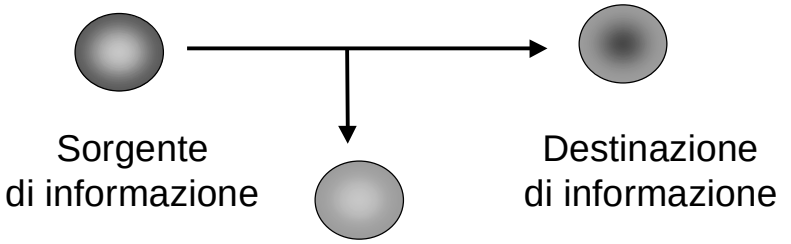


Sorgente di informazione

Destinazione di informazione

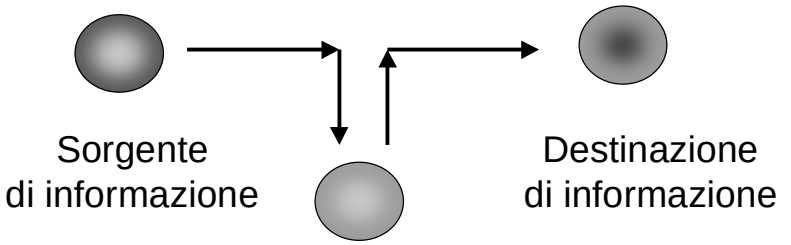
Situazione normale

Categorie di attacco



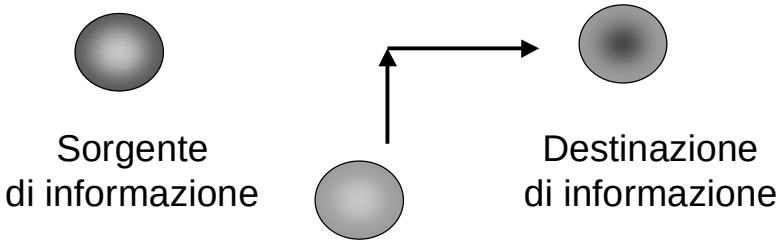
Intercettazione

Categorie di attacco



Modifica

Categorie di attacco



Creazione

Categorie di attacco

Interruzione

Sicurezza

Alcune classificazioni:

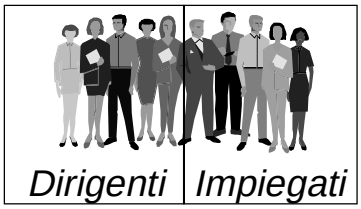
- Attacchi passivi (mirati a conoscere dati, informazioni, configurazioni,...)
- Attacchi attivi (mirati ad alterare dati, informazioni, configurazioni,...)

Politica per la sicurezza

Le fasi principali:

- analisi del contesto (struttura, organizzazione, flussi informativi)
- analisi del sistema informatico(risorse fisiche, risorse logiche, processi)
- classificazione degli utenti e dei processi e relativi diritti di accesso
- analisi e valutazione della vulnerabilità e conseguenti rischi
- individuazione e pianificazione contromisure

Classificazione utenti



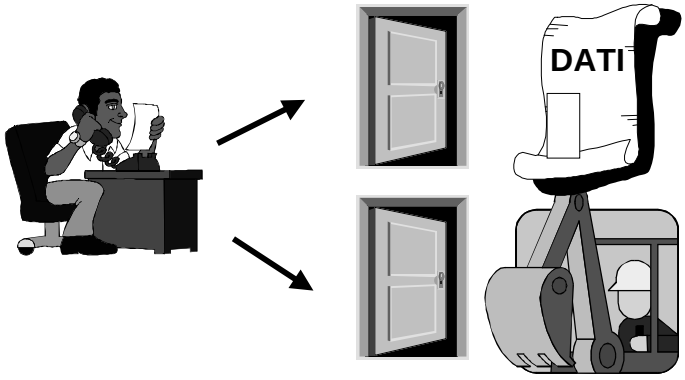
sistemisti

sviluppatori

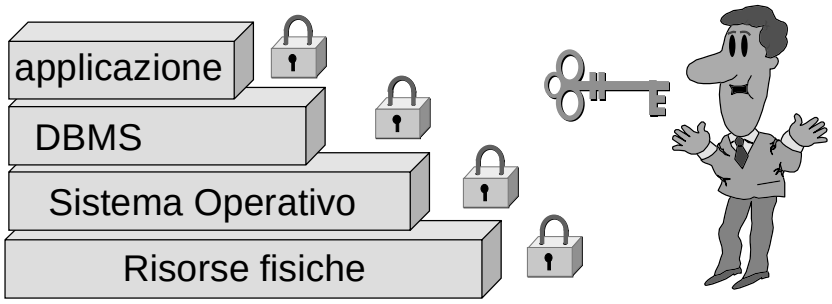
esterni

Diritti di accesso

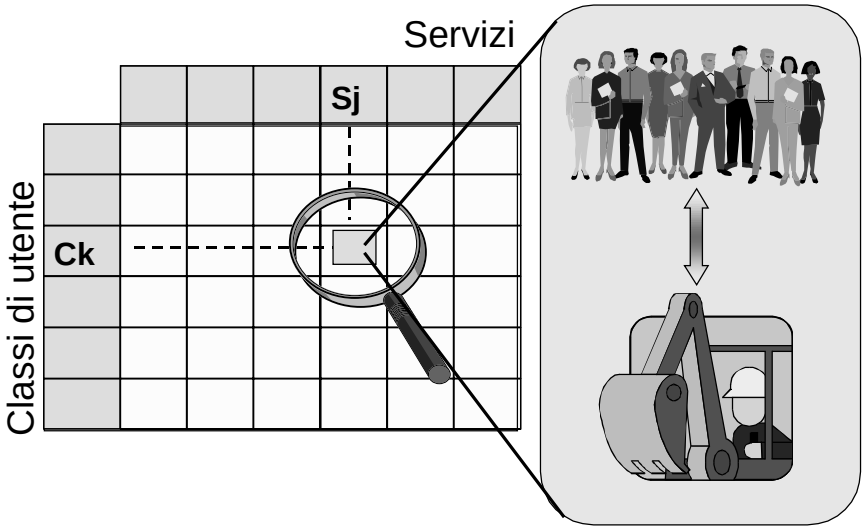
Per ogni utente o processo si deve definire quali **informazioni** e **servizi** possono essere resi disponibili ed in che modo



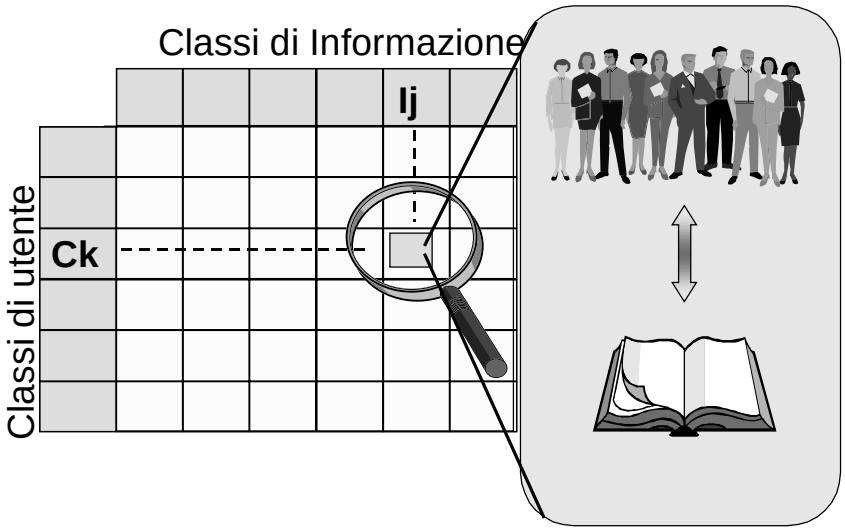
Diritti di accesso



Diritti di accesso



Diritti di accesso



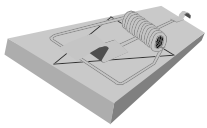
Politica per la sicurezza

Le fasi principali:

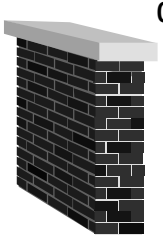
- analisi del contesto (struttura, organizzazione, flussi informativi)
- analisi del sistema informatico(risorse fisiche, risorse logiche, processi)
- classificazione degli utenti e dei processi e relativi diritti di accesso
- analisi e valutazione della vulnerabilità e conseguenti rischi
- individuazione e pianificazione contromisure

Le componenti fondamentali

difesa attiva



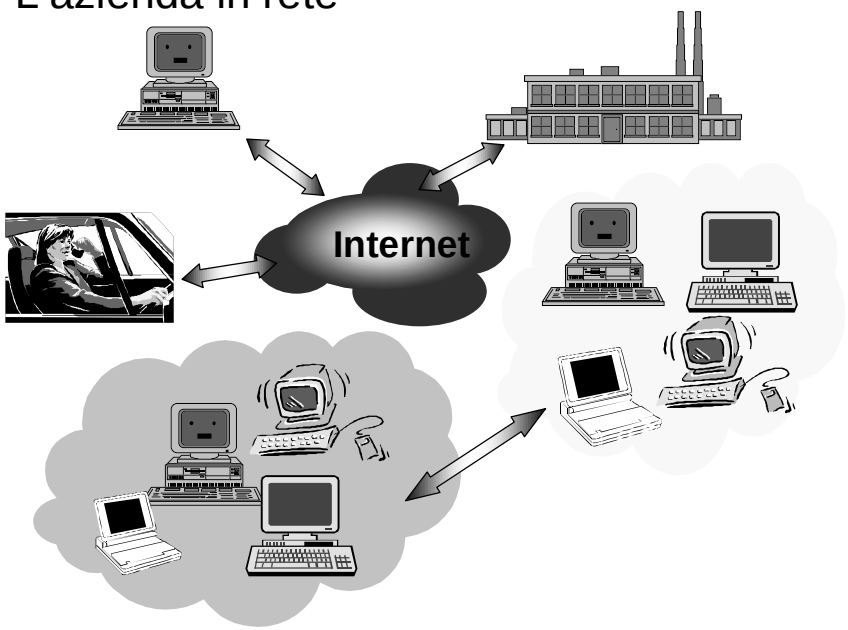
trabocchetti



difesa passiva

osservazione

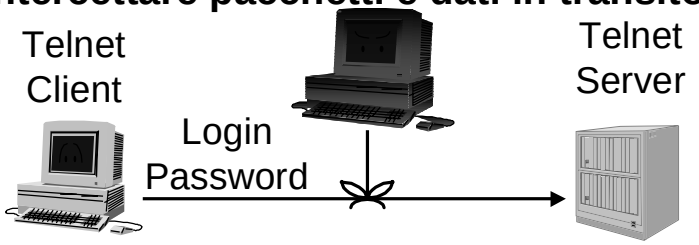
L'azienda in rete



Alcune tipologie di attacco

NETWORK SNIFFING

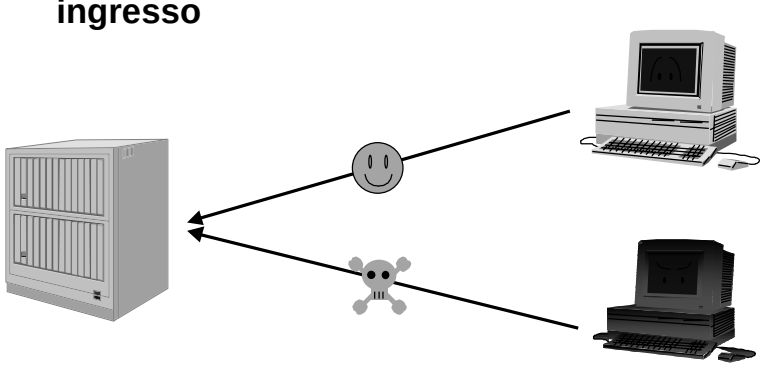
Se i dati viaggiano sulla rete da una macchina all'altra in chiaro (cioè non cifrati in alcun modo) è possibile da una qualsiasi macchina della rete locale intercettare pacchetti e dati in transito



Alcune tipologie di attacco

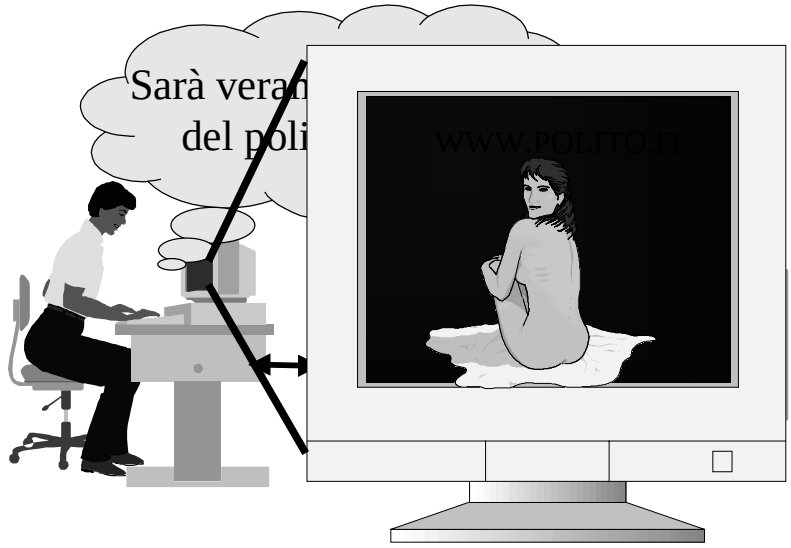
IP SPOOFING:

costruzione di pacchetti IP per ingannare un server sulla provenienza delle chiamate in ingresso



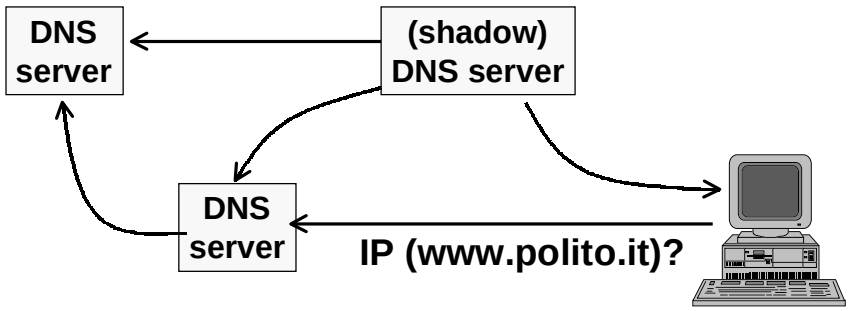
Web sicuro

Web sicuro



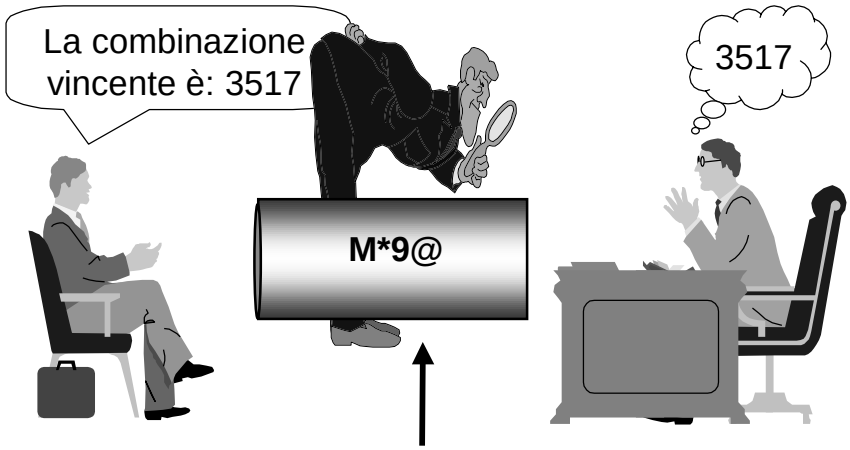
Sicurezza del DNS

- attacchi:
  - shadow server
  - avvelenamento della cache



Crittografia
Firma digitale

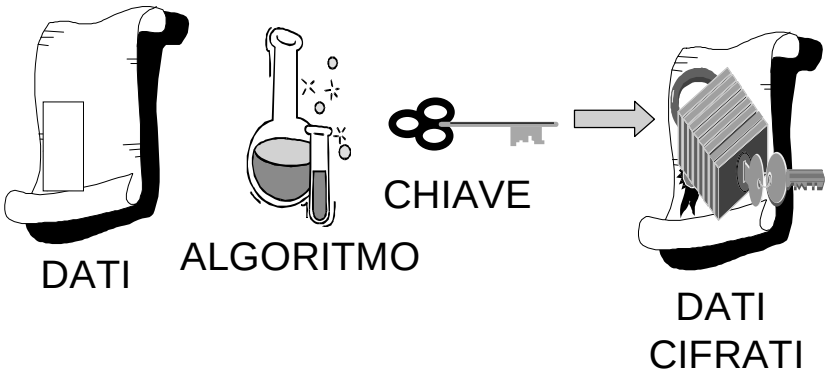
Crittografia



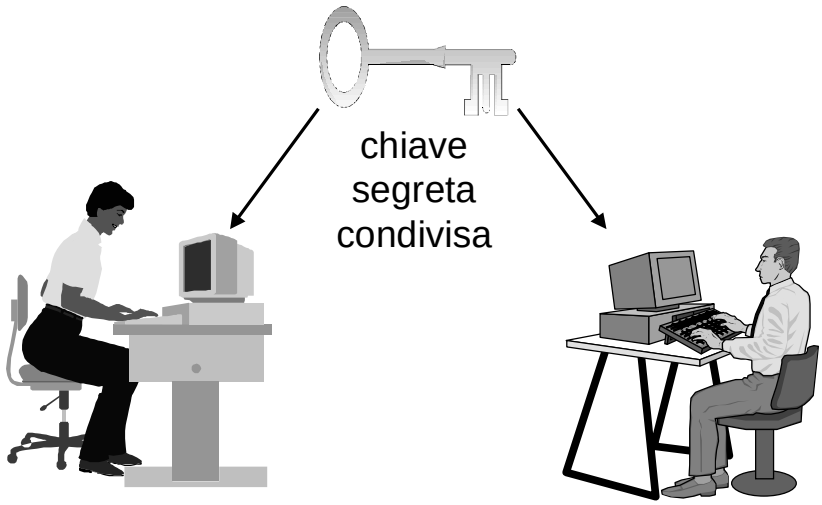
CANALE DI COMUNICAZIONE

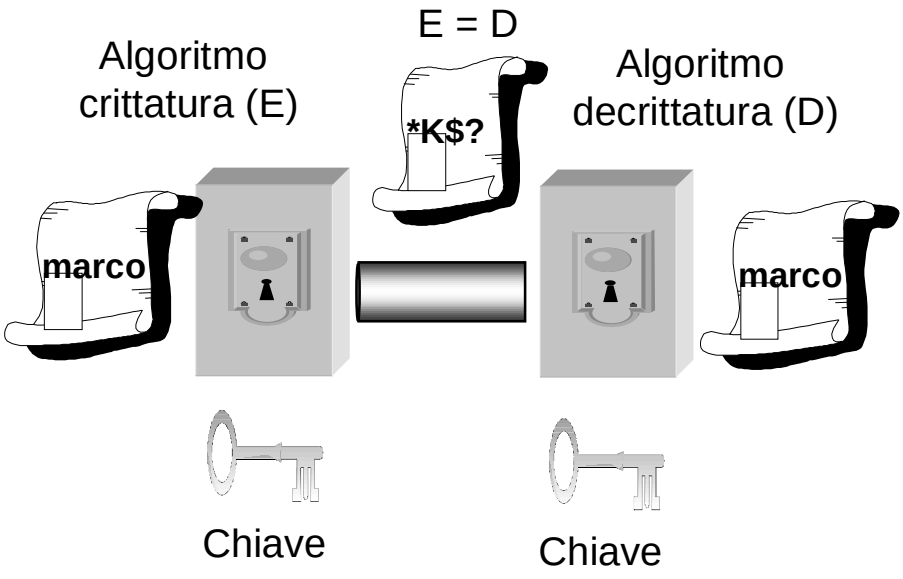
Crittografia

Le componenti di un sistema crittografico

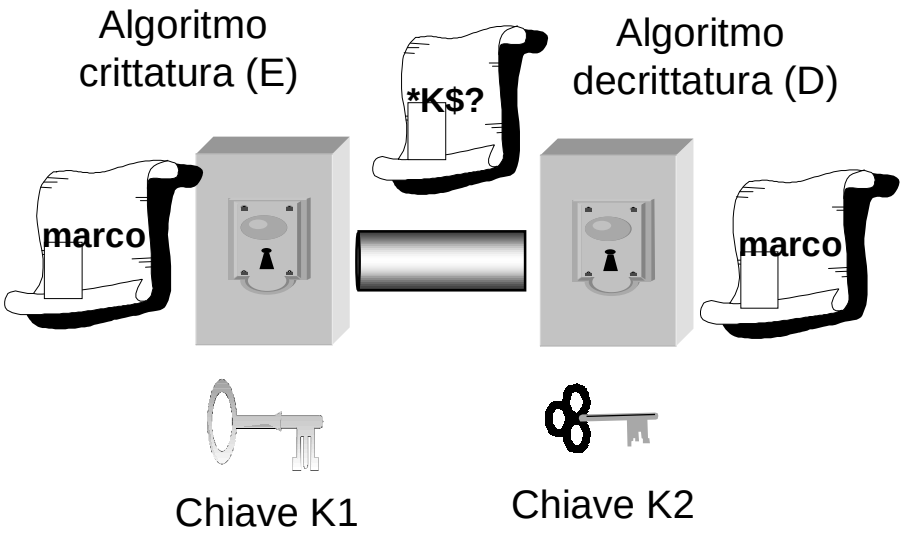


Soluzioni basate su chiavi segrete



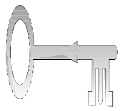

E = D
Algoritmo
crittatura (E)
*K$?
Algoritmo
decrittatura (D)
marco
marco
Chiave
Chiave


Soluzioni basate su chiavi pubbliche
chiave pubblica
di Marco
chiave
privata



Crittografia a chiave pubblica

Ogni utente ha due chiavi

Una delle chiavi è resa pubblica

La chiave segreta (“privata”) è nota soltanto al suo proprietario.

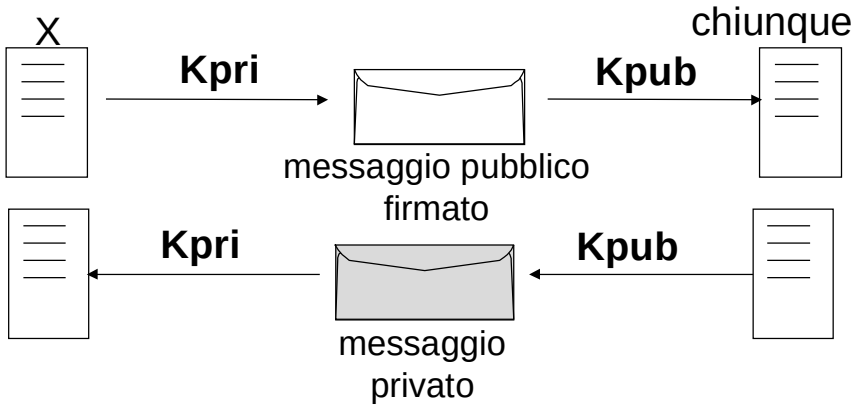
Crittografia a chiave pubblica

Tutte le chiavi pubbliche sono consultabili in un elenco centralizzata

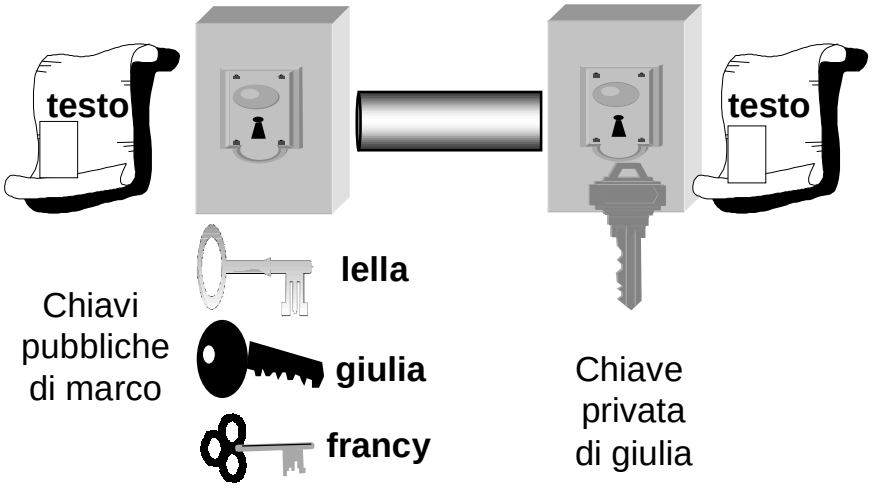
E' possibile firmare ed autenticare i propri documenti in modo inequivocabile.

Crittografia a chiave pubblica

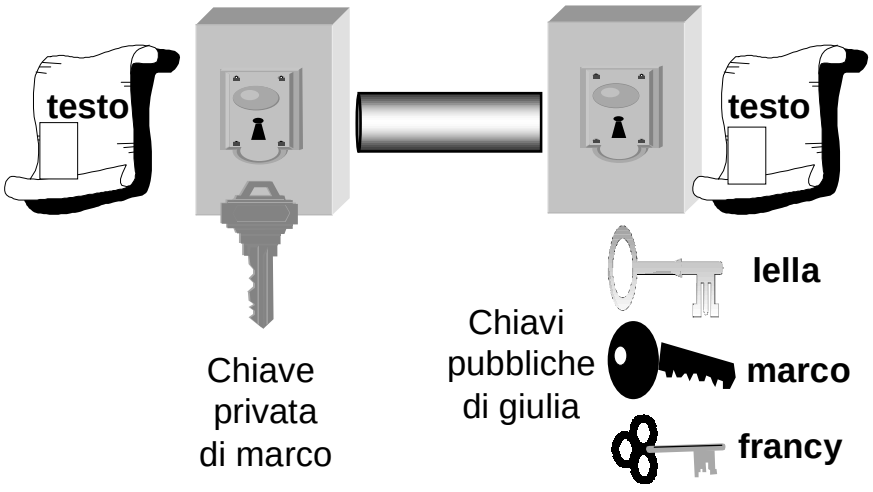
- **chiavi generate a coppie (Kpri , Kpub)**
- **Kpri tenuta segreta, Kpub distribuita**
- **chiavi con funzionalità reciproca**



SEGRETEZZA
(messaggio da marco a giulia)



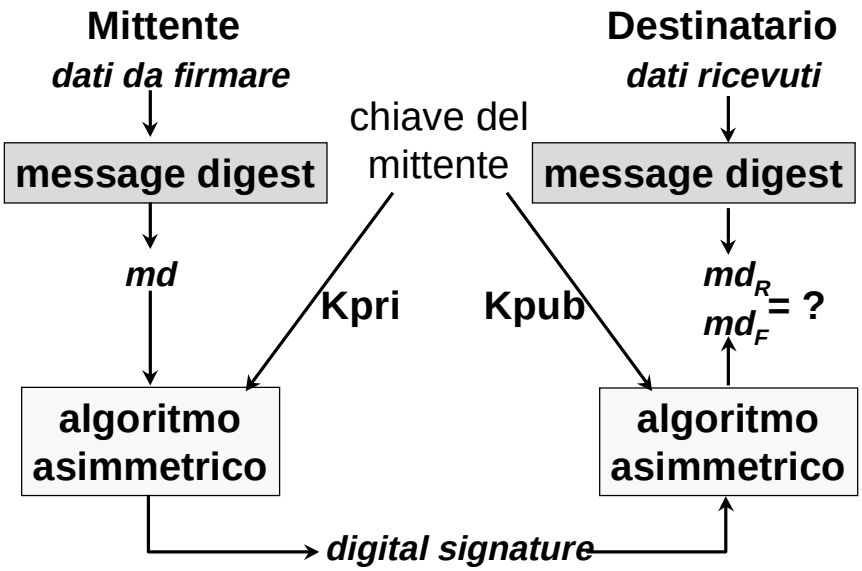
AUTENTICAZIONE
(di un messaggio da marco a giulia)



Autenticazione

- **L'autenticazione permette di:**
  - conoscere l'identità del mittente
  - rilevare alterazioni nel testo
- **ma:**
  - il ricevente può falsificare il testo producendone uno diverso
  - generare un nuovo testo
  - il mittente disconoscere l'invio di un testo

Firma digitale



Message digest (hash)

- **è un riassunto del messaggio che si vuole proteggere**
- **allo scopo si usano algoritmi di hash:**
  - MD5, genera un digest di 128 bit
  - SHA, genera un digest di 160 bit

messaggio
digest
Digest firmato con Kpri

Certificato a chiave pubblica

- **La sola firma con una coppia di chiavi non mi garantisce la *corrispondenza con un soggetto fisico***

Certificato a chiave pubblica

- **E' necessario un *certificato d'autenticità* che garantisca in modo esplicito l'identità del soggetto (SIGILLO)**

Certifico che la seguente è la chiave pubblica di Mezzalama:

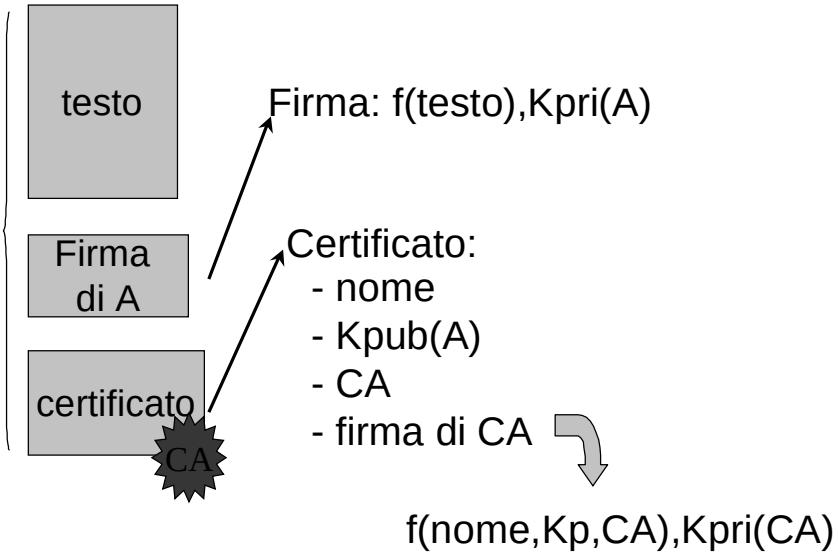
Firmato: il rettore***ZICH***

Certificato a chiave pubblica

"**Una struttura dati per legare in modo sicuro una chiave pubblica ad alcuni attributi**

- tipicamente lega una chiave ad un'identità
- firmato in modo elettronico dall'emettitore: una persona fidata o - meglio - l'autorità di certificazione (CA)
- con scadenza temporale
- revocabile sia dall'utente sia dall'emettitore
- richiede una RA

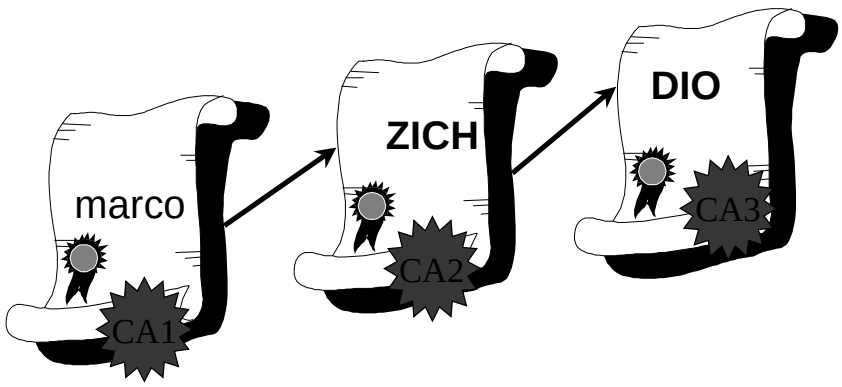
Firma digitale



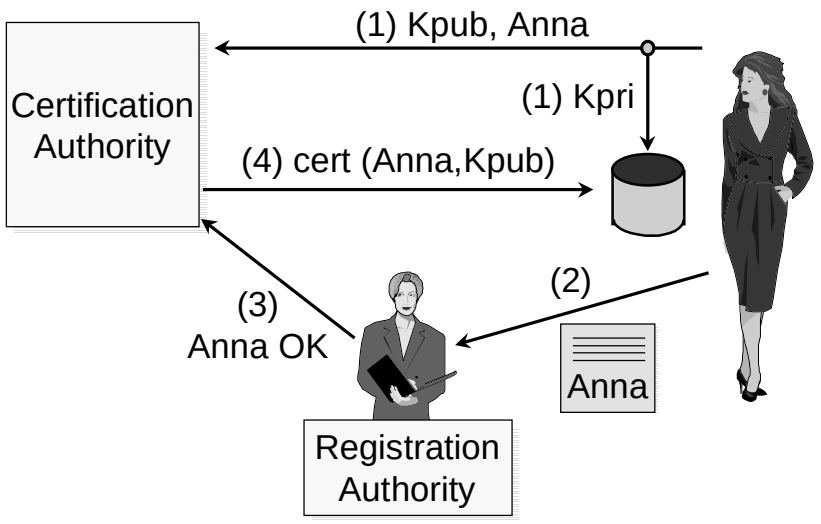
certificato X.509

• versione	....
• algoritmo di firma	RSA with MD2, 512
• issuer	C = IT, O = Polito, OU=CA
• validità	1/1/96 - 31/12/96
• soggetto	C = IT, O = Polito, CN = Marco Mezzalama
• chiave pubblica	RSA, 1024, xxx...
• firma digitale della CA	yy...y

Firma digitale (gerarchia CA)

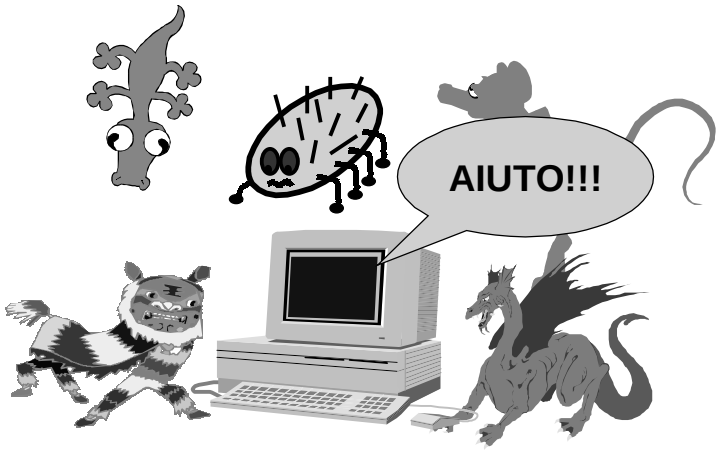


Autorità di certificazione



Sicurezza e virus

I virus dei PC

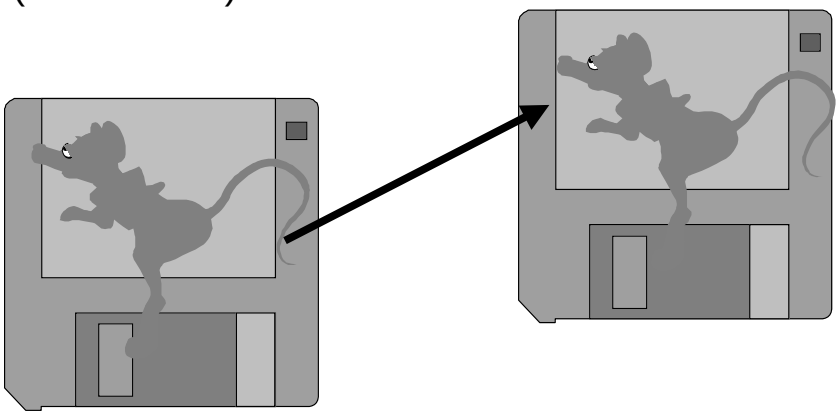


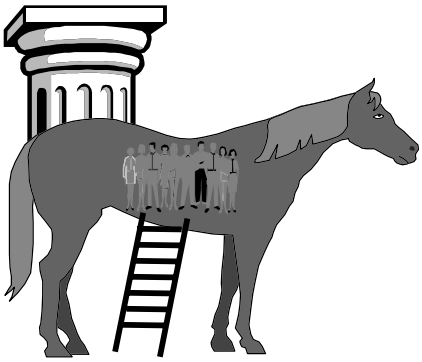
I virus dei PC

Un virus è un piccolo programma che si nasconde in un altro programma e che …….

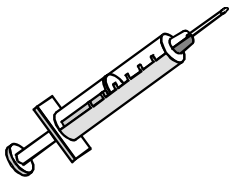
I virus dei PC

… si duplica passando da un file ad un altro (di nascosto!)

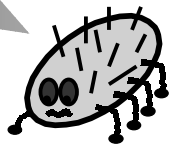




Cavallo di Troia

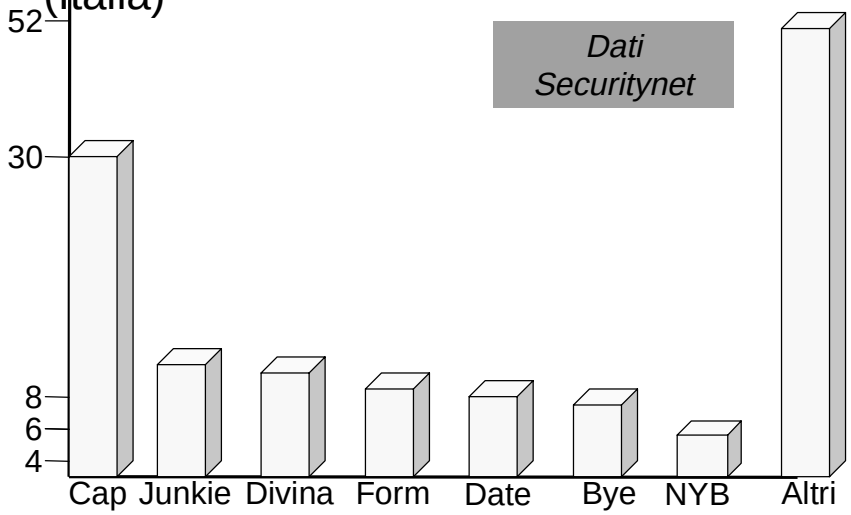


Capacità di infezione

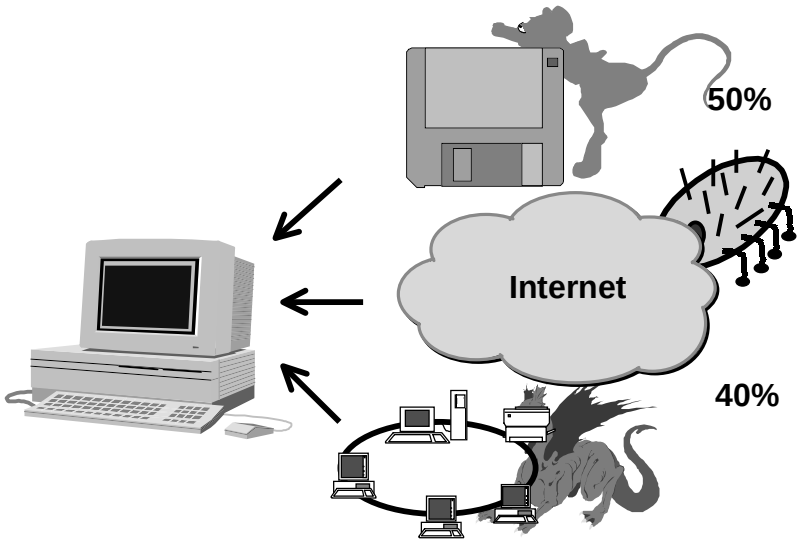


Virus

Diffusione virus (Italia)



Da dove arrivano...



Modalità di infezione

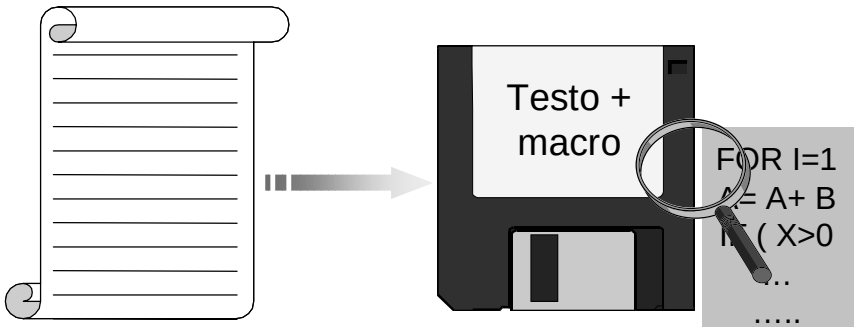
(modalità con cui si introducono e si duplicano nel sistema)

- BOOT VIRUS
- PARASITIC o MULTI VIRUS
- MACRO VIRUS

```
If (a >= 17)  then
….
….
else
…..
for (i = 0; i <= N; i++)
…..
a =b + c
….
….
while (x2>eps)
….
….
```

Il virus è un segmento di codice (insieme di istruzioni) nascosto in un altro segmento di codice (programma)

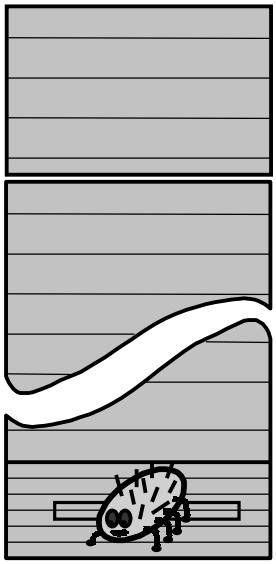
Macro Virus



Macro: - Auto Exec

- Auto Open
- File Save As

Come si rileva un virus

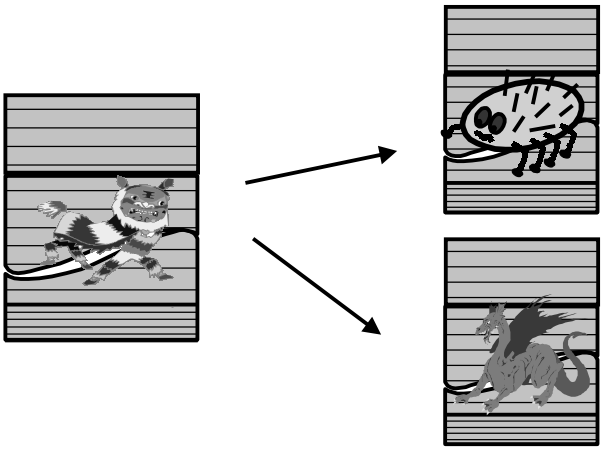


Le istruzioni sono sempre le stesse!

Stringa esadecimale:
BE007C33FFFCF3A42EF
F2E037C33COE8 (Cascade)

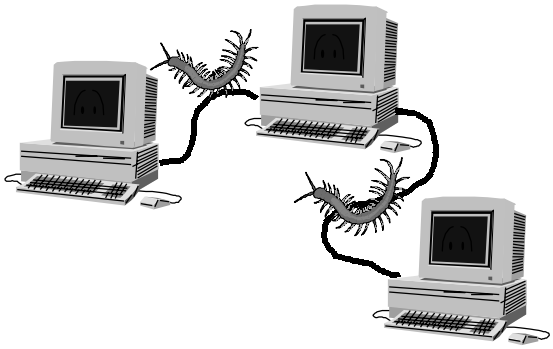
Virus Polimorfi

Il codice virale cambia ad ogni infezione



Gli antivirus

1. WORMS



Programmi che utilizzano la rete
per propagarsi

2. HOAX Virus (e-mail)

ATTENZIONE!
Se ricevete un file del tipo …
non apritelo!

E' un virus!
Passate con urgenza
questa informazione.