Sicurezza su Reti

Barbara Masucci

Dipartimento di Informatica ed Applicazioni

Università di Salerno

masucci@dia.unisa.it
http://www.dia.unisa.it/professori/masucci

Per Favore

Orari Corso

Mercoledì 11:00 - 14:00

- Aula F-4 (Fisciano)

Venerdì 15:00 - 17:00

- Aula F-4 (Fisciano)

Orari di ricevimento

Mercoledì 15:00 - 17:00

- Studio L1-12 (DIA)

Venerdì 12:00 - 13:00

- Studio L1-12 (DIA)

Home-page del corso

http://www.dia.unisa.it/professori/masucci/sicurezza0405

Qui troverete informazioni aggiornate sul corso

- Programma
- Slides delle lezioni (formato pdf)
- Date/Modalità esami
- Tracce di esami con soluzioni
- Risultati delle prove intercorso

Registrazione al corso

Per l'organizzazione del corso

- Prove intercorso, progetti
- Account presso Laboratorio Reti

http://www.dia.unisa.it/professori/masucci/sicurezza0405

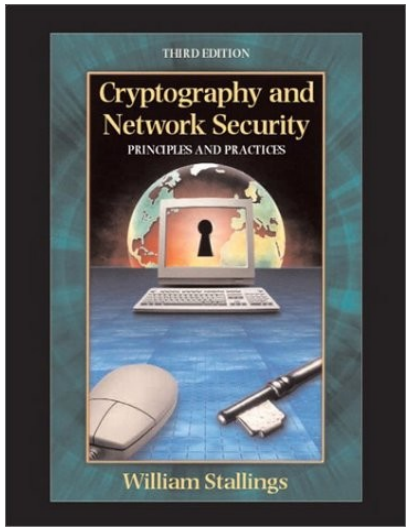
Esami

- Prima prova in itinere e primo appello: Novembre 2004
- Seconda prova in itinere e secondo appello: Febbraio 2005
- Terzo appello: Febbraio 2005
- Quarto appello: Luglio 2005
- Quinto appello: Settembre 2005

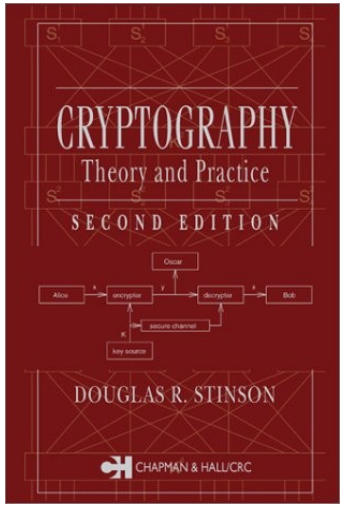
Come usare la posta elettronica

- Inserire l'oggetto del messaggio
- Firmare il messaggio (sempre!)
- Essere brevi
- Non chiedere informazioni disponibili sul sito
  - -Date/Modalità esami
  - -Programma del corso

Testi di riferimento



Cryptography and Network Security: Principles and Practice (3rd Edition)
by William Stallings, 2003



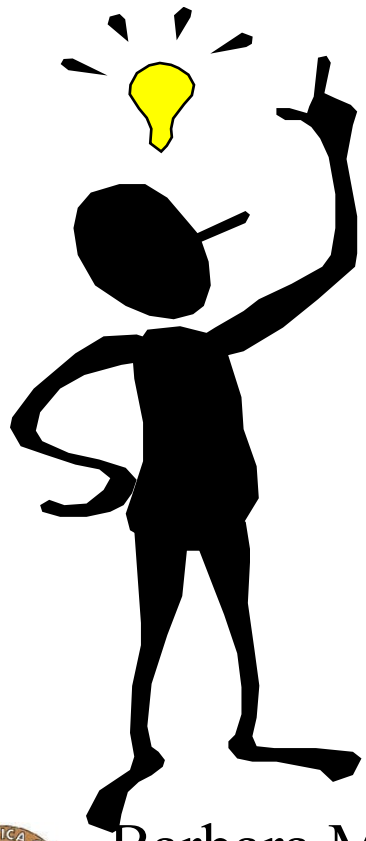
Cryptography: Theory and Practice (2nd Edition)
by Douglas Stinson, 2002

Prerequisiti

Teoria dei Numeri

Fondamenti di Reti

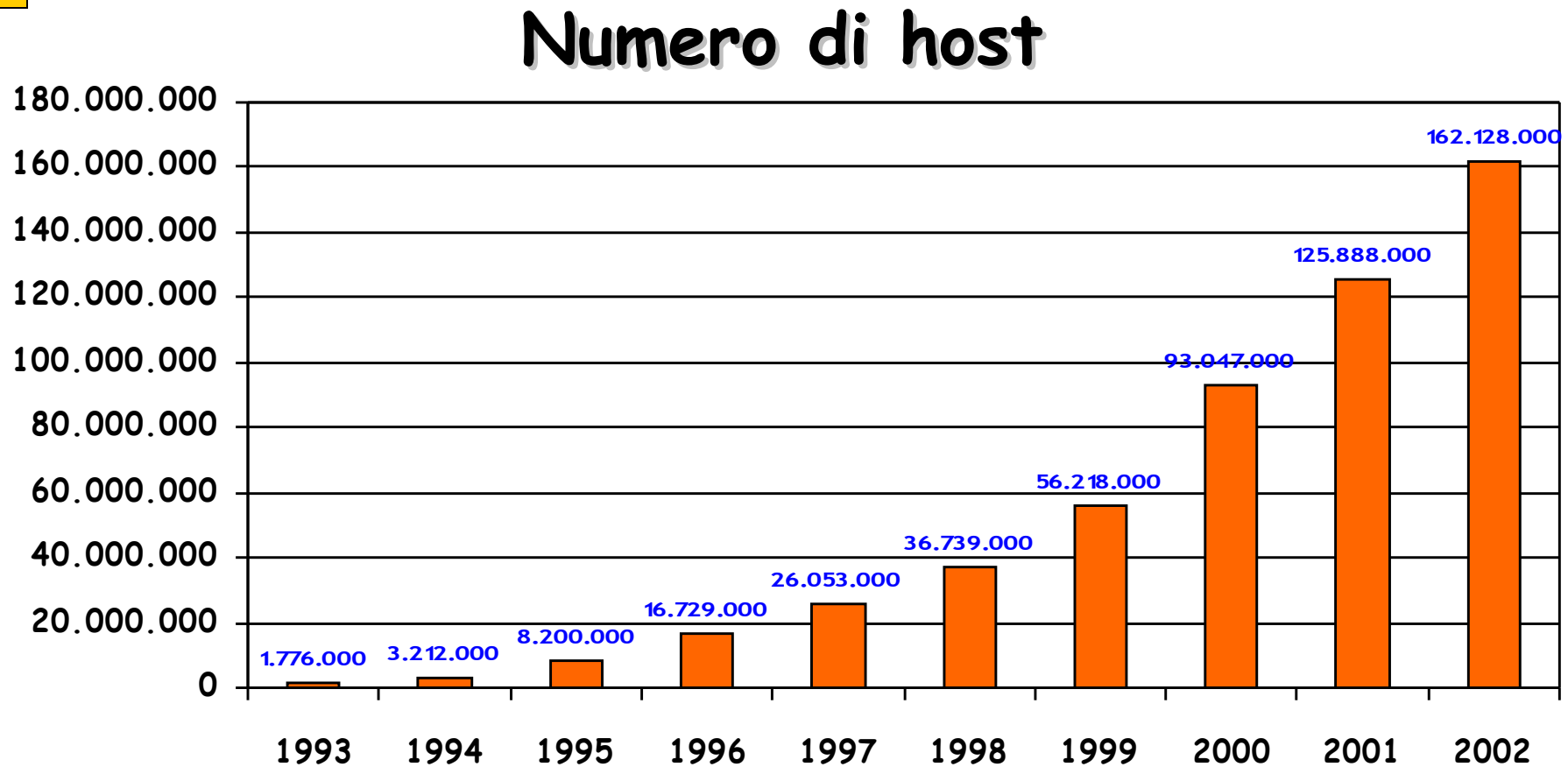
… ma faremo un veloce riepilogo



Ed ora …

qualcosa sui contenuti

Crescita di Internet



Problemi

Internet consente alle aziende di

- Effettuare commercio elettronico
- Fornire un migliore servizio ai clienti
- Ridurre i costi di comunicazione
- Accedere facilmente alle informazioni

…tuttavia…

… espone i computer all'azione di attacchi da parte di malintenzionati

- Il numero di incidenti aumenta di anno in anno
- Le perdite finanziarie hanno raggiunto livelli misurabili in miliardi di dollari

Il worm di Morris

Il 2 Novembre 1988 Internet fu colpita dal Worm di Morris

- Il virus sfruttava bug del sistema operativo Unix per penetrare negli host attraverso la rete
- In una sola ora i computer di molti centri di ricerca furono inutilizzabili, perché sovraccaricati da molteplici copie del worm

Per bloccare il virus fu formato un team di esperti

- Furono sviluppate e divulgate le procedure per lo "sradicamento" del worm
- In una settimana tutto tornò alla normalità

Data la potenzialità del virus, i danni furono minimi, ma ci si rese conto dei rischi legati ad Internet

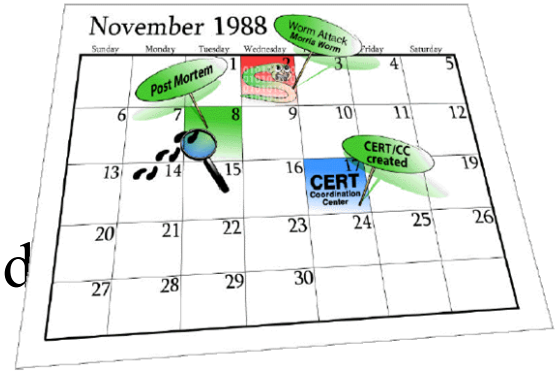
CERT
Computer Emergency Response Team

Team di esperti nell'ambito della sicurezza

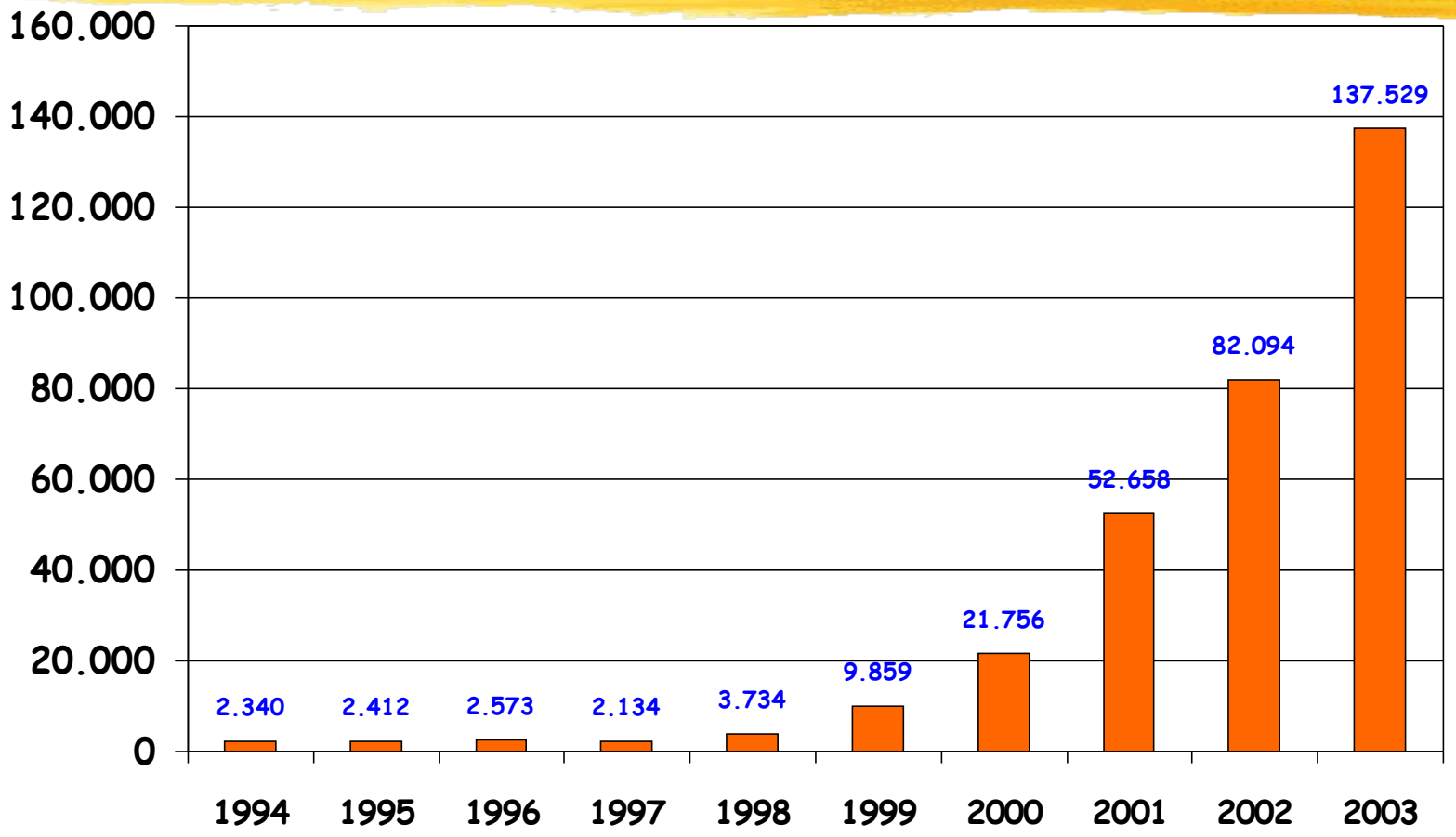
- Creato dal DARPA (Defense Advanced Research Projects Agency) in seguito all'attacco del worm

Si occupa di

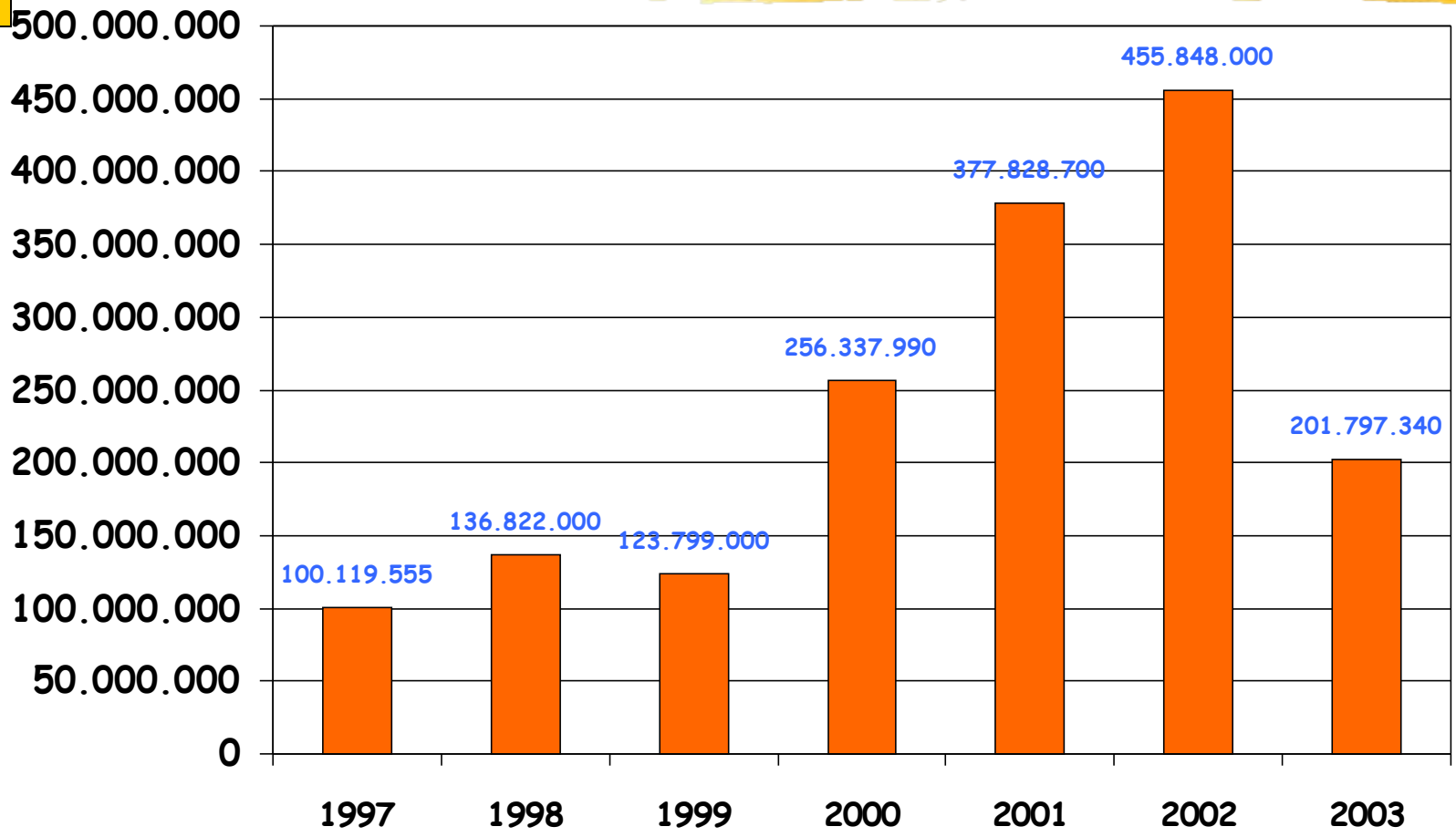
- Identificare il tipo di incidenti
- Quantificare le perdite economiche
- Analizzare le vulnerabilità dei prodotti



Incidenti riportati al CERT



Perdite economiche



Indagine CSI/FBI

Nel 2004, su 494 intervistati (aziende, agenzie governative, università, ospedali, etc…)

- Il 90% ha riportato incidenti legati alla sicurezza
  - I danni più seri riguardano il furto di informazioni delicate e le frodi finanziarie
- Il 75% ha subito danni economici
  - Solo il 47% è stato in grado di quantificare i danni
- Il 74% ritiene che la connessione ad Internet costituisca il maggior punto di attacco
- Solo il 34% ha denunciato gli incidenti subiti
  - Tutti gli altri non lo hanno fatto per evitare pubblicità negativa

Hacker

Steven Levy, *Hackers: Heroes of the Computer Revolution*

- tipo positivo, studente di MIT o Stanford
- ideale: rendere la tecnologia accessibile a tutti
- risolvere i problemi e creare soluzioni

Più recentemente, nei media:

- tipo negativo
- sfruttano buchi di sicurezza

Hacker
(tipo positivo)

Una persona che ama esplorare i dettagli dei sistemi informatici e i modi con cui estenderne le capacità, contrariamente alla maggioranza degli utenti, che impara solo lo stretto necessario.

Chi programma con entusiasmo o che preferisce programmare piuttosto che disquisire sulla programmazione.

Guy L. Steele, et al., ***The Hacker's Dictionary***

Hacker
classificazione

Cracker: programmatori specializzati nell'infrangere sistemi di sicurezza per sottrarre o distruggere dati

Script Kiddie: cracker che adoperano script scritti da altri, non essendo in grado di produrli da sè

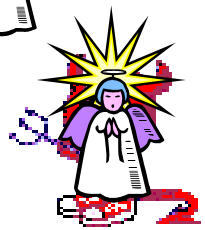
Phracher: rubano programmi che offrono servizi telefonici gratuiti o penetrano computer e database di società telefoniche

Phreaker: utilizzano informazioni telefoniche (numeri telefoni, carte telefoniche,…) per accedere ad altri computer

Hacker
classificazione

Black hat: hacker "cattivo", che sfrutta la propria abilità per delinquere

White hat: hacker che si ritiene moralmente e legalmente integerrimo



Grey hat: una via di mezzo tra white e black hat

Termini coniati nel 1996, in occasione della prima conferenza Black Hat Briefings, a Las Vegas

Vulnerabilità, Attacchi, Minacce

Vulnerabilità

- Debolezza di un sistema di sicurezza che può essere utilizzata per causare danni

Attacco

- Sfruttamento di una vulnerabilità di un sistema

Minaccia

- Circostanza che può causare danni
  - Attacco, disastro naturale, errore umano, buco software o hardware

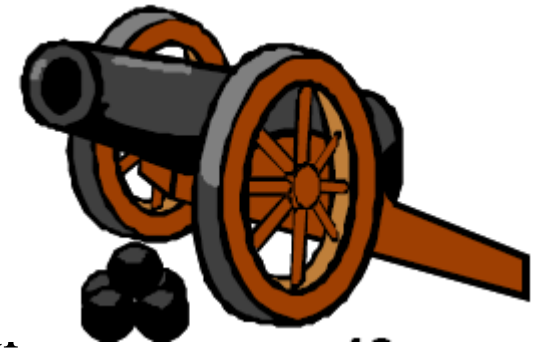
Tipi di attacchi

Attacchi passivi: non alterano i dati in transito

- Intercettazione del traffico
- Analisi del traffico

Attacchi attivi: modificano il flusso di dati o creano un falso flusso:

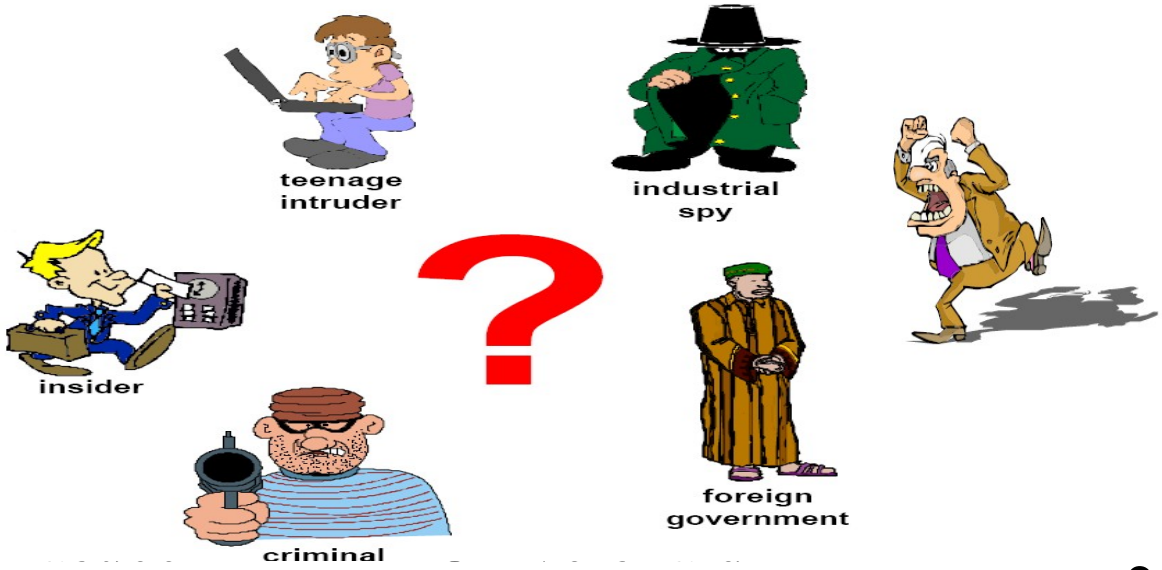
- Mascheramento
- Riproduzione
- Modifica dei messaggi
- Denial of service



Intrusioni

Vari tipi di *intruder*

- Adolescente curioso
- Studente universitario che ha sviluppato nuovo tool
- "Spia" a pagamento
- Dipendente licenziato o arrabbiato



Intrusioni: motivi

- Divertimento
- Senso di potenza
- Sfida intellettuale
- Attenzione politica
- Guadagno economico

Intrusioni

Il manager ragiona così:

- "Nessuno attaccherà la mia azienda, non c'è nulla di prezioso qui!"

Gli hacker invece ragionano così:

- "Scelgo il target più facile, entro e poi guardo
- Al massimo userò il sistema come *ponte* per altri attacchi"

Comunicazione

Ci sono newsgroup, pubblicazioni, conferenze sulle ultime tecniche di intrusione

Conoscenza condivisa su:

sistemi mal configurati, usati per scambio di:

- software pirata
- numeri di carte di credito
- strumenti facili da utilizzare
- identità dei siti compromessi (inclusi account e password)

Tipi di incidenti

- Probing e scanning
- Attacchi alle password
- Intercettazione di pacchetti (packet sniffing)
- Compromissione di account (privilegiati e non)
- Denial of Service
- Codice malizioso (Virus, Worm, Trojan horse)
- Attacchi all'infrastruttura di rete (name server, access provider, grossi archivi di rete,…)

Tools Package

Mantenuti da programmatori competenti, includono anche versione e documentazione

Possono contenere:

- Network Scanner
- Tool per password cracking e grandi dizionari
- Packet Sniffer
- Virus, Trojan horse, programmi e librerie
- Tool per la modifica selettiva dei file di log del sistema

Documenti fisici e digitali

Documenti fisici:

- La copia è distinguibile dall'originale
- L'alterazione lascia tracce
- La "prova" di autenticità si basa su caratteristiche fisiche (firma, ceralacca, …)

Documenti digitali

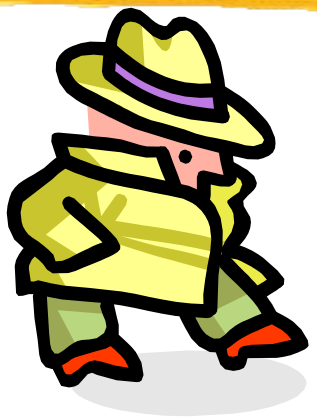
- La copia è indistinguibile dall'originale
- L'alterazione non lascia tracce
- La "prova" di autenticità non si basa su caratteristiche fisiche

Sicurezza Dati: obiettivi

- Confidenzialità
- Autenticazione
- Non-ripudio
- Controllo Accessi
- Integrità
- Anonimia
- Disponibilità Risorse

Confidenzialità

Privacy, Segretezza



Informazioni { trasmesse / memorizzate

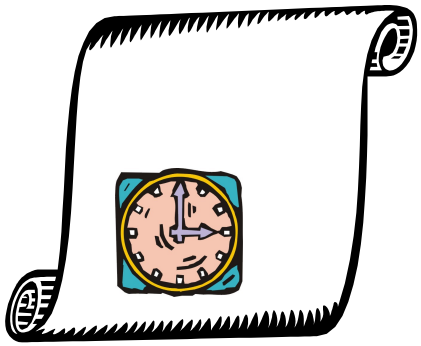
sono accessibili in lettura
solo da chi è autorizzato

Autenticazione

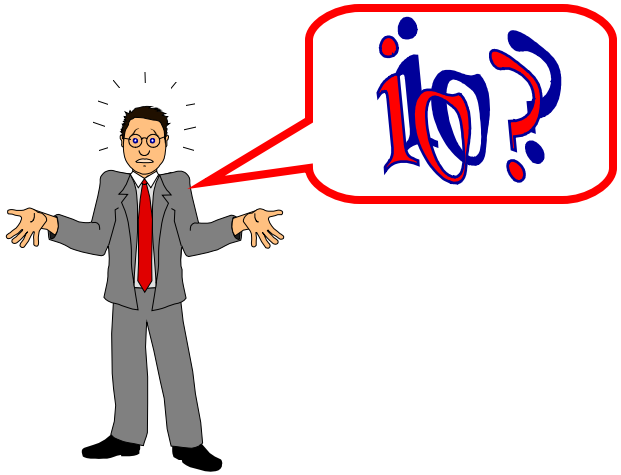
messaggi

entità
(Identificazione)

tempo
(Timestamp)



Non-ripudio



Chi invia
Chi riceve

non può negare la trasmissione del messaggio

Controllo Accessi

Accesso alle informazioni

controllato da o per

il sistema

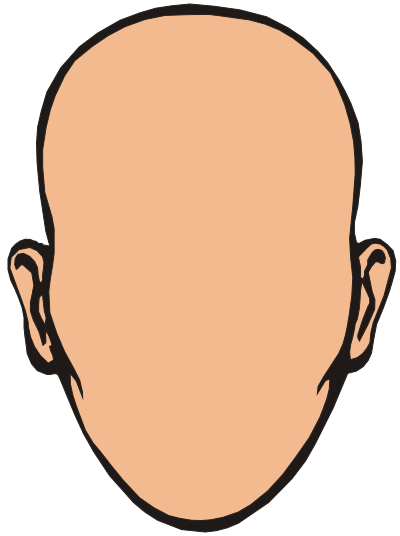
Integrità

Solo chi è autorizzato può modificare l'attività di un sistema o le informazioni trasmesse

modifica = scrittura, cambiamenti, cancellazione, creazione, ritardi, replay e riordino di messaggi, ...

Anonimia

Protezione dell'identità o del servizio utilizzato



Disponibilità Risorse

Risorse disponibili a chi è autorizzato quando necessario

Diverse attese:

- presenza di oggetti e servizi utilizzabili
- capacità di soddisfare le richieste di servizi
- progresso: tempo di attesa limitato
- adeguato tempo del servizio

Contenuto Corso

- Prima parte: Crittografia
  - Cifrari simmetrici
  - Cifrari asimmetrici
  - Firme digitali
  - Funzioni hash e integrità dei dati
  - Protocolli crittografici

Crittografia

Dall'antichità fino a pochi anni fa:

- Essenzialmente comunicazioni private
- Usi Militari e Diplomatici

χρυπτοσ γραφια λογοσ

Oggi: studio di tecniche ed applicazioni che dipendono dall'esistenza di problemi difficili

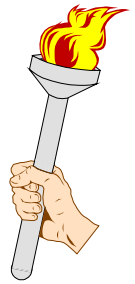
Alcuni metodi antichi di cifratura

Erodoto

Scytala spartana, 500 a.C. (Plutarco in *Vite parallele*)

Polibio

	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z



testo in chiaro: C A S A

testo cifrato: (1,3) (1,1) (4,3) (1,1)

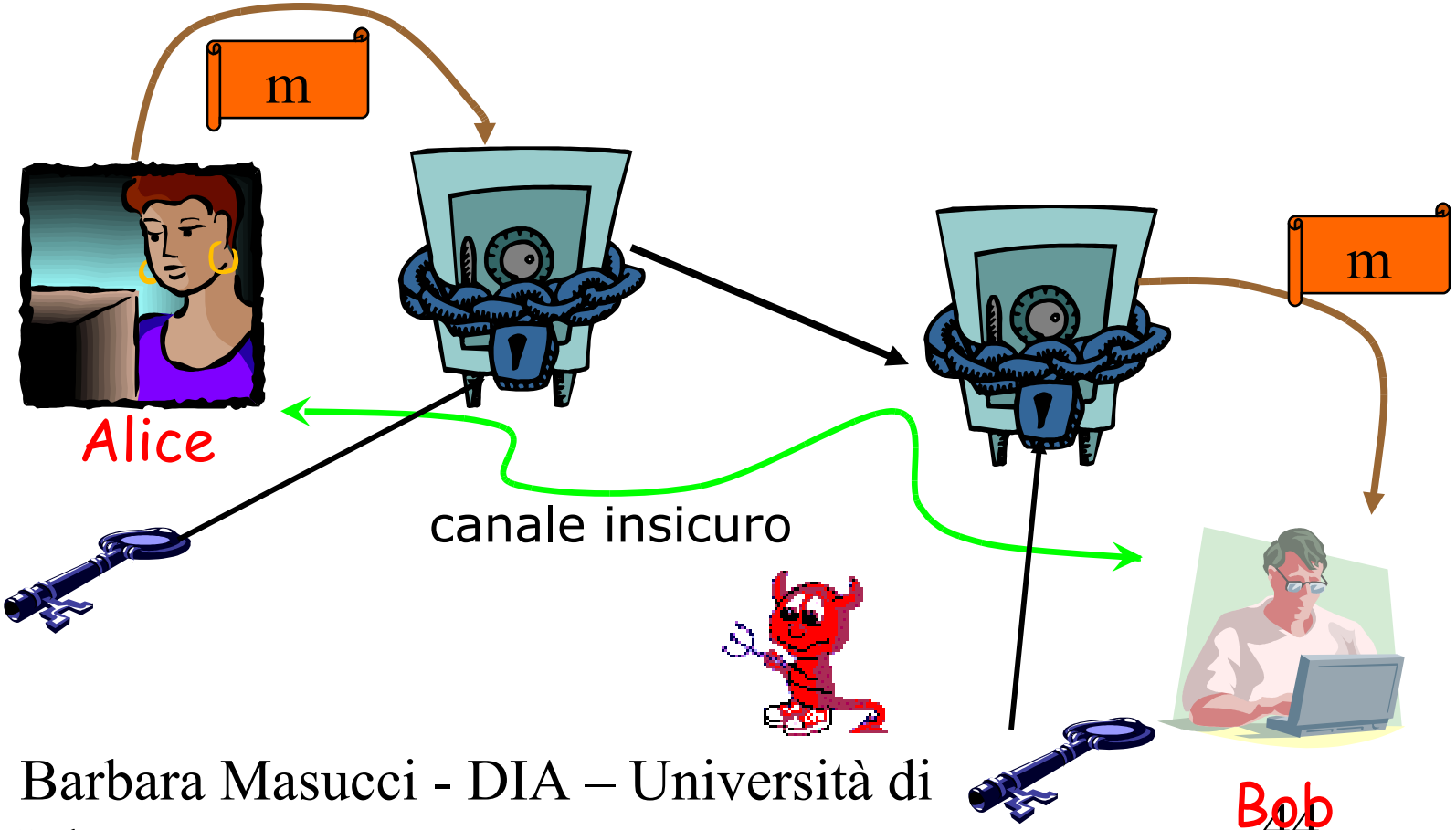
Cifrari simmetrici

Alice

canale insicuro

Bob

Cifrari simmetrici



Cifrari simmetrici

chiave privata k

chiave privata k

C ← CIFRA(k,M)

Alice

C

canale insicuro

M ← DECIFRA(k,C)

Bob

messaggio M

Principio di Kerckhoffs

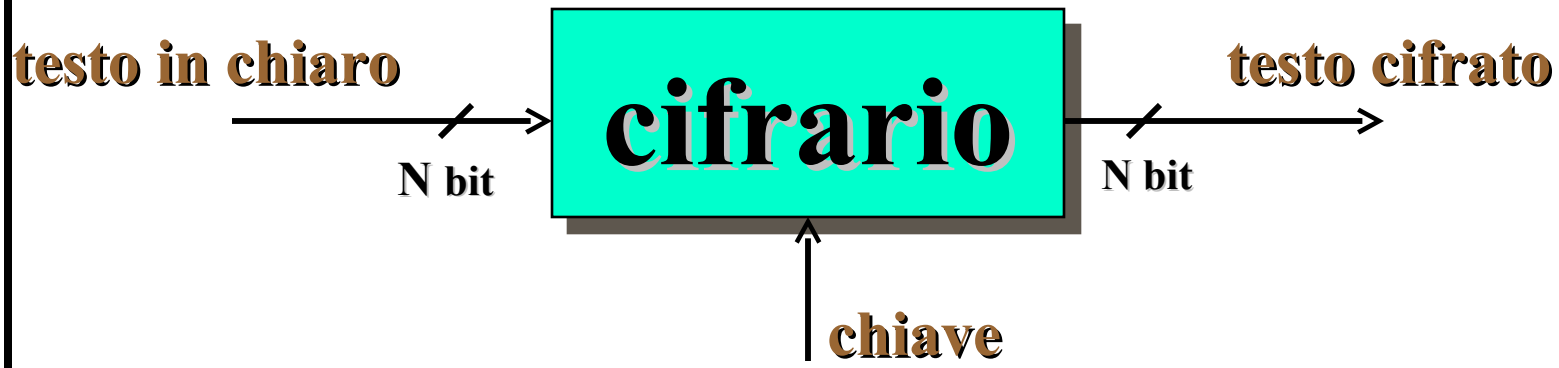
La sicurezza di un cifrario deve dipendere **solo** dalla segretezza della chiave e **non** dalla segretezza dell'algoritmo usato.

Jean Guillaume Hubert Victor Francois Alexandre Auguste Kerckhoffs von Nieuwenhof (1835-1903), filologo olandese, *"La Criptographie Militarie"* [1883]

Cifrari simmetrici

- Cifrari a blocchi
  - Messaggi divisi in blocchi e poi cifrati
- Stream cipher
  - Messaggi cifrati carattere per carattere

Cifrari a blocchi che vedremo

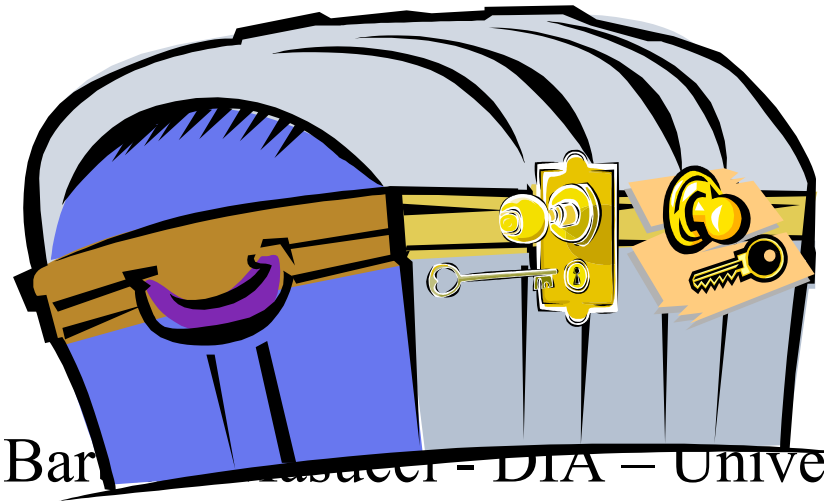


Data Encryption Standard (DES)
DES triplo, RC2, RC5, RC6, Blowfish,
Advanced Encryption Standard (AES)
e poi … Modalità di cifratura

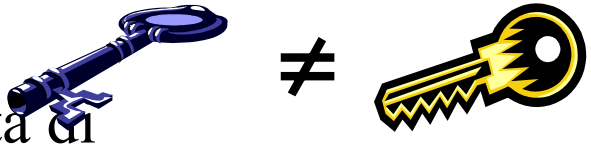
Cifrari asimmetrici

Usano una cassaforte con due lucchetti

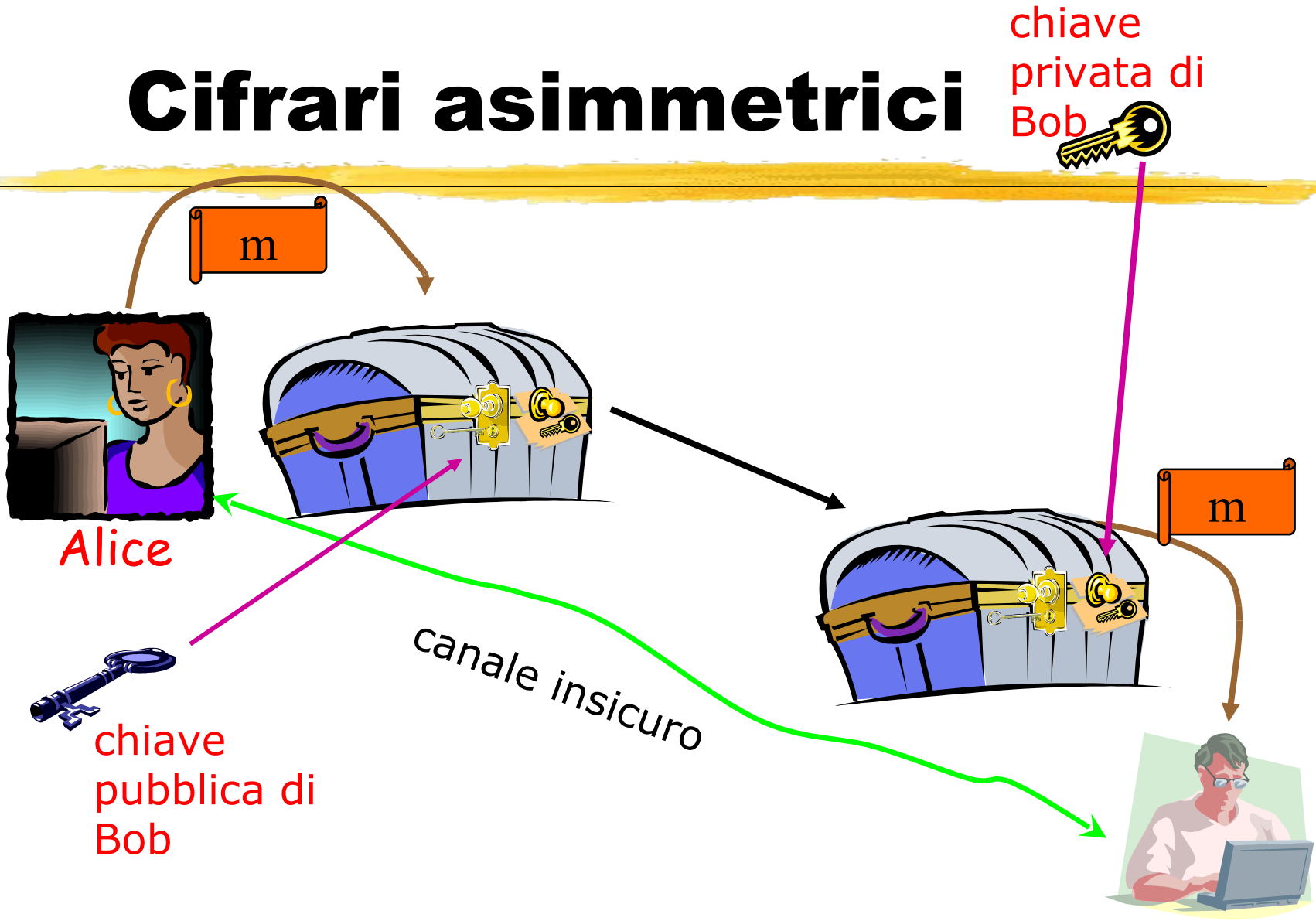
- Con una chiave (pubblica) chiudiamo la cassaforte
- Con l'altra chiave (privata) apriamo la cassaforte



Public key ≠ Private key



Cifrari asimmetrici



Cifrari asimmetrici

chiave privata
kpriv

Alice

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Cifratura

chiave privata
kpriv

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Alice

canale insicuro

Bob

Devo cifrare il messaggio M ed inviarlo ad Alice

Cifratura

chiave privata
kpriv

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Alice

C

canale insicuro

Bob

Cifratura di M per Alice

C ← **CIFRA** (kpub, M)

Decifratura

Devo decifrare il messaggio cifrato **c**

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Alice

Decifratura

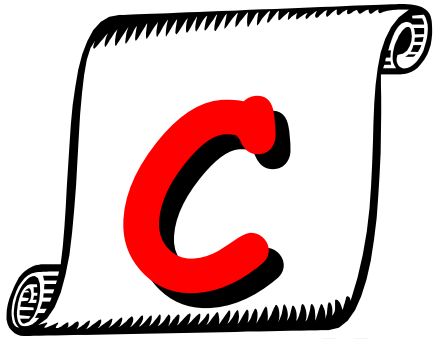
chiave privata
kpriv

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Decifratura di C
M ← DECIFRA (kpriv, C)

Alice



Cifrari asimmetrici

Chiunque può cifrare un messaggio per Alice

Solo Alice può decifrare un messaggio cifrato per lei

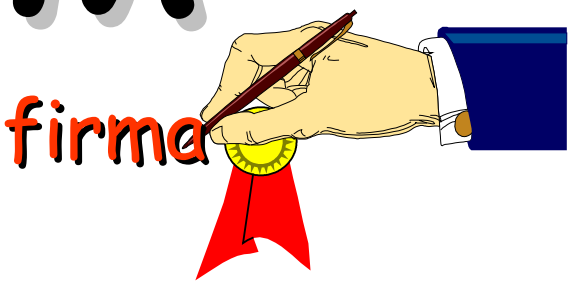
Non ci sono chiavi condivise tra Alice e Bob

- Ciascuno dei due utente genera da solo la propria coppia di chiavi e rende pubblica la chiave pubblica

Ogni utente memorizza una sola chiave (privata)

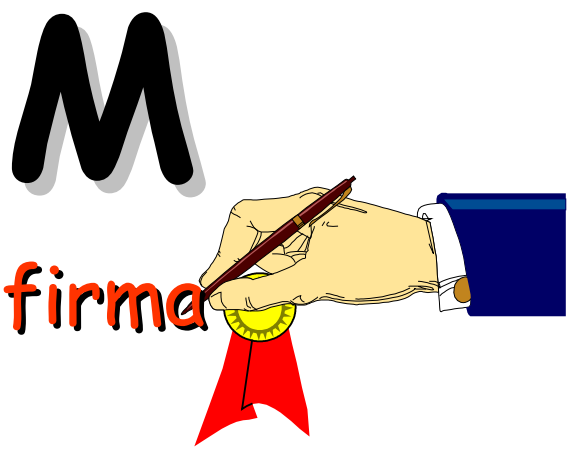
Firma Digitale

M



Equivalente alla firma convenzionale

Firma Digitale

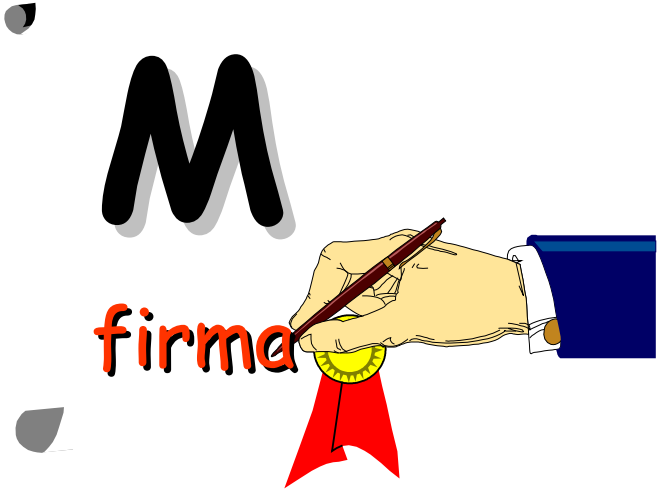


Equivalente alla firma convenzionale

Soluzione naive:

incollare firma digitalizzata

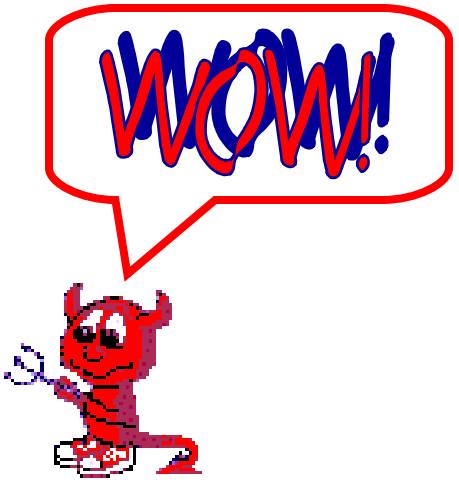
Firma Digitale



Equivalente alla firma convenzionale

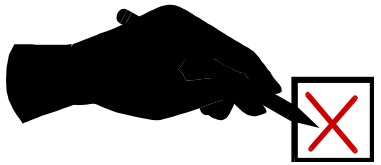
Soluzione naive:

incollare firma digitalizzata



Requisiti per la Firma Digitale

La firma digitale deve poter essere facilmente prodotta dal legittimo firmatario



Nessun utente deve poter riprodurre la firma di altri

Chiunque può facilmente verificare una firma

Firma digitale

Alice

chiave privata
kpriv

M
Alice
??

Devo firmare M

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Firma digitale

chiave privata
kpriv

Alice

M
Alice

F

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Firma di M

F ← FIRMA (M,kpriv)

Firma digitale

chiave privata
kpriv

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Alice

M
Alice

F

(M,F)

canale insicuro

Bob

Verifica firma digitale

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Devo verificare se F
è una firma di Alice per M

Bob

Verifica firma digitale

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Verifica firma di M

vera se **VERIFICA** (**F**,M,kpub) = SI
falsa altrimenti

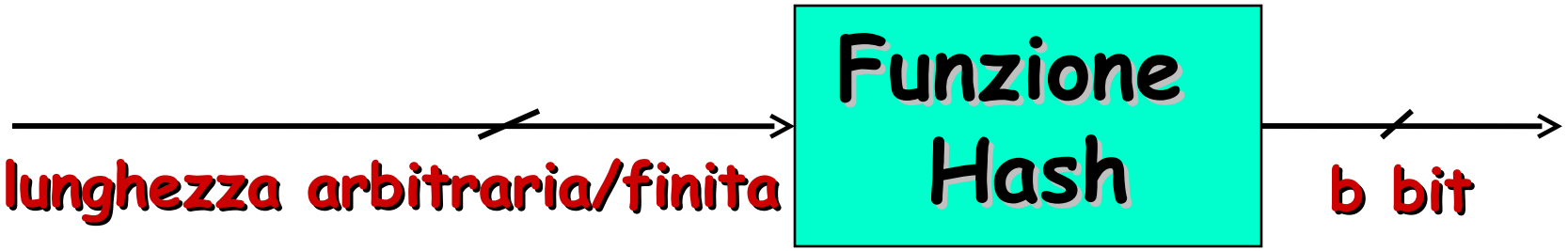
Bob

Firme digitali che vedremo

RSA

Digital Signature Standard (DSS)

Funzioni Hash



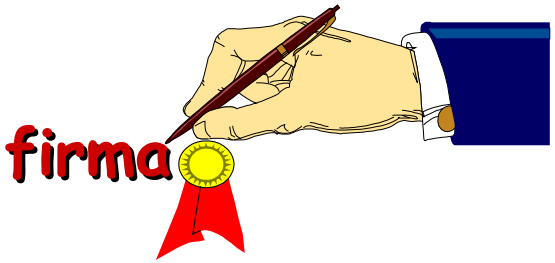
Idea alla base:

il valore hash h(M) è una rappresentazione non ambigua e non falsificabile del messaggio M

Proprietà: comprime ed è facile da computare

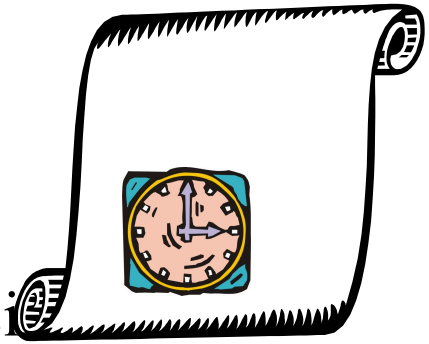
Uso delle funzioni hash

Firme digitali



Integrita' dei dati

Certificazione del tempo



Firme digitali e Funzioni hash

Problema: firma digitale di messaggi lunghi

Soluzione naive: Divisione in blocchi e firma per ogni blocco

problema per la sicurezza: una permutazione/composizione delle firme è una nuova firma

Soluzione di uso corrente:

firmare il valore hash del messaggio

[firma di M] = $F_k(h(M))$

Vantaggi: integrità dei dati ed efficienza degli algoritmi

Integrità dei dati e Funzioni hash

Tipico uso delle funzioni hash

Computo al tempo T il valore hash del file M

Conservo H = h(M) in un luogo sicuro

Per controllare se il file è stato successivamente modificato, calcolo h(M´) e verifico se H = h(M´)

h(M) è l'impronta digitale del file

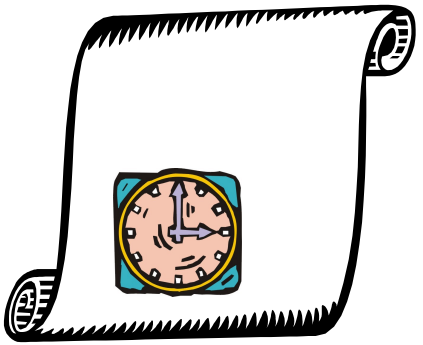
Assicura se un file è stato modificato!

Certificazione del tempo e Funzioni Hash

Il notaio digitale

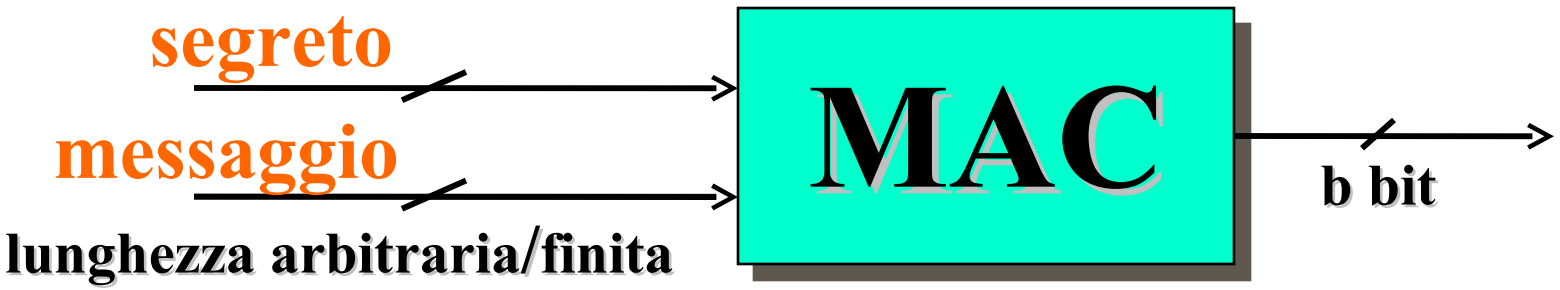
Quando è stato creato

il documento **D** ?



MAC

Message Authentication Code

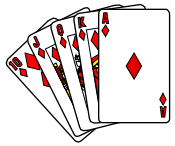


Integrità dei dati

Autenticità dei dati

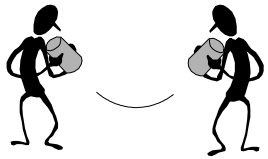
Protocolli crittografici

Lancio di una moneta 

Poker 

Moneta elettronica 

Elezioni 

Condivisione di segreti 

Email certificata 

Crittografia visuale 

Contenuto Corso

- Seconda parte: Sicurezza su Reti
  - Public Key Infrastructure
  - Autenticazione utente
  - Sicurezza della posta elettronica
  - Sicurezza e anonimia nel WEB
  - Strumenti per la sicurezza delle reti
  - Codice malizioso
  - Firewall

Public Key Infrastructure

- Come vengono distribuite le chiavi pubbliche?
- Chi ci assicura che una chiave pubblica è quella di un prefissato utente?

Public Key Infrastructure

Mondo fisico

- Carta di identità
  - Un'autorità riconosciuta lega un nome ad una foto

Mondo digitale

- Certificato digitale
  - Un'autorità riconosciuta lega un nome ad una chiave

Public Key Infrastructure

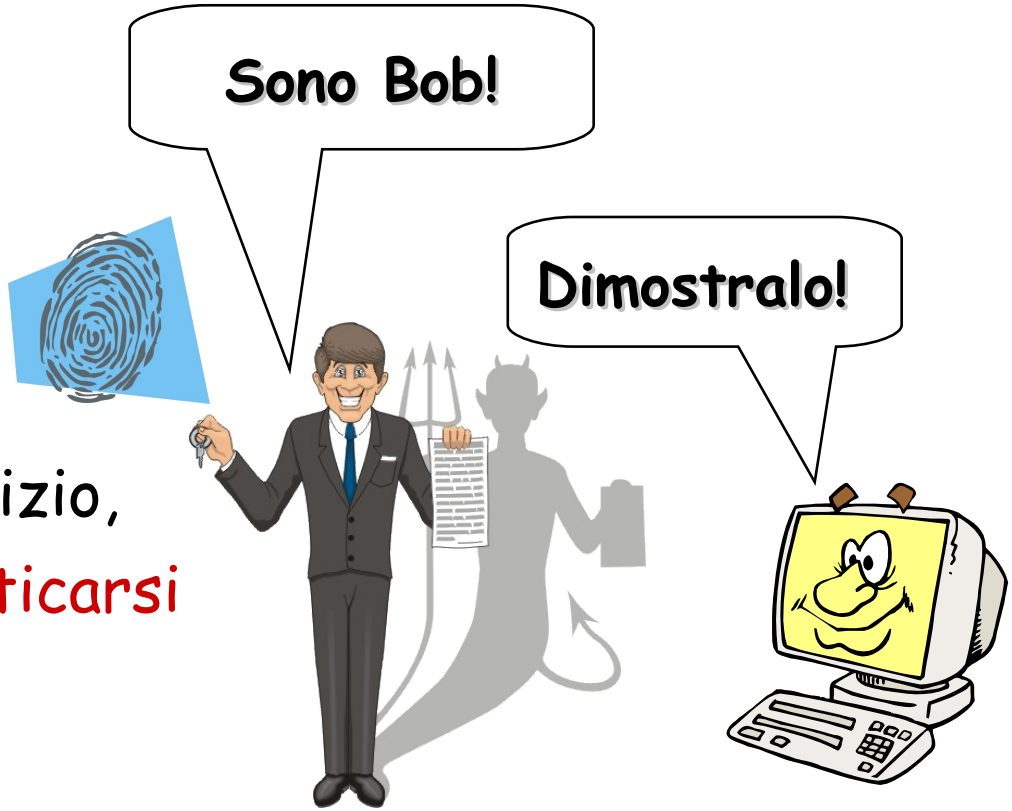
Insieme di hardware, software, procedure, politiche, per

- Creare
- Gestire
- Memorizzare
- Distribuire
- Revocare

certificati digitali

Autenticazione utente

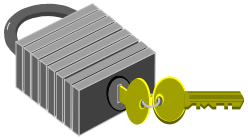
Per utilizzare un servizio, un utente deve autenticarsi



Autenticazione utente: Principi

Qualcosa che l'utente **POSSIEDE**

- cose fisiche o elettroniche, …



Qualcosa che l'utente **CONOSCE** .

- password, PIN,…

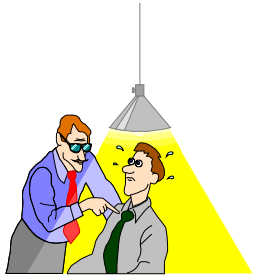
Qualcosa che l'utente **E´** (o come si comporta)

- **biometria**, cioè misura di proprietà biologiche

Autenticazione utente: Caratteristiche

- Sicurezza
- Tempo dell'autenticazione (password, analisi DNA,…)

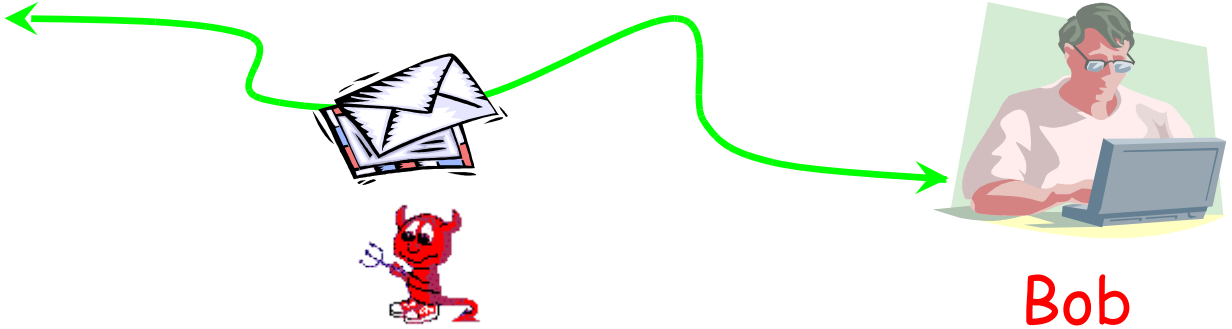
- Costo
- Complessità dell'update (riconoscimento vocale,…)
- Affidabilità e Mantenibilità
- Fattori psicologici:
  - accettabilità, facilità d´uso, …



Sicurezza e-mail

I messaggi inviati per e-mail possono essere intercettati e falsificati

Alice



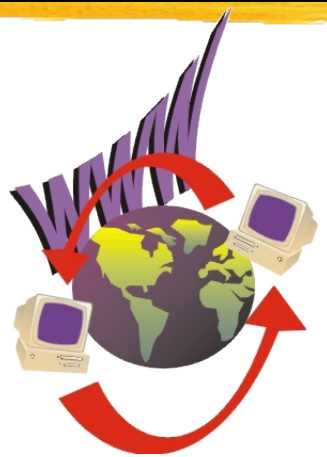
Bob

Possibili soluzioni:

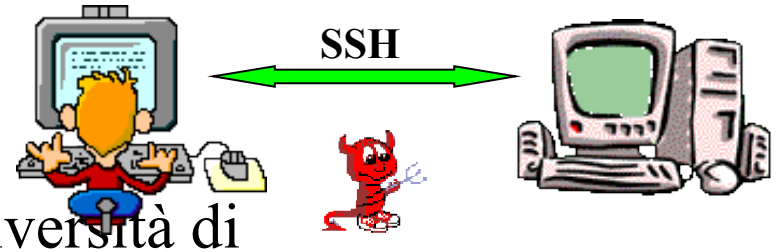
- PGP
- S/MIME

Sicurezza sul WEB

- Protocollo SSL
  - Consente alle applicazioni client/server di comunicare in modo sicuro
  - Utilizzato per il commercio elettronico e l'accesso riservato ai dati



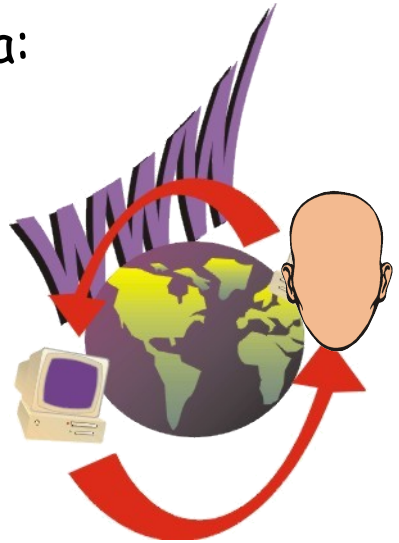
- Protocollo SSH
  - Consente il login remoto sicuro e altri servizi di rete sicuri su un canale insicuro
  - Nato per rimpiazzare i comandi Berkeley r* con le rispettive versioni sicure



Anonimia sul WEB

- Internet non garantisce l'anonimato
  - Ogni computer connesso ad Internet ha un indirizzo IP unico

- Alcune tecniche per mantenere una certa anonimia:
  - Remailers
    -Invio di posta elettronica con mittente anonimo
  - Crowds, Anonymizer
    -Accesso anonimo a siti WEB
  - Autenticazione Anonima
    -Accesso anonimo a risorse



Strumenti per la sicurezza delle reti

Packet sniffer

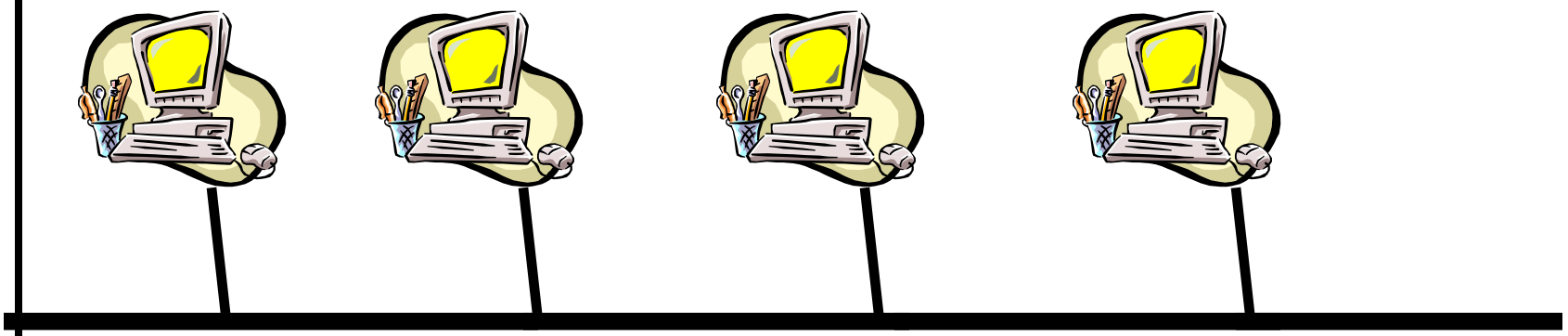
Port scanner

Tripwire

Packet sniffing

In ambienti distribuiti:

- Le risorse sono dislocate in punti diversi di una rete
- Spesso più macchine condividono delle risorse
- I dati transitano ripetutamente attraverso la rete ed alcuni suoi nodi



Modalità normale

Consente solo all'interfaccia del destinatario di passare i dati allo strato superiore

Modalità promiscua

Permette ad una macchina l'ascolto di
tutto il traffico di rete

Cosa è uno Sniffer?

- Qualsiasi strumento, software o hardware, che raccoglie le informazioni che viaggiano lungo una rete

- Usato per
  - Monitorare il funzionamento e le performance della rete
  - Visualizzare dati altrui
    - Password
    - Numeri di carte di credito
    - Dati segreti

Rischi

PRIVACY

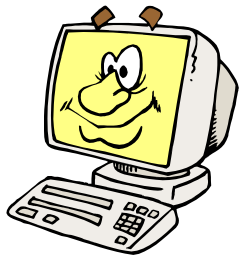
SICUREZZA

Probing

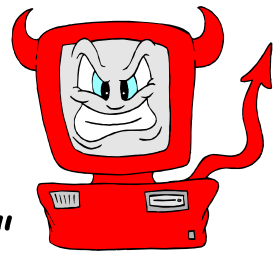
- Nei server su reti TCP/IP i servizi di rete sono associati ad un numero di porta
  - Server di posta elettronica: porta numero 25
  - Server ftp: porta numero 21
  - Server http: porta numero 80
- Accede a questi servizi chi è autorizzato
- Tuttavia un intruso potrebbe
  - Utilizzare il servizio come "porta" per accedere alla macchina, e persino ottenerne il controllo
  - Bloccare il servizio, o la macchina, per impedirne l'utilizzo
  - Utilizzare illecitamente il servizio "fingendosi" un utente autorizzato

Probing

- Un client onesto
  - Si connette al server indicando il numero di porta del servizio a cui è interessato
  - Dialoga con il server attraverso un protocollo stabilito



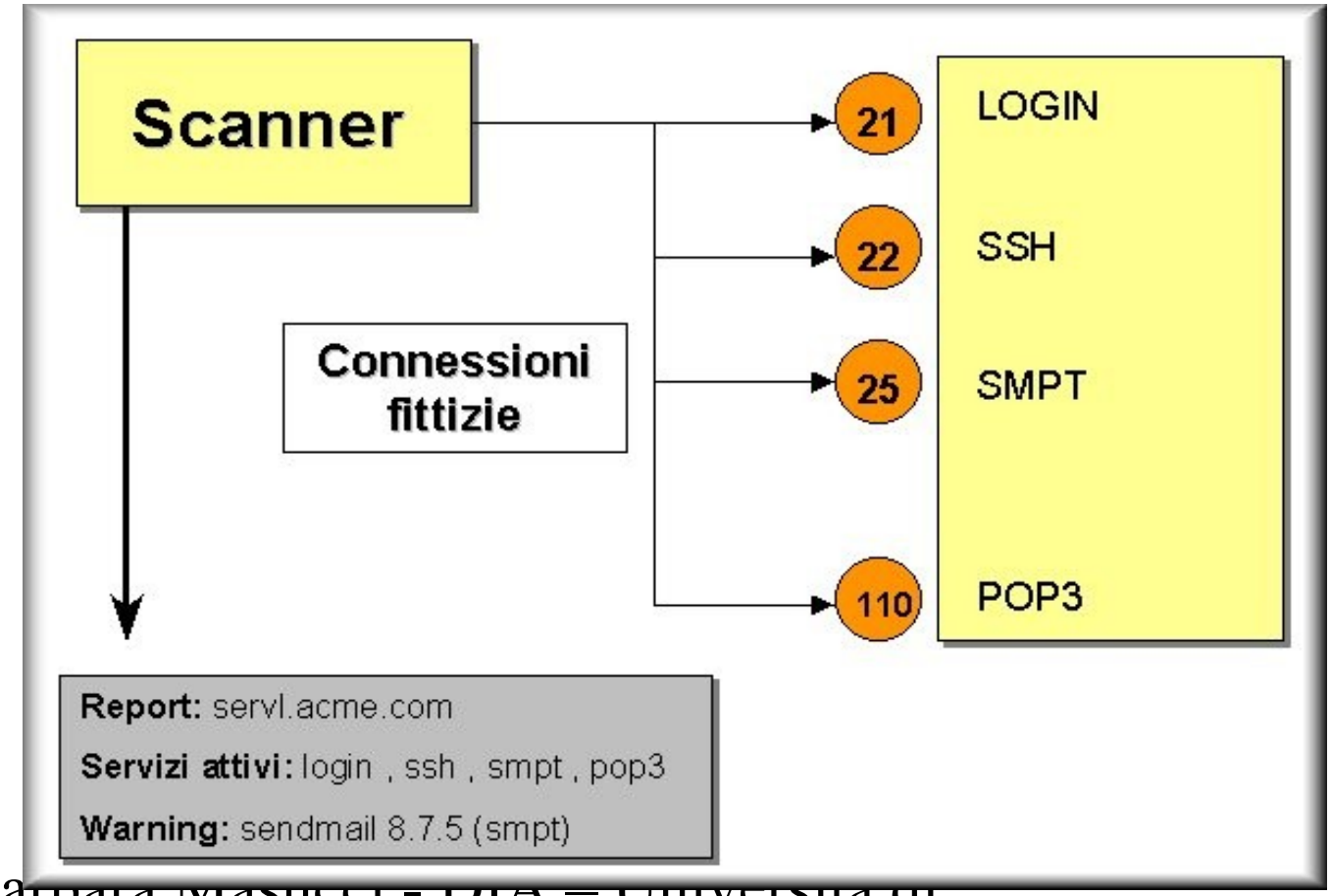
- Un client fraudolento
  - Si connette come un normale client
  - Invia messaggi "strani" che possono indurre il server a bloccarsi o eseguire codice "pericoloso"



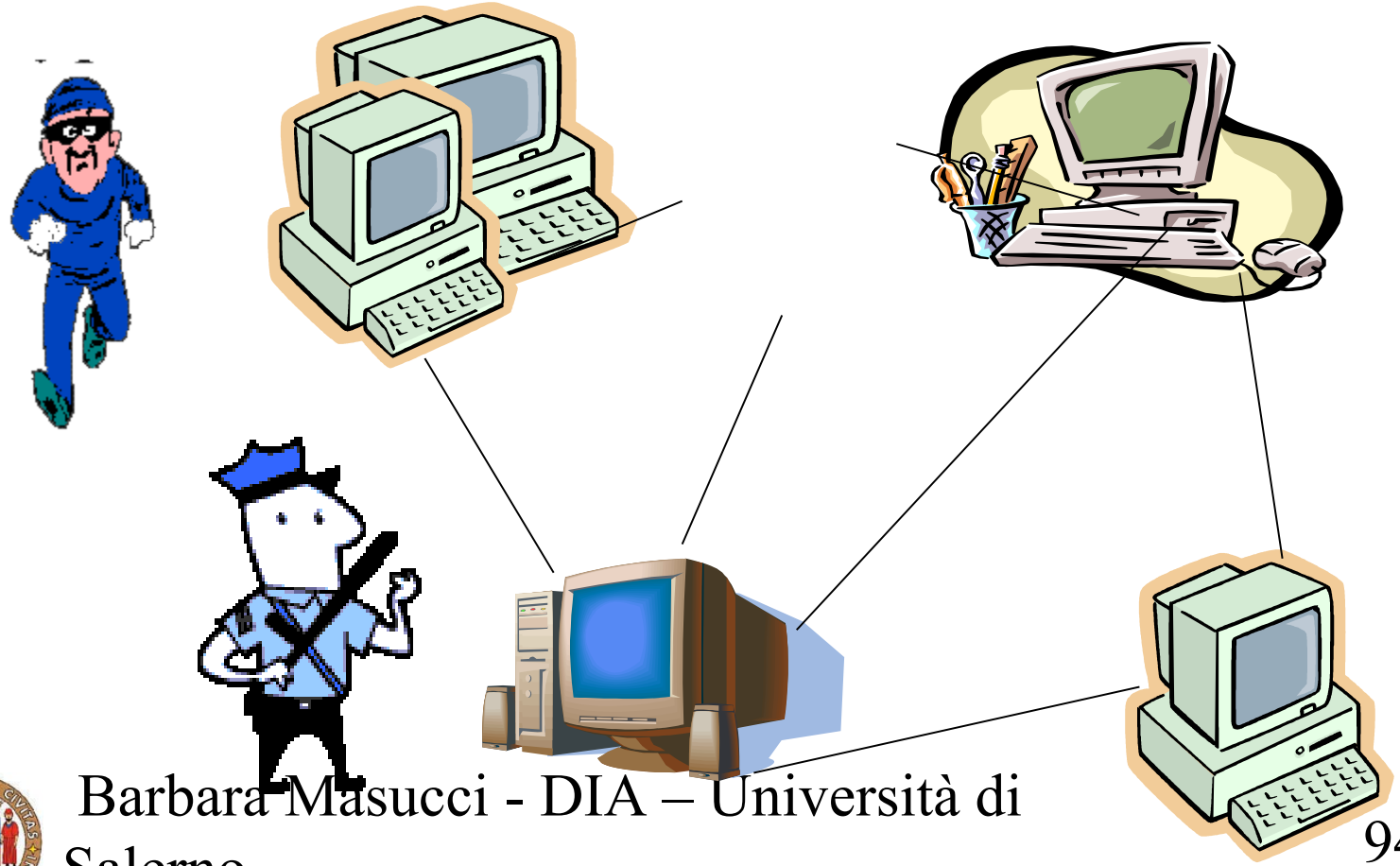
Probing e scanning

- Mediante un software di probing
  - il pirata può ottenere informazioni sul sistema allo scopo di sfruttarne le vulnerabilità
  - l'amministratore di rete può verificare la robustezza dei servizi e delle macchine e scoprire eventuali attività sospette
- Una diffusa tecnica di probing e' detta port scanning
  - Simula connessioni ai servizi di rete, scandendo tutte le porte per appurare quali servizi sono attivi
  - Per ciascun servizio identifica il tipo di server e ne determina il grado di vulnerabilità

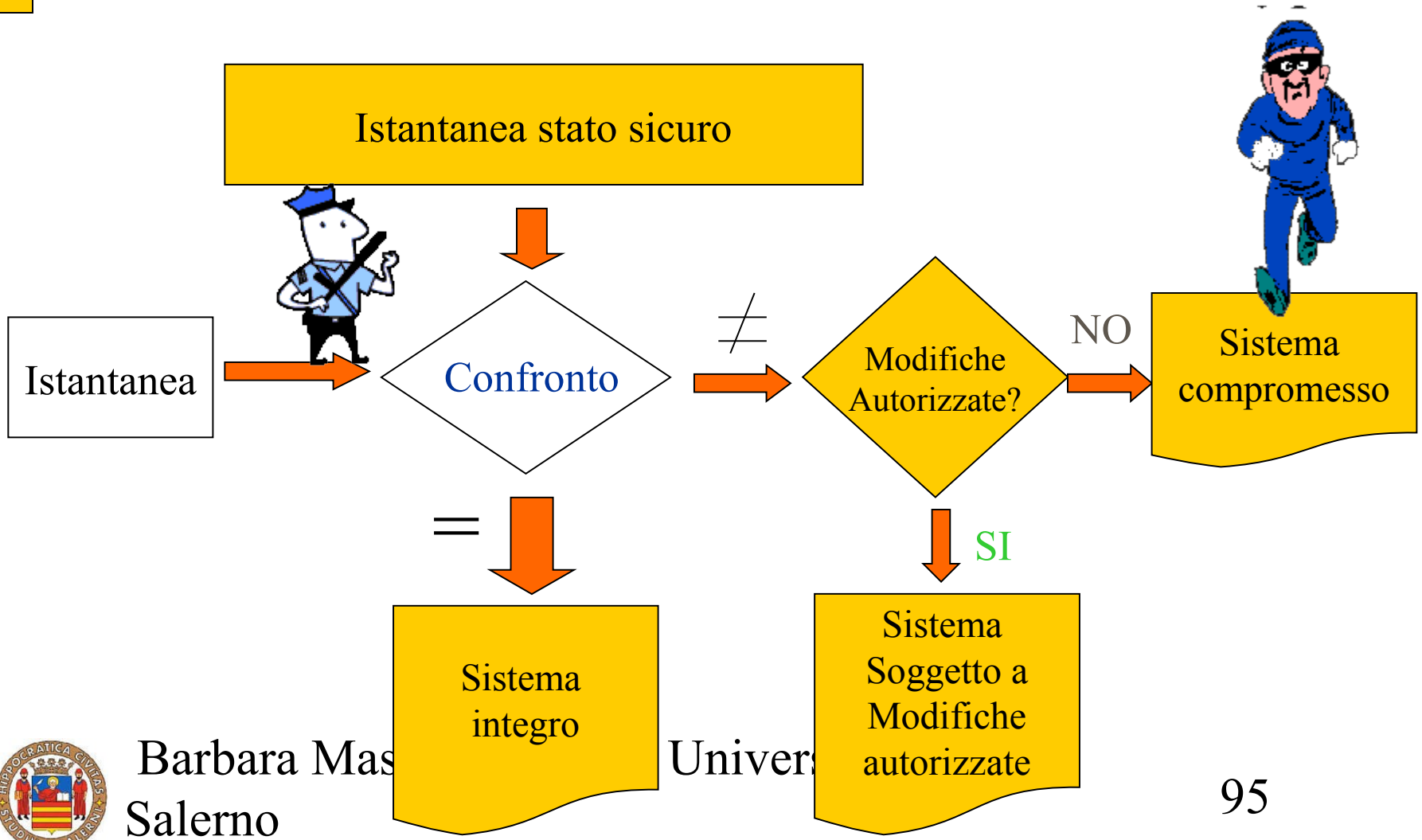
Scanning di un server



Tripwire



Tripwire


Istantanea stato sicuro
Istantanea
Confronto
≠
Modifiche Autorizzate?
NO
Sistema compromesso
=
SI
Sistema integro
Sistema Soggetto a Modifiche autorizzate

Codice “malizioso”

Virus

Cavalli di Troia

Macrovirus

Codice “malizioso”

- Dopo una violazione del sistema, un intruso potrebbe installare del codice per
  - sottrarre dati riservati
  - muovere attacchi verso altre macchine

- Tale codice può anche sostituire comandi di sistema
  - Sostituzione di sendmail con una nuova versione che memorizza in un file i messaggi inviati dall’utente
  - Sostituzione di ls con una nuova versione che non visualizza il file creato dal sendmail fasullo

Codice “malizioso”

- Altro metodo per l’installazione o esecuzione di software malizioso su una macchina
  - indurre un utente/amministratore a scaricarlo dalla rete ed eseguirlo (anche inconsapevolmente)
- Un’applicazione tipica di questo approccio sono

  i Virus
  - Programmi che penetrano in un programma ospite modificandolo, per riprodursi e danneggiare dati e/o programmi

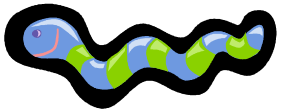
Il termine "Virus"

- David Gerrold, 1972
  - Nel libro "When Harlie Was One" viene descritto un programma chiamato virus creato da uno scienziato pazzo
    - Il computer infettato provava a contattare un altro computer via telefono
    - Entrava in quel sistema e lo infettava con una sua copia
    - Si infiltrava nel software di sistema e lo rallentava fino a renderlo inutilizzabile
    - Antivirus Vaccine creato dall'inventore a scopo di lucro
- Fred Cohen
  - Il primo a definire in modo formale il concetto di virus
  - "a program that can infect other programs by modifing them to include a possibly evolved copy of itself "

Virus e simili

- **Cavallo di Troia**
  - Programma apparentemente legale che contiene istruzioni che realizzano funzioni non richieste dell'utente (anche dannose)

- **Worm**
  - Programma che si ricopia su reti di computer sfruttando bug del sistema operativo
  - Non necessita di un programma portatore



- **Virus**
  - Porzioni di codice autoreplicante
  - Boot virus, macrovirus, etc…

Macrovirus

- Virus scritti come macro di applicazioni utente
  - Macro: insieme di istruzioni usate per automatizzare compiti
- Possono essere eseguiti all'atto dell'apertura di un documento

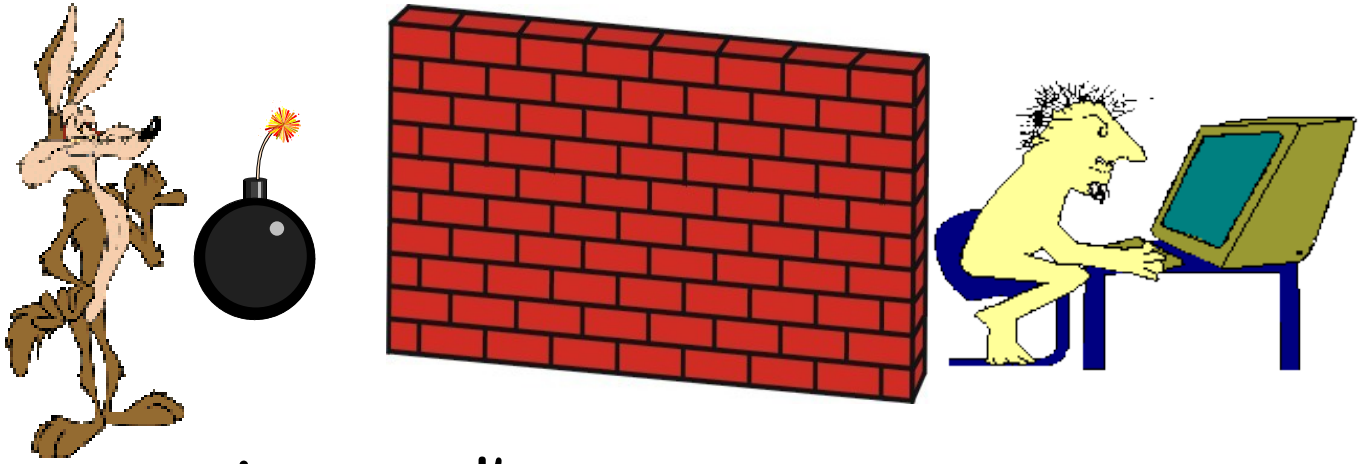
- Esempi: Melissa e I Love You
  - Scritti in VBS
  - Si trasmettono via E-Mail
  - Accedono e modificano il file registro di Windows

Difendersi dai virus

- Utilizzare/installare software solo se di provenienza fidata
- Microsoft e Sun hanno proposto alcuni sistemi per la certificazione (mediante firma digitale) dell'affidabilità di ActiveX ed Applet
- Molti Anti Virus possono verificare la presenza di file infetti anche quando questi sono giunti sul sistema come allegati di posta elettronica

Firewall

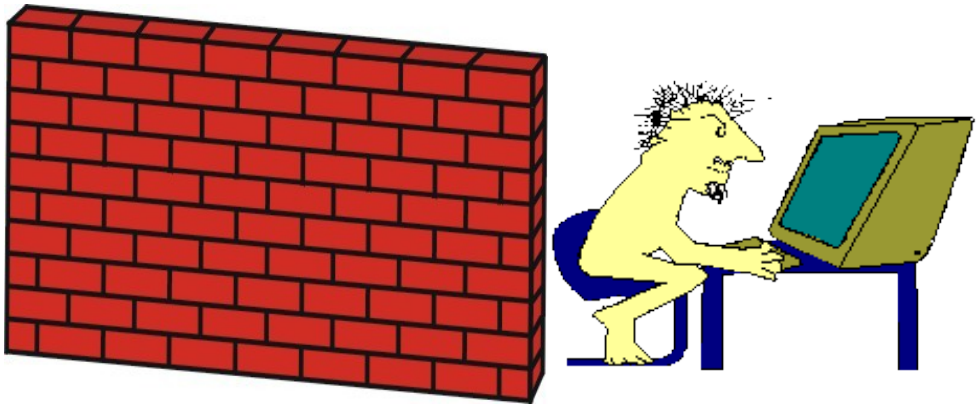
Fire wall: A fireproof wall used as a barrier to prevent the spread of a fire. - American Heritage Dictionary



"Modo per restringere l'accesso tra Internet e la rete interna"

Firewall

Fire wall: A fireproof wall used as a barrier to prevent the spread of a fire. - American Heritage Dictionary



"Modo per restringere l'accesso tra Internet e la rete interna"