Sicurezza

a.a. 2013/14

Alfredo De Santis

Dipartimento di Informatica ed Applicazioni
Università di Salerno

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

Marzo 2014

Informazioni sul Corso

- Durata: 12 settimane
  - 72 ore di lezioni frontali
  - 36 lezioni
- Orario lezioni:
  - Martedì 15:00 - 18:00, Aula F/4
  - Giovedì 16:00 - 18:00, Lab Sistemi
  - Venerdì 9:00 - 11:00, Aula F/4
- Home-page del corso:
  - http://www.dia.unisa.it/professori/ads/ads/Sicurezza.html

Variazioni da anni precedenti

- Fino all'anno 2010/11:
  Sicurezza su Reti II, 6 crediti e non 9
- Solo pochi studenti hanno sostenuto Sicurezza su Reti alla triennale
- Rivedremo i punti principali di Crittografia e Sicurezza su Reti

Organizzazione

- Bibliografia
  - Libri
  - Materiale/Appunti dalle lezioni
  - http://www.dia.unisa.it/professori/ads/ads/Sicurezza.html
- Laboratorio
- Progetti e presentazioni di argomenti specifici

06/03/14

http://www.di.unisa.it/~ads/corso-security/www/CORSO-9900

Sicurezza su Reti

Docente prof. Alfredo De Santis, *ads@dia.unisa.it*

Anno Accademico 1999/2000

Benvenuti alla pagina principale del corso di Sicurezza su Reti.

Tesine (molte sono ancora bozze!)

- Crittografia Classica (versione 7/3/2001)
- Crittoanalisi (Vigenere) (versione finale 27/7/2000)
- Data Encryption Standard (DES) (versione finale 27/7/2000)
- Advanced Encryption Standard (AES) (versione finale 21/7/2000)
- Crittografia a chiave pubblica (versione finale 31/7/2000)
- Firme Digitali (versione 31/7/2000)
- Funzioni Hash (versione finale 13/10/2000)
- Autenticazione e Password (versione 27/10/2000)
- Sistemi Biometrici (versione finale 21/3/2001)
- Schemi di Identificazione (versione finale 1/8/2000)
- Randomness (versione finale 17/10/2000)
- Key Escrow (versione finale 30/10/2000)
- Schemi a Condivisione di Segreto (versione 31/7/2000)
- Crittografia Visuale (versione finale 2/8/2000)
- PKI (versione 7/9/2000)
- Sistema di telefonia GSM (versione finale 21/7/2000)
- UMTS (versione finale 3/9/2001)
- Windows NT (versione finale 27/7/2000)
- Hacking Windows NT (versione finale 25/10/2000)
- Sicurezza Unix (versione finale 27/10/2000)
- TCP/IP (versione finale 4/8/2000)
- HTTP (versione 5/9/2000)
- SSL (versione finale 12/9/2000)
- Firewall (versione 11/12/2000)
- WAP (versione finale 10/10/2000)
- PGP (versione finale 24/7/2000)
- SET (versione finale 4/8/2000)
- Commercio Elettronico (versione finale 3/8/2000)
- IPv6 (versione finale 14/9/2000)
- Anonimia (versione 4/8/2000)
- Network Sniffer (versione 2/8/2000)
- Network Scanner (versione 31/7/2000)
- Common Gateway Interface and Web Security (versione 26/7/2000)
- Script Ostili (versione finale 25/7/2000)
- Sicurezza in Java (versione finale 12/10/2000)
- Sicurezza e ASP (Active Server Pages) (versione 5/3/2001)
- Sicurezza nei Data Base (Oracle) (versione finale 18/10/2000)
- Computer Virus (versione finale 5/10/2000)
- Watermark (versione finale 28/9/2000)
- Monitoraggio attivo utenti (versione finale 3/8/2000)
- Distributed Denial of service (versione 3/8/2000)
- CryptoAPI (versione 1/8/2001)
- Smart Card (versione 5/12/2001)
- PGP con Windows (versione 28/10/2003)
- Modello tesine (exe, zip)

Presentazioni

- Introduzione (html, ps, pdf)
- Crittografia Classica (html, ps, pdf)
- Crittoanalisi (html, ps, pdf)
- DES (html, ps, pdf)
- AES (html, ps, pdf)
- Stream Cipher (html, ps, pdf)
- Crittografia a Chiave Pubblica (html, ps, pdf)
- Firme Digitali (html, pdf, ps)
- Diffie Hellman (html, ps, pdf)
- Funzioni Hash (html, pdf, ps)
- Randomness (html, ps, pdf)
- Digital Timestamping (html, ps, pdf)
- Digital Watermark (html, ps, pdf)
- Tecniche biometriche di identificazione (html, ps, pdf)
- Protocolli (html, ps, pdf)
- Mental Poker (html, ps, pdf)
- Crittografia Visuale (html, ps, pdf)
- PGP (html, pdf, ps)
- Windows NT: architettura del sistema (html, pdf, ps)
- Windows NT: sicurezza in locale (html, pdf, ps)
- Windows NT: organizzazione di rete (html, pdf, ps)
- Windows NT: password (html, pdf, ps)
- Hacking Windows NT (html, pdf, ps)
- File System cifrati (html, pdf, ps)
- Java security (html, pdf, ps)
- Web & CGI Security (html, pdf, ps)
- Network Sniffer (html, ps, pdf)
- Distributed Denial of Service (html, ps, pdf)
- Monitoraggio attivo utenti (html, ps, pdf)
- Network scanner (html, pdf, ps)
- Progetti del corso, Progetti assegnati e gruppi

Anno Accademico 1998/1999

http://www.di.unisa.it/~ads/corso-security/www/CORSO-0001

Sicurezza su Reti

Docente prof. Alfredo De Santis, *ads@dia.unisa.it*

Anno Accademico 2000/2001

Benvenuti alla pagina principale del corso di Sicurezza su Reti.

Presentazioni

- Introduzione (html, pdf)
- Crittografia Classica (html, pdf)
- Crittoanalisi (html, pdf)
- DES (html, pdf)
- RC2, RC5 (html, pdf)
- AES (html, pdf)
- Crittografia a Chiave Pubblica (html, pdf)
- Accordo su chiavi (html, pdf)
- Firma digitale (html, pdf)
- Funzioni Hash (html, pdf)
- Message Authentication Codes (MAC) (html, pdf)
- Autenticazione (html, pdf)
- Crack (html, pdf)
- PKI (html, pdf)
- Pluggable Authentication Modules (PAM) (html, pdf)
- Protocolli Crittografici (html, pdf)
- Pretty Good Privacy (PGP) (html, pdf)
- SSH (html, pdf)
- SSL ed OpenSSL (html, pdf)
- Protezione posta sotto Linux (html, pdf)
- Randomness (html, pdf)
- Kerberos (html, pdf)
- Firewall 1 (html, pdf)
- Intrusion Detection (html, pdf)
- Snort (html, pdf)
- StackGuard (html, pdf)
- Tools Steganografici (html, pdf)
- Packet Sniffing (html, pdf)
- Packet Sniffer con libreria PCAP (html, pdf)
- Packet Sniffing: la libreria Winpcap (html, pdf)
- Port Scanning (html, pdf)
- Retina (html, pdf)
- StegFS (html, pdf)
- How Assess, Evaluate, Optimize a .COM Security Infrastructure (pdf)

Tesine

- Message Authentication Codes (MAC) (versione finale 14/12/01)
- Cifrari a blocchi: AES, RC2, RC5 (versione finale 20/12/01)
- Crittosistemi basati su Curve Ellittiche (versione finale 20/12/01)
- Steganografia (versione finale 9/7/01)
- PGP con Windows (versione 5/12/01)
- SSH (versione finale 2/8/01)
- OpenSSL (versione finale 20/7/01)
- Protezione posta sotto Linux (versione finale 14/11/01)
- Packet Sniffer (versione 31/7/01)
- Packet Sniffer con libreria PCAP (versione finale 10/7/01)
- Packet Sniffing: la libreria Winpcap (versione 26/7/01)
- SNORT (versione finale 26/7/01)
- Port Scanning (versione 26/7/01)
- Retina (versione finale 4/12/01)
- Rilevazione dello Scanning (versione finale 18/10/01)
- StackGuard (versione finale 24/7/01)
- Crack (versione 5/7/01)
- Kerberos V5 (versione finale 11/9/01)
- Sicurezza in Windows 2000 (versione finale 19/10/01)
- StegFS (versione finale 22/3/02)
- Firewall 1 (versione finale 4/12/01)
- PAM (versione finale 8/4/02)

Anno Accademico 1999/2000

Anno Accademico 1998/1999

Progetti di Digital Forensics

- Windows Forensics (Valerio Cinque, Francesco Testorio, Andrea Di Maio)
- Falso alibi digitale su Windows 7 (Alessandro Bove, Alfonso Martorelli, Giuseppe Valentino, Luigi Di Biasi)
- Distribuzioni Linux per analisi forense (Helix 3, DEFT Linux 6, CAINE, Backtrack)
  - Live forensic (Mario Fiore Vitale, Fabio Fulgido, Gaetano Rocco)
  - Post-mortem forensic (Umberto Annunziata, Claudio Gargiulo)
- Linux Forensics (Domenico Viscito, Fabio Favale)
- Falso alibi digitale su Linux (Antonio Sanfelice, Sara Cantalupo, Demia Massaro, Giovanni Costa)
- iPod ed iPhone Forensics (Giovanni Mastroianni, Luisa Siniscalchi, Domenico Voto)
- Android Forensics (Davide Barbuto, Francesco Capano, Gaetano Contaldi, Andrea Vallati)
- Image Forensics (Giuseppe Lanzilli, Hamza Hamim, Gianluca Roscigno)
- GPS Navigation Devices Forensics (Ermanno Travaglino, Armando Faggiano)
- Investigazione di un Computer (Alessio Marzaioli, Francesco Pisano)
- Network Investigations (Dario Casciello, Domenico Memoli, Antonio Della Sala)

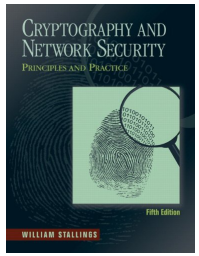
http://www.dia.unisa.it/professori/ads/ads/Sicurezza.html

Interazione

Domande

Interesse

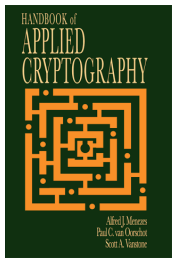
Testi di riferimento



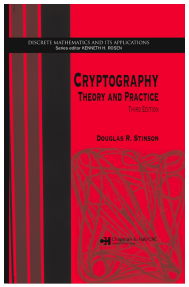
Cryptography and Network Security: Principles and Practices
Prentice-Hall (5/Ed)
by William Stallings, 2010

Crittografia e Sicurezza delle Reti
McGraw-Hill (2/Ed)
by William Stallings, 2007

Altri testi utili



Handbook of Applied Cryptography
by Alfred J. Menezes, Scott A. Vanstone, 1996



Cryptography: Theory and Practice (3rd Ed.)
by Douglas Stinson, 2006

Laboratorio

Una simulazione della rete Internet
Collaborazione dott. Luigi Catuogno

- a.a. 2004/05
- a.a. 2005/06
- a.a. 2006/07
- a.a. 2007/08

http://sicurezza2.dia.unisa.it/

06/03/14

Esami

- Esame classico
- Laboratorio
- Progetti e presentazioni

06/03/14

Esami

- L'esame prevede una prova scritta e una prova orale
- Sono previsti sette appelli suddivisi come segue:
  - 17 giugno 2014, ore 10:00, aula F/1
  - 8 luglio 2014, ore 10:00, aula F/1
  - 25 luglio 2014, ore 10:00, aula F/1
  - 2 settembre 2014, ore 10:00, aula P/6
  - Un appello straordinario (riservato a studenti con non più di 4 esami alla Laurea), a Novembre 2014;
  - Due appelli nel periodo Gennaio 2015 – Febbraio 2015.

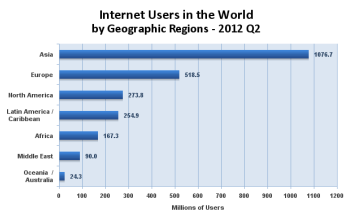
Niente prove intercorso

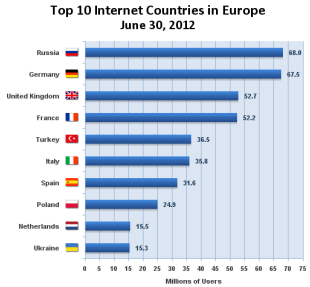
06/03/14

Ed ora … qualcosa sui contenuti

06/03/14

Utenti Internet nel mondo





Internet Usage and World Population Statistics are for June 30, 2012:
Population 7.017.846.922
34,3% of population 2.405.518.376

06/03/14

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

06/03/14

CERT
Computer Emergency Response Team

Team di esperti nell'ambito della sicurezza

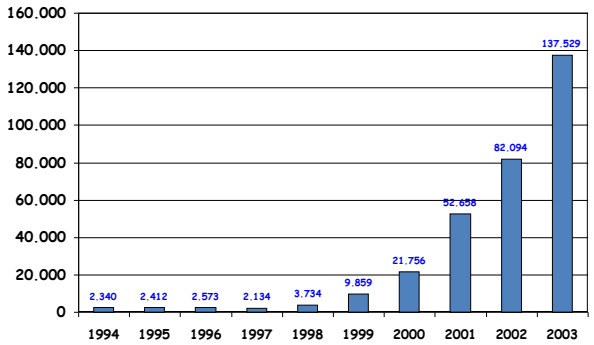
- Creato dal DARPA (Defense Advanced Research Projects Agency) in seguito all'attacco del worm

Si occupa di

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

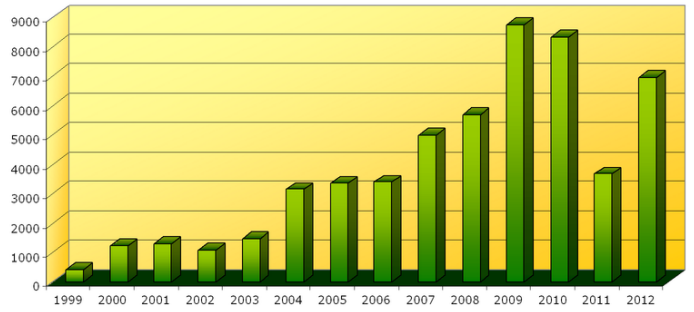
06/03/14

Incidenti riportati al CERT

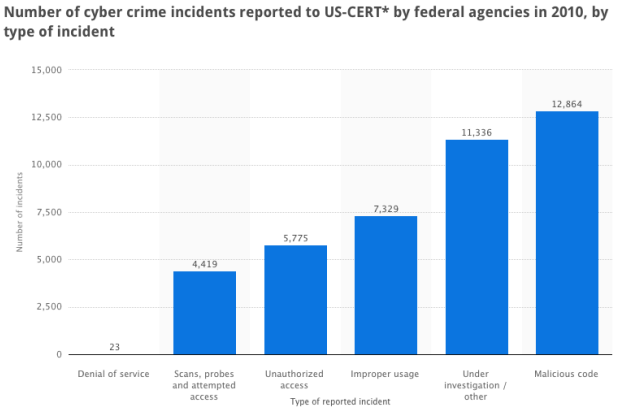


06/03/14

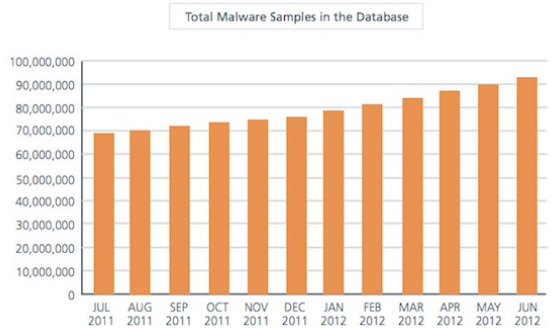
Incidenti riportati al GARR- CERT



06/03/14



Malware Rilevati da McAfee



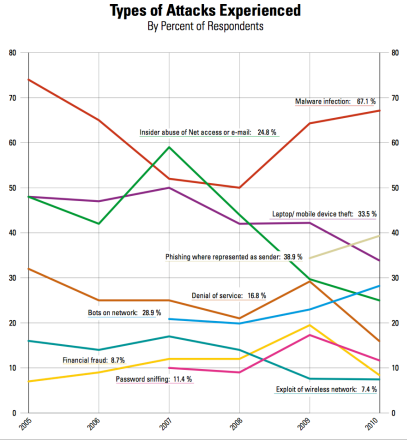
Conteggio totale di malware nel database di McAfee Labs

06/03/14

Indagine CSI

Eseguita tra Luglio 2008 e Giugno 2009, su 443 intervistati negli Stati Uniti (aziende, agenzie governative, università, ospedali, etc…)

Indagine CSI



Types of Attacks Experienced
By Percent of Respondents

Type of Attack	2005	2006	2007	2008	2009	2010
Malware infection	74%	65%	52%	50%	64%	67%
Bots / zombies within the organization	added in 2007		21%	20%	23%	29%
Being fraudulently represented as sender of phishing messages	added in 2007		26%	31%	34%	39%
Password sniffing	added in 2007		10%	9%	17%	12%
Financial fraud	7%	9%	12%	12%	20%	9%
Denial of service	32%	25%	25%	21%	29%	17%
Extortion or blackmail associated with threat of attack or release of stolen data	option added in 2009				3%	1%
Web site defacement	5%	6%	10%	6%	14%	7%
Other exploit of public-facing Web site	option altered in 2009				6%	7%
Exploit of wireless network	16%	14%	17%	14%	8%	7%
Exploit of DNS server	added in 2007		6%	8%	7%	2%
Exploit of client Web browser	option added in 2009				11%	10%
Exploit of user's social network profile	option added in 2009				7%	5%
Instant messaging abuse	added in 2007		25%	21%	8%	5%
Insider abuse of Internet access or e-mail (i.e. pornography, pirated software, etc.)	48%	42%	59%	44%	30%	25%
Unauthorized access or privilege escalation by insider	option altered in 2009				15%	13%
System penetration by outsider	option altered in 2009				14%	11%
Laptop or mobile hardware theft or loss	48%	47%	50%	42%	42%	34%
Theft of or unauthorized access to PII or PHI due to mobile device theft/loss	option added in 2008			8%	6%	5%
Theft of or unauthorized access to intellectual property due to mobile device theft/loss	option added in 2008			4%	6%	5%
Theft of or unauthorized access to PII or PHI due to all other causes	option added in 2008			8%	10%	11%
Theft of or unauthorized access to intellectual property due to all other causes	option added in 2008			5%	8%	5%

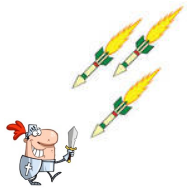
2010 CSI Computer Crime and Security Survey — 2010: 149 Respondents

Indagine CSI

Danno economico in media per intervistato

Difese statiche e dinamiche

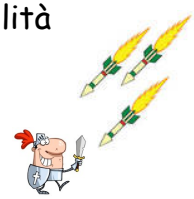
- Difesa statica prima o poi cede dopo nuovi attacchi



Difese statiche e dinamiche

- Difesa statica prima o poi cede dopo nuovi attacchi
- Difesa deve adattarsi dinamicamente ai nuovi attacchi per avere maggiori possibilità





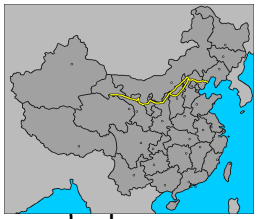
Linea Maginot

- Costruita 1930-37
- Ministro della guerra André Maginot
- 400 km, frontiera franco-tedesca
- Francia invasa nel 1940
  Tedeschi passarono attraverso il Belgio
- Idea difensiva vecchia (guerra 1914-18)
  Non considerata l'estrema mobilità dei reparti meccanizzati

Weakest link principle

06/03/14

Muraglia cinese



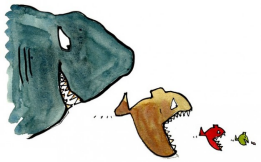
- III secolo A.C.
- 8.851 km, spessore 9,5 m, altezza 4,5 – 12 m
- Difesa da Mongoli
- *Insider attack nel* 1644: dopo che la sua concubina Chen Yuanyuan era stata presa dall'imperatore Li Zicheng, il generale Wu Sangui apri le porte a Shenhaiguan e fece entrare i ribelli della Manciuria

Missili Scud

- Usati da Iraq, Gulf war (1990-91)
- Veicolo TEL (trasportatore-elevatore-lanciatore),
  - Autonomia carburante per distanza di 250 km (500 km andata e ritorno)
  - Velocità max 60 km/h
- Precisione scarsa: CEP 1100m a 440 km
- Molto mobile e difficile da individuare

Prede e predatori

- Teoria dell'evoluzione
- Evoluzione dei predatori
  Canini ed artigli più grandi ed affilati,
  … ed evoluzione prede
  corazze più resistenti e zampe più veloci




Antilocapra americana

- Habitat: prateria
- Predatori: lupo, coyote, lince rossa
- Animale terrestre più veloce dopo il ghepardo
  - Raggiunge i 100 km/h (superato solo su brevi distanze)
- Rileva movimenti ad una distanza di 4-5 km

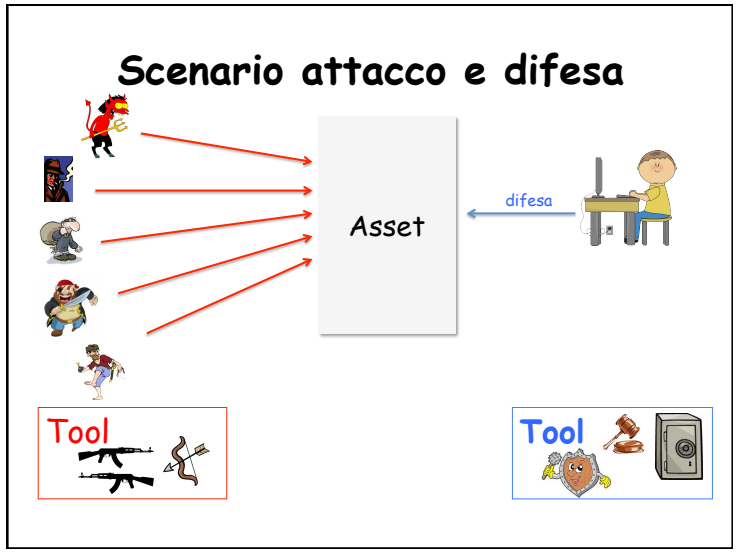
Drosofilia (moscerino della frutta)

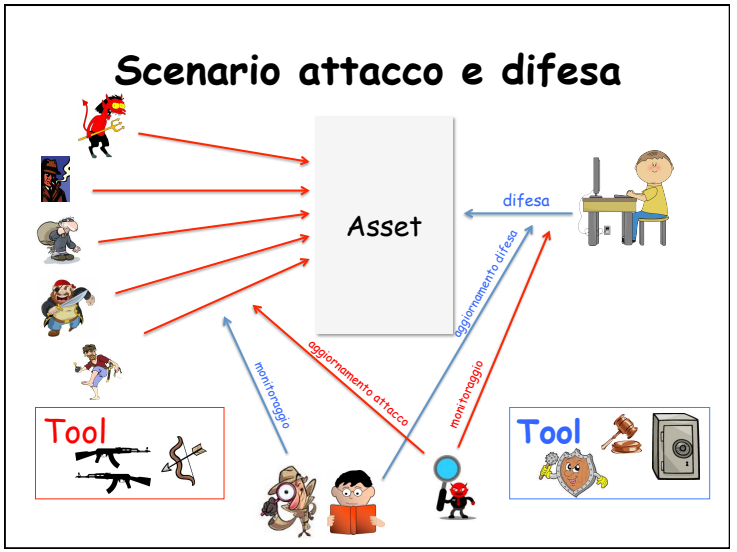
- Le ali di una mosca possono battere fino a 250 volte al secondo.
- Volo con tratti lineari, con rapidi cambi di direzione
  - Può ruotare di 90 gradi in meno di 50 millisecondi
- Presenta nervi ottici collegati direttamente ai muscoli delle ali (mentre in altri insetti c'è in ogni caso un passaggio attraverso il cervello), rendendo bassissimo il tempo di reazione


Mondo digitale

esempio

- Virus Polymorphic si modificano continuamente per evitare di essere rilevati.
- Autori dei virus modificano algoritmi di mutazione dopo aver appreso le nuove tecniche di rilevazione.
- Bisogna essere costantemente aggiornati e rispondere subito alle novità!





Vulnerabilità e Attacchi

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

Attacco
- Sfruttamento di una vulnerabilità di un sistema

06/03/14

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:
- Riproduzione
- Modifica dei messaggi
- Denial of service

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

06/03/14

Sicurezza Dati: obiettivi

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

06/03/14

Confidenzialità

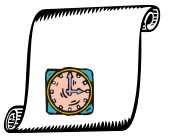
Privacy, Segretezza

Informazioni { trasmesse / memorizzate

sono accessibili in lettura
solo da chi è autorizzato

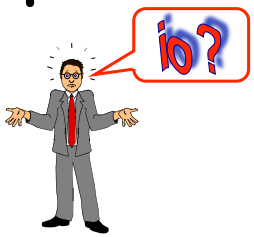
06/03/14

Autenticazione

messaggi	entità (Identificazione)	tempo (Timestamp)
		

06/03/14

Non-ripudio



Chi invia
Chi riceve

non può negare la trasmissione del messaggio

06/03/14

Controllo Accessi

Accesso alle informazioni controllato da o per il sistema

06/03/14

Integrità

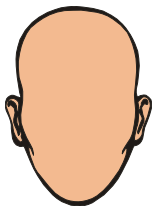
Solo chi è autorizzato può modificare l'attività di un sistema o le informazioni trasmesse

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

06/03/14

Anonimia

Protezione dell'identità o del servizio utilizzato



06/03/14

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

06/03/14

Contenuto Corso

- Prima parte: Crittografia
  - Cifrari simmetrici
  - Cifrari asimmetrici
  - Firme digitali
  - Funzioni hash e integrità dei dati
- Seconda parte: Sicurezza su Reti
  - PKI
  - Autenticazione utenti
  - Posta elettronica sicura
  - Sicurezza IP e WWW
  - Sicurezza sistemi
    - Intrusioni, software malizioso, firewall

06/03/14

Contenuto Corso

- Terza parte:
  - Crittografia (Curve ellittiche, …)
  - Serrature
  - Steganografia
  - Watermark
  - Wireless Security
  - Bluetooth
  - Digital Right Managment (DRM)

Digital Video Broadcasting (DVB), Pay Tv
- Radio-Frequency Identification (RFId)
  - Anonimia
  - Sicurezza del Software
  - Buffer Overflow
  - Psicologia della Sicurezza
  - Economia della Sicurezza
  - Elezioni Elettroniche
  - Micropagamenti
  - Malware
  - SPAM
  - Analisi del Rischio
  - Digital Forensic
  - Bitcoin
  - Cloud Storage
  - …

06/03/14

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

06/03/14

Alcuni metodi antichi di cifratura

Erodoto

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

Polibio

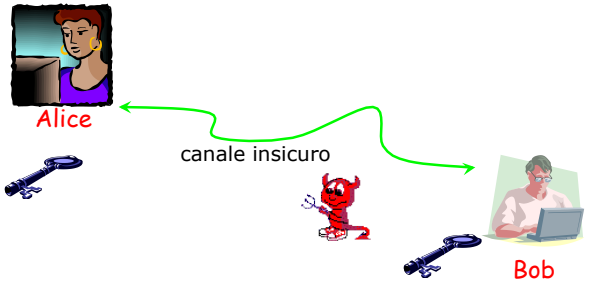
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	IJ	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

testo in chiaro: C A S A

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

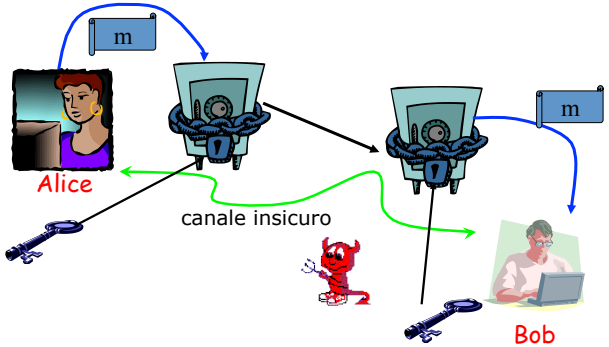
06/03/14

Cifrari simmetrici



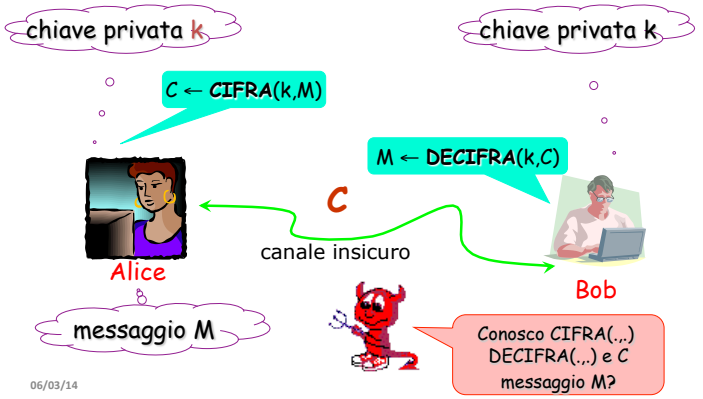
06/03/14

Cifrari simmetrici



06/03/14

Cifrari simmetrici



06/03/14

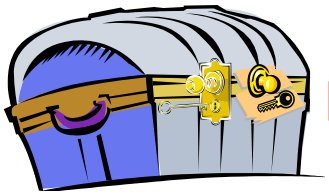
Cifrari simmetrici che vedremo

- Cifrari a blocco:
  - DES
  - Blowfish
  - RC5
  - RC6
  - AES
- Stream Cipher:
  - Cifrario autokey
  - LSFR (Linear Feedback Shift Register)
  - RC4

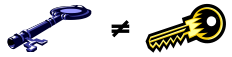
06/03/14

Cifrari asimmetrici

- Usano una cassaforte con due lucchetti
  - Con una chiave (pubblica) chiudiamo la cassaforte
  - Con l' altra chiave (privata) apriamo la cassaforte

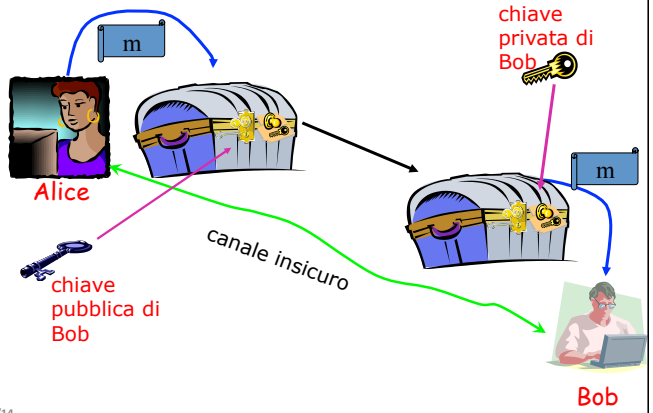


Public key ≠ Private key



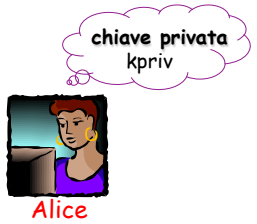
06/03/14

Cifrari asimmetrici



06/03/14

Cifrari asimmetrici

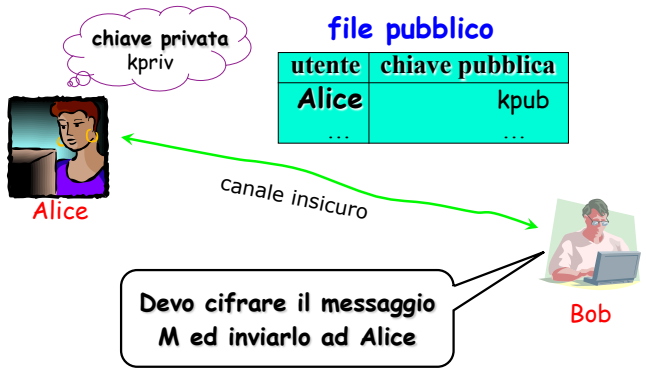


file pubblico

utente	chiave pubblica
Alice	kpub
…	…

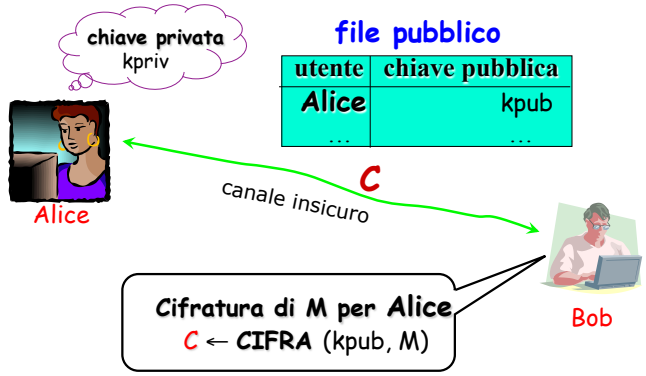
06/03/14

Cifratura



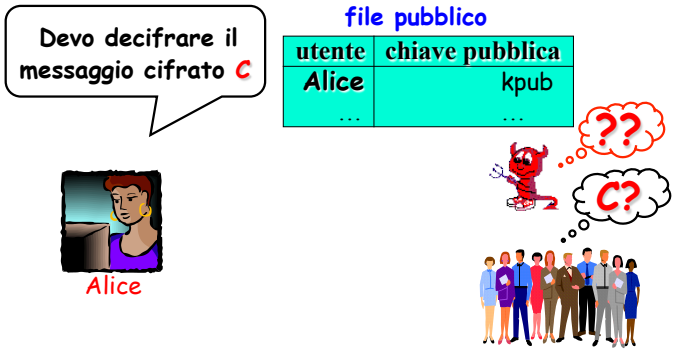
06/03/14

Cifratura



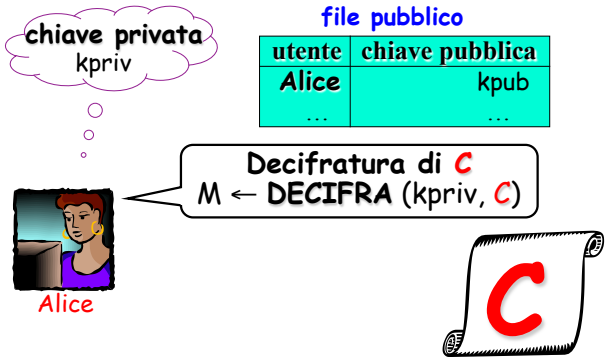
06/03/14

Decifratura



06/03/14

Decifratura



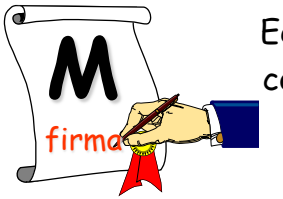
06/03/14

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 utenti genera da solo la propria coppia di chiavi e rende pubblica la chiave pubblica
- Ogni utente memorizza una sola chiave (privata)

06/03/14

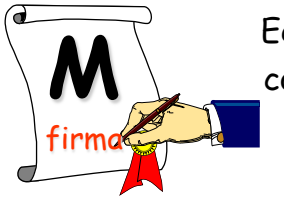
Firma Digitale



Equivalente alla firma convenzionale

06/03/14

Firma Digitale



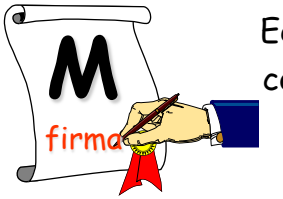
Equivalente alla firma convenzionale

Soluzione naive:

incollare firma digitalizzata

06/03/14

Firma Digitale



Equivalente alla firma convenzionale

Soluzione naive:

incollare firma digitalizzata

06/03/14

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

06/03/14

Firma digitale

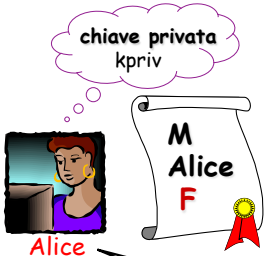
file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Devo firmare M

06/03/14

Firma digitale



file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Firma di M
F ← FIRMA (M,kpriv)

06/03/14

Firma digitale

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

(M,F)

canale insicuro

Bob

06/03/14

Verifica firma digitale

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

Devo verificare se F è una firma di Alice per M

Bob

06/03/14

Verifica firma digitale

file pubblico

utente	chiave pubblica
Alice	kpub
…	…

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

Bob

06/03/14

Public Key Infrastructure

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

06/03/14

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

06/03/14

Public Key Infrastructure

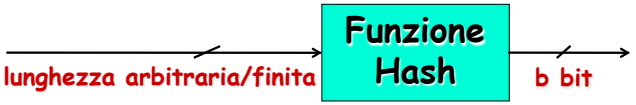
Insieme di hardware, software, procedure, politiche, per

- Creare
- Gestire
- Memorizzare
- Distribuire
- Revocare

certificati digitali

06/03/14

Funzioni Hash



Idea alla base:

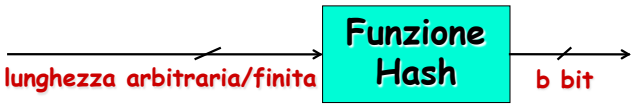
il valore hash h(M) è una rappresentazione non ambigua e non falsificabile del messaggio M

Proprietà:

- facile da computare
- difficile trovare una collisione

06/03/14

Funzioni Hash



- Le più comuni:
  - MD5 (Message Digest Algorithm), valore di 128 bit
  - SHA-0, SHA-1 con 160 bit, SHA-2, cioè SHA-224, SHA-256, SHA-384 e SHA-512, (Secure Hash Algorithm)
- Esempi:
  - SHA1("Cantami o diva del pelide Achille l'ira funesta") = 1f8a690b7366a2323e2d5b045120da7e93896f47
  - SHA1("Contami o diva del pelide Achille l'ira funesta") = e5f08d98bf18385e2f26b904cad23c734d530ffb

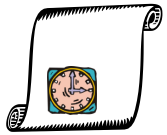
06/03/14

Uso delle funzioni hash

Firme digitali

Integrita' dei dati

Certificazione del tempo



06/03/14

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

06/03/14

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´)

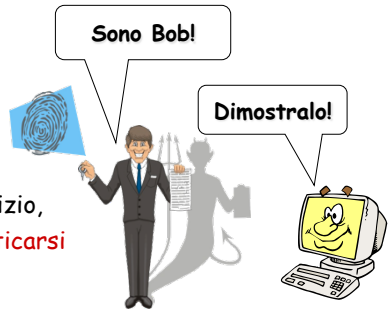
h(M) è l'impronta digitale del file

Assicura se un file è stato modificato!

06/03/14

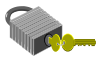
Autenticazione utente

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

06/03/14

Protocolli Crittografici

- Poker Mentale
- Condivisione di segreti
- Lancio di una moneta
- Blind Signature
- Moneta Elettronica
- Elezioni
- Certified email
- Crittografia Visuale

06/03/14

Sicurezza e-mail

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

Possibili soluzioni:

- PGP
- S/MIME


06/03/14

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

Codice "malizioso"

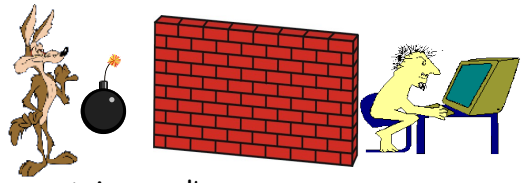
Virus 

Cavalli di Troia 

Macrovirus 

Firewall

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

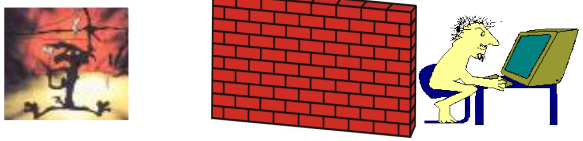


"Modo per restringere l'accesso tra Internet e la rete interna"

06/03/14

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"

06/03/14

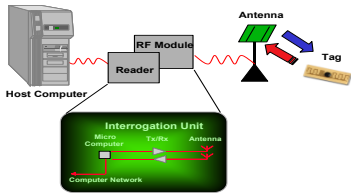
Protezione del software dalla copia

- Trovare un metodo contro la pirateria
  - efficiente
  - economico
  - resistente contro i pirati esperti
  - non invasivo
- Compito impossibile!
- Però si può rendere la copia difficile per il pirata esperto ed impossibile per il pirata occasionale

06/03/14

RFId

- Acronimo di **Radio Frequency IDentification**
- E' una tecnologia per la identificazione automatica di oggetti, animali o persone
- Il sistema si basa sul leggere a distanza informazioni contenute in un tag RFID usando dei lettori RFID



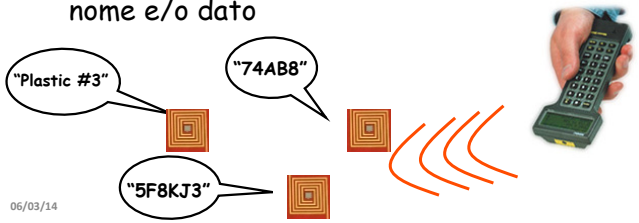
Componenti:
- RFId tag
- Reader o transceiver
- Sistema di elaborazione dati (PC) middleware server

06/03/14

Il tag

Caratteristiche dei tag più semplici:

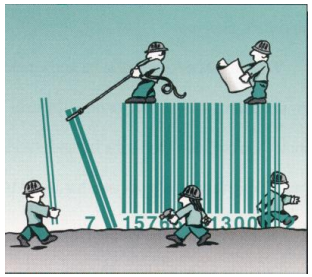
- Dispositivo passivo
  riceve energia dal lettore
- Ha un range di diversi metri
- E' un "etichetta intelligente" che grida il suo nome e/o dato



06/03/14

Codici a barre

RFId può sostituire il codice a barra

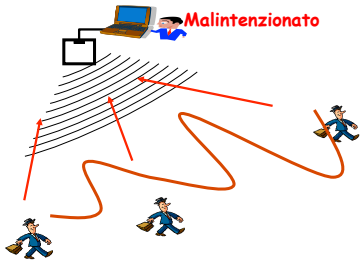


06/03/14

Problemi di privacy

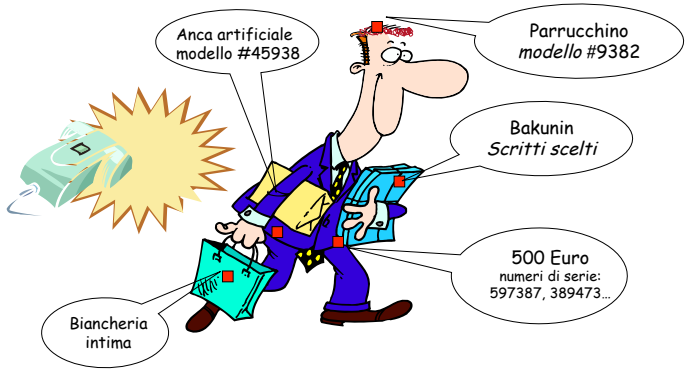
Furto di dati personali

Tracciamento



06/03/14

Problemi di privacy



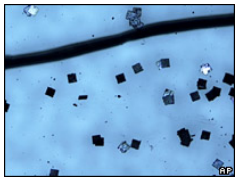
06/03/14

Due esigenze contrastanti

Tutelare la *privacy*
Identificare i beni non acquistati

06/03/14

Tag piccolissimi

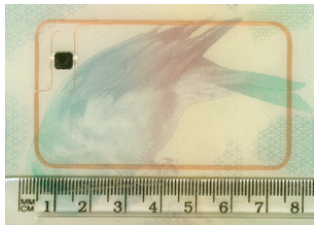


- Hitachi, 2007
- Grandezza: 0,05 mm x 0,05 mm
- Unico problema … attualmente l'antenna è 80 volte più grande!

06/03/14

Passaporti con RFId

Tag RFID utilizzati nei passaporti
- 2005 Norvegia
- 2006 Giappone, Spagna, Italia, UK, USA
- 2007 Australia
- …



Tag RFID inserito in un passaporto

06/03/14

Passaporti con RFId


la Repubblica.it Tecnologia&Scienze

SCIENZA & TECNOLOGIA

Passaporto elettronico a rischio clonazione I dati scaricabili dal microchip

- Potevano essere letti da 10m
- In seguito, i passaporti contengono anche una sottile membrana metallica al fine di rendere difficile le letture non autorizzate (skimming) quando il passaporto è chiuso

06/03/14

Passaporti con RFId

- In Italia dal 2010
- impronte vengono memorizzate solo nel chip del passaporto
- non esiste in Italia una banca dati delle impronte digitali (AFIS, Automated fingerprints identification system) civile
- non per i minori di anni 12

06/03/14

Steganografia

Nasconde l'esistenza di un messaggio

Esempio: immagini Bitmap

Red Green Blue

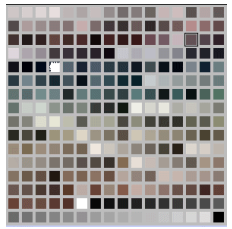
(11100001, 00000100, 00010111)

- Livello colore primario: 0,…,255
- Uso dei bit meno significativi

06/03/14

Steganografia

immagini GIF



palette

06/03/14

Watermark

- Letteralmente "filigrana"
- Assicura autenticità ed integrità ai documenti in cui è immerso
- E' una sequenza di bit inseriti all'interno del documento da proteggere con le caratteristiche:
  - **Impercettibile** - Il documento marcato e quello originale devono apparire identici.
  - **Legata al documento** - La marca deve essere funzione del documento e parte integrante di esso.
  - **Robusta** - La marca deve essere in grado di resistere a tutte le più comuni trasformazioni operabili sul documento.

06/03/14

Digital Right Managment

- FairPlay
  Usato da iPod e iTunes
- Content Scrambling System (CSS)
  - Sviluppato nel 1996 da Matsushita e Toshiba, per DVD
  - Rotto da un ragazzo scandinavo, Jon Lech Johansen, che rilasciò il deCSS, un DVD decoder per PC nel 1999
- Advanced Access Content System (AACS)
  - sviluppatori: Disney, Intel, Microsoft, Matsushita (Panasonic), Warner Brothers, IBM, Toshiba e Sony .
  - specifiche rilasciate nell'aprile 2005
  - per HD-DVD e Blu-ray
  - prima notizia di un craccaggio pubblicata il 18 dicembre 2006 da parte dell'hacker **muslix64**
- SONY

06/03/14

DRM Sony

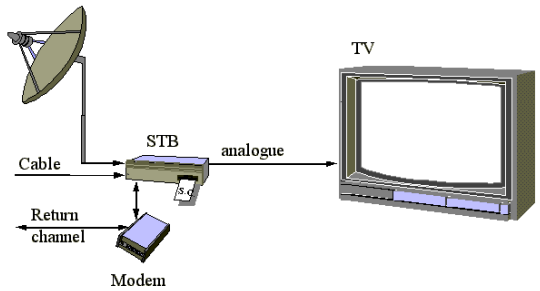
- I cd audio distribuiti devono gestire la musica in formato *Compact Disc Digital Audio (CDDA)*
- Come impedire ai programmi di leggere un tale formato audio?
  Meccanismi di protezione attiva e passiva

  installano software all'insaputa dell'utente

  modificano il layout dei dati sul disco
- Ottobre 2005: Russinovich scopre la tecnologia DRM eXtended Copy Protection sui cd audio Sony BMG
- I cd audio Sony BMG detengono un applicativo che si installa come servizio di Windows e monitorizza le attività del PC .. scatenando un malcontento tra gli utenti

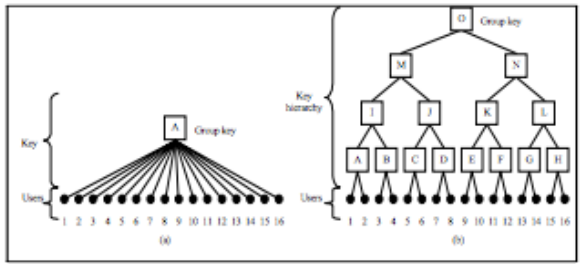
06/03/14

Pay TV



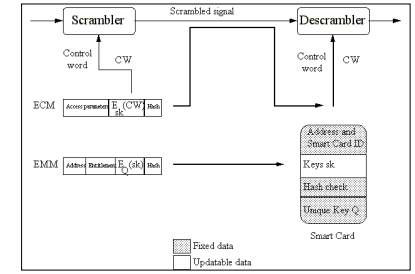
06/03/14

Gerarchia di chiavi



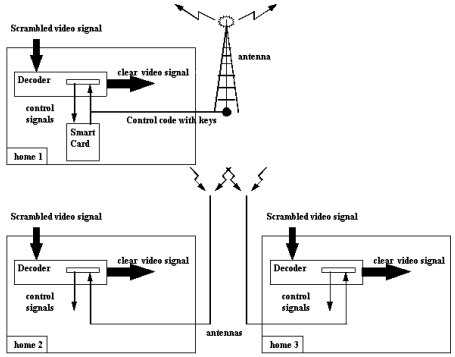
06/03/14

Pay TV



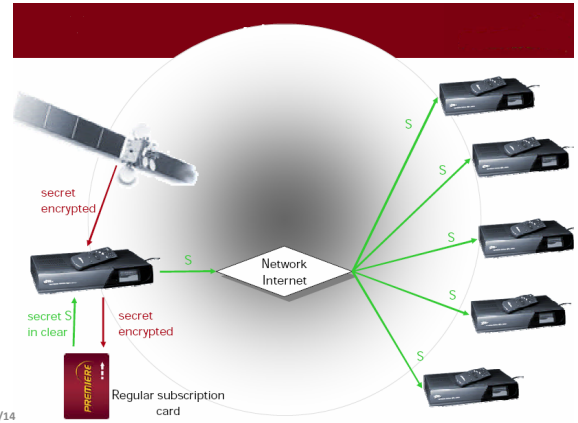
06/03/14

Videocrypt: McCormac Hack



06/03/14

Card Sharing



06/03/14

Card Sharing

la Repubblica ROMA.it

Violavano i codici Mediaset e Sky
Trentanove persone indagate

Guardia di Finanza

Smantellata una rete pirata per la diffusione di programmi audiovisivi

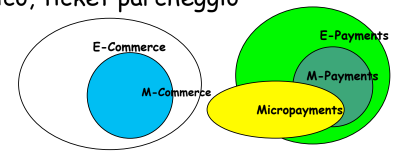
Comando Provinciale Lecce - 1 dicembre 2011 - ore 11:22

06/03/14

Micropagamenti

Pagamenti di piccolo importo (max € 5)

- Acquisti "pay-per-click" sul Web
  - Musica, filmati, giochi, informazioni
- Acquisto di servizi mediante dispositivi mobili
  - Informazioni sul traffico, biglietti per il trasporto pubblico, ticket parcheggio



Indagine Ipsos-Insight

Nel 2004, negli USA

Più di 14 milioni di utenti ha effettuato acquisti via Web per meno di 2 dollari

- 4 milioni nel 2003

Più di 37 milioni di utenti ha detto di essere disposto ad utilizzare carte di credito, di debito o ricaricabili per piccoli acquisti online

Indagine Juniper Research

In tutto il mondo

Il volume d'affari dei micropagamenti via cellulare varrà 40 miliardi di dollari entro il 2009

Gli utenti in Europa occidentale acquisteranno in media tramite cellulare 28 volte l'anno entro il 2009

Il valore medio di ogni transazione sarà di circa 3 dollari

Micropagamenti

- Necessario un sistema di pagamento sicuro ma anche rapido e semplice
- Idea:

  Utilizzo di una terza parte affidabile in grado di
  - Contabilizzare la spesa e addebitarla al Cliente
  - Far pervenire il pagamento al Mercante

06/03/14

Alcune proposte

- Acquisti tramite operatore telefonico
  - Addebitano i pagamenti sulla bolletta telefonica del Cliente
  - Utilizzano IVR per la gestione dell'interazione tra Cliente e Mercante (sito Web)
  - Esempio: Internet FastPay
- Acquisti via SMS
  - Addebitano i pagamenti sulla SIM o sulla carta di credito del Cliente
  - Esempio: TextPayMe

06/03/14

Sistemi di micropagamenti che vedremo

- PayWord
- MicroMint
- Millicent
- Lottery Tickets
- Peppercoin
- Pepercoin 2

06/03/14

Economia della Sicurezza

- Incentivi per la sicurezza
- Banche
  - Negli USA è la banca che deve provare che l'utente sbaglia/imbroglia
  - In Gran Bretagna, Norvegia e Paesi Bassi è l'utente che deve provare
- *Health records:* gli ospedali e non i pazienti acquistano sistemi IT, quindi proteggono gli interessi degli ospedali piuttosto che quello dei pazienti
- Perché il software della Microsoft è così insicuro nonostante il dominio sul mercato?

06/03/14

Curve Ellittiche

- La maggioranza della crittografia a chiave pubblica (RSA, DH) usa aritmetica sugli interi oppure sui polinomi con numeri/polinomi molto grandi
- "grandi" richieste per memorizzazione e processamento di chiavi e messaggi
- Alternative: usare curve ellittiche
- Offre lo stesso grado di sicurezza con minori lunghezze
- Sistemi più recenti, ma non analizzati come i precedenti

06/03/14

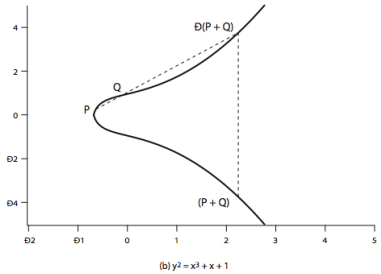
Curve Ellittiche Reali

- Una curva ellittica è definita da una equazione in 2 variabili
- Curva ellittica cubica della forma
  - $y^2 = x^3 + ax + b$
  - dove x, y, a, b sono numeri reali
  - Definisci anche il punto zero *O*
- Operazione di addizione
  - Somma geometrica dei punti Q+R è il punto riflesso dell'intersezione della curva con la retta QR

06/03/14

Esempio di una Curva Ellittica

Interpretazione geometrica di una addizione



(b) $y^2 = x^3 + x + 1$

06/03/14

Comparable Key Sizes for Equivalent Security

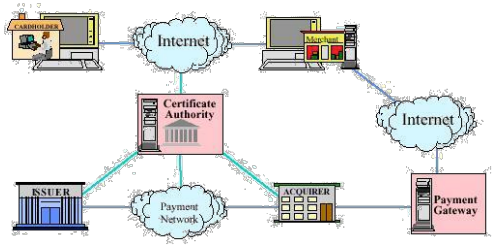
Cifrario simmetrico (grandezza chiave in bit)	Schema basato su ECC (grandezza di *n* in bit)	RSA/DSA (grandezza modulo in bit)
56	112	512
80	160	1.024
112	224	2.048
128	256	3.072
192	384	7.680
256	512	15.360

06/03/14

Secure Electronic Transaction SET

•Protocollo per transazioni sicure con carte di credito su reti aperte

•VISA e Mastercard, novembre 1995



Algoritmo LUHN-10

Card Type	Prefix	Length
MASTERCARD	51-55	16
VISA	4	13, 16
AMEX	34, 37	15
Diners Club/ Carte Blanche	300-305 36, 38	14
Discover	6011	16
JCB	3	16
JCB	2131, 1800	15

Specificato in ISO-7812-1, standard per il formato delle carte di credito

Ultima cifra per controllo dell'errore
4563 9601 2200 1999

Algoritmo LUHN-10

Position	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Number	4	3	2	1	2	3	4	2	7	5	6	7	8	1	9	0
Multiplier	2		2		2		2		2		2		2		2	
Total	8	3	4	1	4	3	8	2	14	5	12	7	16	1	18	0
Sum	8	3	4	1	4	3	8	2	5	5	3	7	7	1	9	0

Somma = 70 multiplo di 10

Domande?

06/03/14