Sicurezza su Reti

Alfredo De Santis

Università di Salerno

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

ads@unisa.it

Orari Corso

- Martedi 15:00 - 18:00, aula C38
- Giovedi 15:00 - 17:00, aula C38
- Venerdi 10:00 - 12:00, aula D19

Organizzazione

- Compitini di valutazione
- Progetti:
  - Appunti dalle lezioni
  - Presentazione di argomenti specifici
  - Laboratorio

- Interazione
- Commenti benvenuti

Disponibilità materiale

http://www.dia.unisa.it/~ads/corso-security/www

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

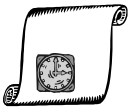
Ed ora …

i contenuti

Sicurezza Dati: obiettivi I

Confidenzialità (Privacy,Segretezza)

Autenticazione

messaggi	entità (Identificazione)	tempo (Timestamp)
		

Sicurezza Dati: obiettivi II

Non-ripudio

Controllo Accessi

Sicurezza Dati: obiettivi III

Integrità

- non-modificato
- modificato solo in modi accettabili
- modificato solo da processi autorizzati
- modificato solo da persone autorizzate
- consistente
- significativo, risultati corretti

Integrità: aspetti caratteristici

- azioni autorizzate
- separazione e protezione di risorse
- rilevamento e correzione di errori

Sicurezza Dati: obiettivi IV

Anonimia

Ricevuta

Informazioni date
Servizi forniti

Sicurezza Dati: obiettivi V

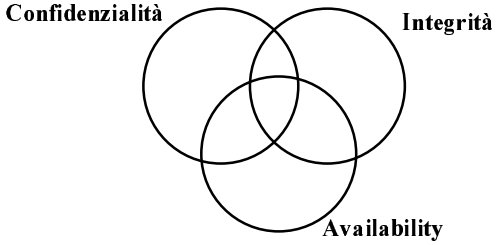
Disponibilità Risorse (Availability)

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

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

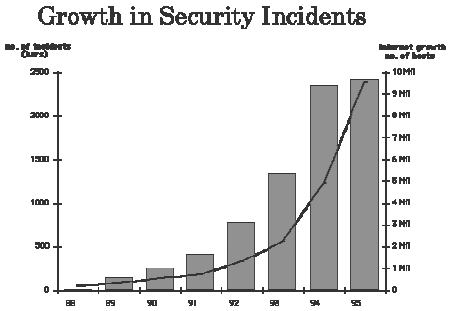
Introduzione 12

Alcune relazioni



Introduzione 13

Incidenti riportati al CERT



Introduzione 14

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

Introduzione 15

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!

Introduzione 16

Intrusioni

- Vari tipi di *intruder*:
  - Adolescente curioso
  - Studente universitario che ha sviluppato un nuovo tool
  - "Spia" a pagamento
  - Dipendente licenziato o arrabbiato
  - …
- Ragioni per intrusioni:
  - Divertimento
  - Senso di potenza
  - Sfida intellettuale
  - Attenzione politica
  - Guadagno economico

Introduzione 17

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*
  - 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

Contenuto Corso

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

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	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

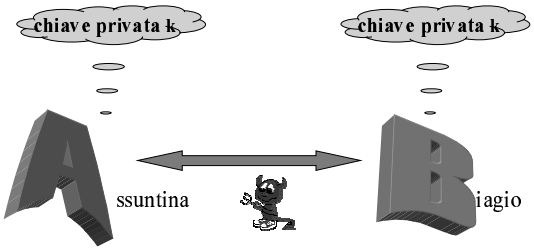
testo in chiaro: C A S A

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

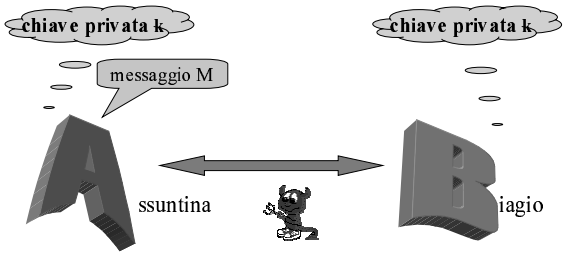
Crittografia: Primitive

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

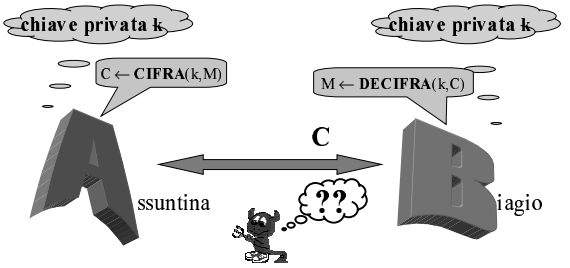
Chiavi simmetriche



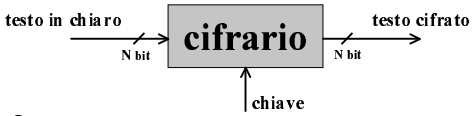
Chiavi simmetriche



Chiavi simmetriche



Cifrari a blocchi che vedremo



- Data Encryption Standard (DES)
- DES triplo
- Advanced Encryption Standard (AES)
  - in particolare RC6
- e poi … Modalità di cifratura

Crittosistema a chiave pubblica

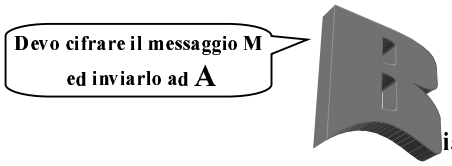
file pubblico

utente	chiave pubblica
A	kpub
…	…

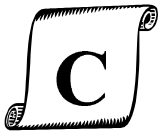
Cifratura

file pubblico

utente	chiave pubblica
A	kpub
…	…

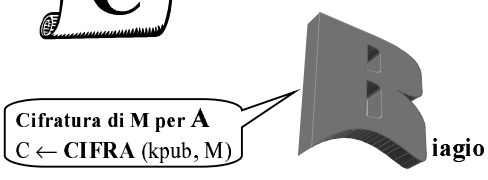


Cifratura

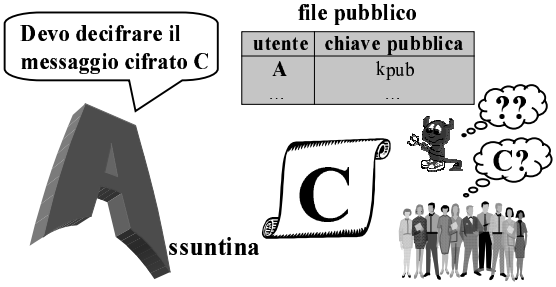


file pubblico

utente	chiave pubblica
A	kpub
…	…



Decifratura



file pubblico

utente	chiave pubblica
A	kpub
…	…

Decifratura

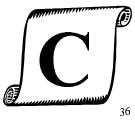
chiave privata
kpriv

file pubblico

utente	chiave pubblica
A	kpub
…	…

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

ssuntina

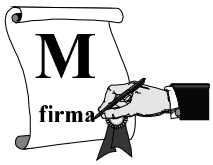


Principio di Kerckhoffs

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

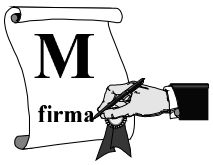
Jean Guillaume Hubert Victor Francois Alexandre Auguste Kerckhoffs von Nieuwenhof (1835-1903), filologo olandese, *"La Criptographie Militarie"* [1883]

Firma Digitale



Equivalente alla firma convenzionale

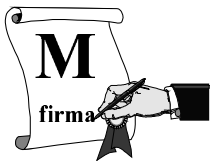
Firma Digitale



Equivalente alla firma convenzionale

Soluzione naive:
incollare firma digitalizzata

Firma Digitale



Equivalente alla firma convenzionale

Soluzione naive:
incollare firma digitalizzata

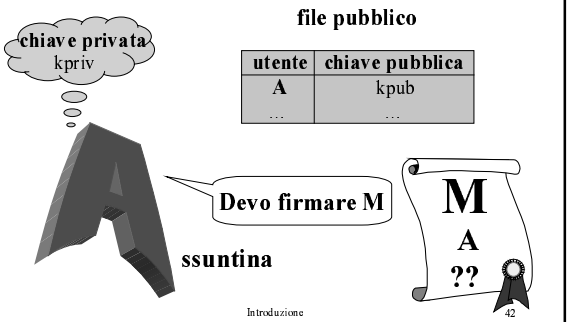
Desiderata per la Firma Digitale

La firma digitale deve poter essere facilmente prodotta dal legittimo firmatario

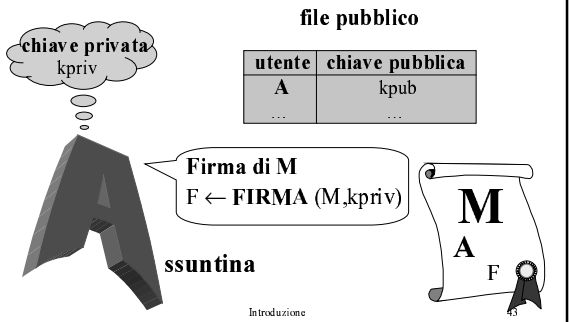
Nessun utente deve poter riprodurre la firma di altri

Chiunque può facilmente verificare una firma

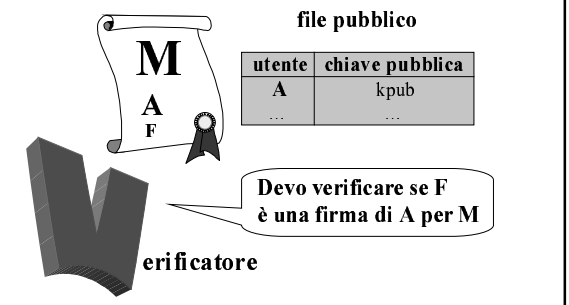
Firma digitale



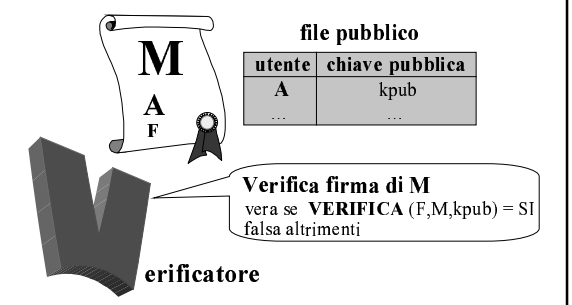
Firma digitale



Verifica firma digitale



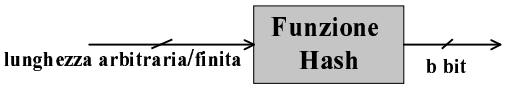
Verifica firma digitale



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′)

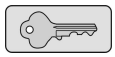
h(M) è l'impronta digitale del file

Assicura se un file è stato modificato!

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 1000 MHz $\approx 3,15 \cdot 10^{18} \approx 1,37 \cdot 2^{61}$
- Cicli in un secolo di 1.000.000 macchine a 1000 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

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 120 bit

Quanto è "sicura" una chiave di 120 bit?

Chiave di 120 bit

Supponiamo di avere 1.000.000.000 macchine a 1.000 MHz ed ognuna prova una singola chiave in un ciclo

Provare tutte le possibili chiavi ≈ 421.034.025 secoli

Provare 1/622.614.630 delle possibili chiavi ≈ 67.6 anni

Numero colonne per l'Enalotto = 622.614.630