Sicurezza su Reti

Alfredo De Santis

Università di Salerno

http://www.dia.unisa.it/~ads

ads@unisa.it

Orari Corso

- Martedi 11:00 - 13:00, aula A10/11
- Giovedi 9:00 - 11:00, aula A10/11
- Venerdi 15:00 - 18:00, aula A10/11

Organizzazione

- Bibliografia
  - Appunti dalle lezioni
  - http://www.dia.unisa.it/~ads/corso-security/www
- Laboratorio
- Progetti
  - Presentazione di argomenti specifici
- Compitini di valutazione

Interazione

Prerequisiti

- Teoria dei Numeri
- Fondamenti di Reti

Prerequisiti

- Teoria dei Numeri
- Fondamenti di Reti

... ma faremo un veloce riepilogo

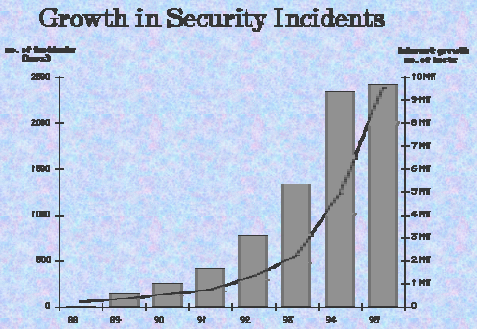
Elenco studenti

- Per l'organizzazione del corso (prove, progetti, laboratorio)
- Nome, Cognome, matricola

Ed ora …

qualcosa sui contenuti

Incidenti riportati al CERT



Indagini FBI

- Nel 1998:
  - 3.700 denunce per intrusioni
  - 547 indagini aperte
  - 56 condanne
  - 12 condanne in prigione

  Si rischia fino a 5 anni per incidente e multa di $250.000
- Nel 1999:
  - 8.268 denunce per intrusioni
  - 1.154 indagini aperte

Indagine CSI/FBI

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 …

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 minacce

- Interruzione risorsa distrutta, inutilizzabile (distruzione di hardware, cancellazione di software o file dati, malfunzionamento del sistema operativo, …)
- Intercettazione accesso non autorizzato a dati o componenti del sistema
- Modifica di dati o componenti del sistema
- Contraffazione di oggetti in un sistema (aggiunta di messaggi falsi alla comunicazione, record a data base, …)

Computer System assets

hardware

software dati

Sicurezza Dati: obiettivi

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

Confidenzialità

Privacy, Segretezza

Informazioni { trasmesse / memorizzate

(anche la semplice esistenza di un oggetto)

sono accessibili in lettura

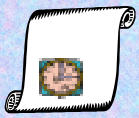
solo da chi è autorizzato

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.

… meglio "Grado di anonimia"

Disponibilità Risorse

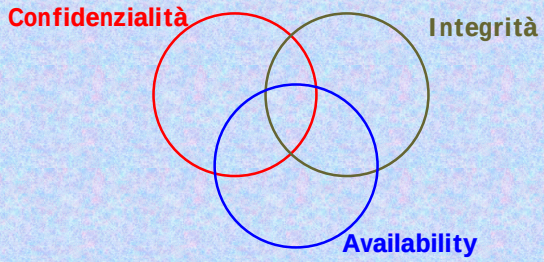
Risorse disponibili a chi è autorizzato quando necessario

Availability

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

Obiettivi:
- risposta pronta
- allocazione fair
- utilizzabilità
- fault tolerance
- concorrenza controllata (accessi simultanei, gestione deadlock, accesso esclusivo)

Alcune relazioni



Attacchi su rete

- Tipico attacco:
  - ottenere accesso all'account di un utente
  - ottenere accesso privilegiato
  - usare il sistema compromesso come base per attaccare altri macchine

E' possibile manualmente in 45 secondi

…automaticamente in meno!

Intrusioni

Vari tipi di *intruder*:
- Adolescente curioso
- Studente universitario che ha sviluppato nuovo tool
- "Spia" a pagamento
- Dipendente licenziato o arrabbiato
- …

Ragioni per intrusioni:
- Divertimento
- Senso di potenza
- Sfida intellettuale
- Attenzione politica
- Guadagno economico

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

- Probe
- Scan
- Compromissione di account (privilegiati e non)
- Packet Sniffer
- Denial of Service
- Codice malizioso (Virus, Worm, Troian horse)
- Attacchi all'infrastruttura di rete (name server, access provider, grossi archivi di rete,...)

Tipologia di 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, Troian horse programmi e librerie
  - Tool per la modifica selettiva dei file di log del sistema

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

HACKER noun 1. A person who enjoys learning the details of computer systems and how to stretch their capabilities - as opposed to most users of computers, who prefer to learn only the minimum amount necessary. 2. One who programs enthusiastically or who enjoys programming rather than just theorizing about programming.

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

Hacker: tre tipi

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

Hack = "tagliare", "fare a pezzi"

Origine termine:

- Tech Model Railroad Club, Massachussets Institute of Technology [1958]
- Plastico ferroviario, due gruppi:
  - Modelli treni
  - Signal and Power: segnali e distribuzione energia

Hack = gergo, scherzo, denotava virtuosismo, innovazione

Membri gruppo si definivano Hacker

IBM 704 ... Tx-0 ... PDP-10

Etica dell'Hacker

Hackers: Heroes of the Computer Revolution

- Access to computers - and anything which might teach you something about the way the world works - should be unlimited and total. Always yield to the *Hands-On* imperative.
- All information should be free.
- Mistrust Authority. Promote Decentralization.
- Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
- You can create art and beauty on a computer.
- Computers can change your life for the better.

Contenuto Corso

- Crittografia
- Sicurezza in Reti
  - PKI, E-mail (PEM, PGP), SSL, Anonimia, Firewall, IPsec, VPN, WWW, Java
- Sicurezza nei Sistemi Operativi
  - Unix, Windows NT
- Codice malizioso (Virus, Worm)
- Commercio Elettronico
  - Moneta elettronica, iKP, SET
- Watermark, Smart Card, GSM, WAP
- Laboratorio

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

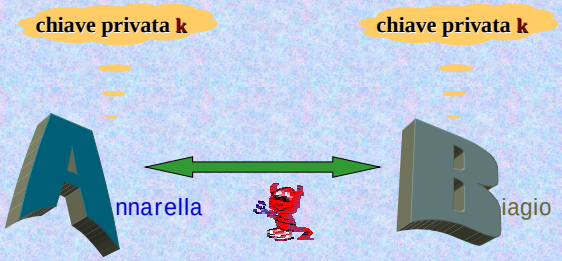
testo in chiaro: C A S A

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

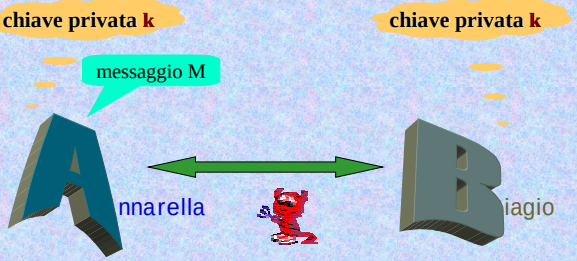
Crittografia: Primitive

- Cifratura
  - Cifrari simmetrici (cifrari a blocchi, stream cipher)
  - Cifrari a chiave pubblica
- Tecniche per autenticazione ed integrità
  - Funzioni Hash
  - MAC
- Firme Digitali
- Tecniche per l'identificazione
- Generazione pseudo-casuale

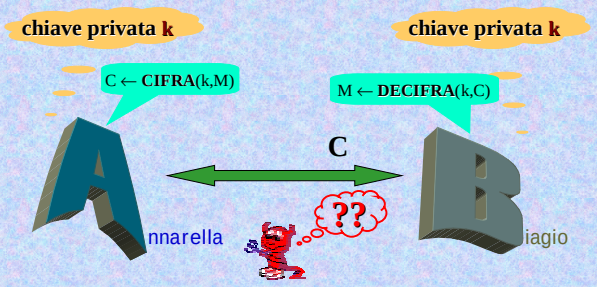
Chiavi simmetriche



Chiavi simmetriche



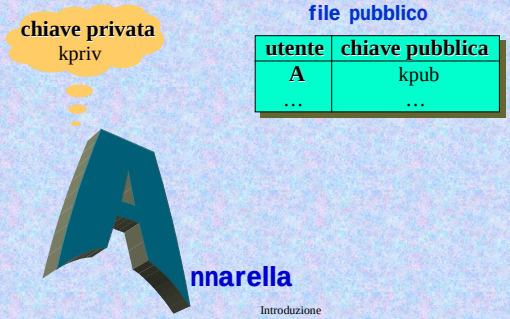
Chiavi simmetriche



Cifrari a blocchi che vedremo

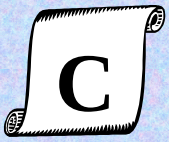
- Data Encryption Standard (DES)
- DES triplo, RC2, RC5, Skipjack
- Advanced Encryption Standard (AES)
  - in particolare RC6 e Rijndael
- e poi … Modalità di cifratura

Crittosistema a chiave pubblica



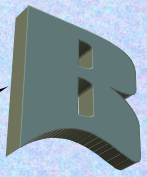
Cifratura

Cifratura



file pubblico

utente	chiave pubblica
A	kpub
…	…



Cifratura di M per **A**
C ← **CIFRA** (kpub, M)

iagio

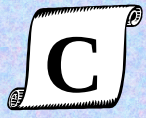
Decifratura

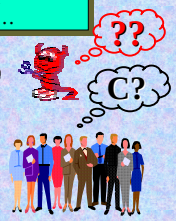
Devo decifrare il messaggio cifrato C

file pubblico

utente	chiave pubblica
A	kpub
…	…

nnarella





Decifratura

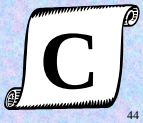
chiave privata
kpriv

file pubblico

utente	chiave pubblica
A	kpub
…	…

Decifratura di C
M ← **DECIFRA** (kpriv, C)

nnarella

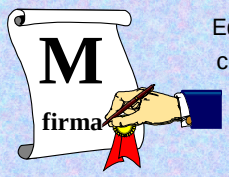


Principio di Kerckhoffs

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

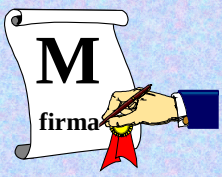
Jean Guillaume Hubert Victor Francois Alexandre Auguste Kerckhoffs von Nieuwenhof (1835-1903), filologo olandese, *"La Criptographie Militarie"* [1883]

Firma Digitale



Equivalente alla firma convenzionale

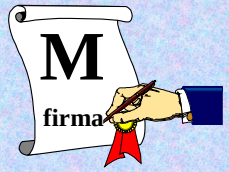
Firma Digitale



Equivalente alla firma convenzionale

Soluzione naive:
incollare firma digitalizzata

Firma Digitale



Equivalente alla firma convenzionale

Soluzione naive:
incollare firma digitalizzata

Desiderata 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

chiave privata
kpriv

file pubblico

utente	chiave pubblica
A	kpub
…	…

Devo firmare M

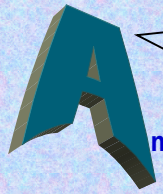
nnarella

Firma digitale

chiave privata
kpriv

file pubblico

utente	chiave pubblica
A	kpub
…	…



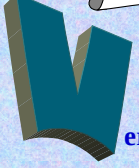
Firma di M
F ← **FIRMA** (M,kpriv)

nnarella

Verifica firma digitale

file pubblico

utente	chiave pubblica
A	kpub
…	…



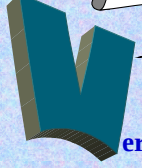
Devo verificare se F è una firma di A per M

erificatore

Verifica firma digitale

file pubblico

utente	chiave pubblica
A	kpub
…	…



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

erificatore

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
- Applicazioni: firme digitali ed integrità dei dati

Firme digitali e Funzioni hash

Problema: firma digitale di messaggi grandi

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

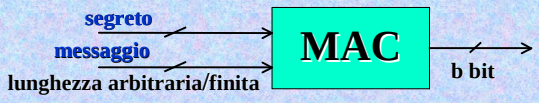
- Computo al tempo T il valore hash del file M
- Conservo H = h(M) in un luogo sicuro
- Per controllare se il file è stato successivamente modificato, calcolo h(M´) e verifico se H = h(M´)

h(M) è l'impronta digitale del file

Assicura se un file è stato modificato!

MAC

Message Authentication Code



Integrità dei dati

Grandi Numeri

- Numero colonne per l'Enalotto $\binom{90}{6} = 622.614.630 \approx 1{,}15 \cdot 2^{29}$
- Microsecondi in un giorno $8.640.000.000 \approx 1{,}26 \cdot 2^{36}$
- Microsecondi in un secolo $\approx 3{,}15 \cdot 10^{15} \approx 1{,}4 \cdot 2^{51}$
- Secondi dalla creazione del sistema solare $\approx 2 \cdot 10^{17} \approx 1{,}38 \cdot 2^{57}$
- Cicli in un secolo di una macchina a 500 MHz $\approx 1{,}57 \cdot 10^{18} \approx 1{,}37 \cdot 2^{60}$
- Cicli in un secolo di una macchina a 1.000 MHz $\approx 3{,}15 \cdot 10^{18} \approx 1{,}37 \cdot 2^{61}$
- Cicli in un secolo di 1.000.000 macchine a 1.000 MHz $\approx 3{,}15 \cdot 10^{24} \approx 1{,}3 \cdot 2^{81}$
- Numeri primi di 75 cifre (cioè 249 bit) $\approx 5{,}2 \cdot 10^{72} \approx 1{,}83 \cdot 2^{244}$
- Numero di elettroni nell'universo $\approx 8{,}37 \cdot 10^{77} \approx 1{,}8 \cdot 2^{258}$

Chiave di 40 bit

Quanto è "sicura" una chiave di 40 bit?

Chiave di 40 bit

Supponiamo di avere una macchina che in un microsecondo prova una singola chiave

Provare tutte le possibili chiavi	≈ 12 giorni 17 ore
Provare 10% delle possibili chiavi	≈ 30.5 ore

Se avessimo 4 macchine …

Provare tutte le possibili chiavi	≈ 3 giorni 4 ore
Provare 10% delle possibili chiavi	≈ 7.6 ore

Chiave di 112 bit

Quanto è "sicura" una chiave di 112 bit?

Chiave di 112 bit

Supponiamo di

- avere 1.000.000.000 macchine a 1.000 MHz
- ognuna prova una singola chiave in un ciclo

Numero chiavi = 2^{112}

Chiavi provate in un anno = $10^9 \bullet 10^6 \bullet 60 \bullet 60 \bullet 24 \bullet 365$
$\approx 3{,}15 \bullet 10^{22} \approx 1{,}67 \bullet 2^{74}$

Provare tutte le possibili chiavi ≈ 164.646.653.302 anni

Provare 1/622.614.630 delle possibili chiavi ≈ 264,44 anni

Numero colonne per l'Enalotto = 622.614.630

Esercizio

Quanto è "sicura" una chiave di 128 bit?