
Parte VIII

Sicurezza e protezione

Sicurezza e Protezione

Sicurezza

Insieme di problemi relativi alle discipline di accesso e modifica delle informazioni gestite da un sistema di elaborazione

Protezione

Politiche e meccanismi predisposti nel sistema di elaborazione per impedire accessi non consentiti e garantire quelli consentiti

La protezione si basa su meccanismi implementati nel kernel, e gestiti dal file system

Problemi

- Perdita dei dati
 - Atti di Dio: terremoti, alluvioni
 - Errori H/W software
 - Errori umani
- Intrusione
 - Penetrazione di estranei non autorizzati nel sistema
 - Il problema è esplosivo nel contesto di rete
- Segretezza
 - Protezione dell'informazione che riguarda gli individui
 - Oggetto in Italia di recente normativa

Obiettivi della gestione della sicurezza

- Disponibilità
 - L'accesso ai dati deve essere garantito
- Confidenzialità
 - Accesso consentito ai soli utenti autorizzati
- Integrità
 - I dati non devono corrompersi
- Autenticazione
 - L'identità degli utenti deve essere controllata
- Non ripudio
 - Il responsabile di una azione non deve poter negarla

Disponibilità (availability)

- Gli utenti legittimi devono poter accedere ai servizi e ai dati ogniqualvolta ne hanno necessità
- L'accesso può essere impedito da azioni di sabotaggio
- *Attacco di Denial of service*
- Spesso si tende a sottostimare il sabotaggio
- Gli sforzi si concentrano ancora sulle intrusioni
- Grandi portali sono stati attaccati (tramite *spamming*), rendendo il servizio indisponibile agli utenti (es. attacco al sito Yahoo)

Confidenzialità

- I dati devono essere protetti dagli accessi di persone non autorizzate
- Nessun utente deve ottenere dal sistema informazioni (di qualsiasi tipo), che non è previsto che abbia
- Occorre definire e far rispettare schemi di controllo, basati su:
 - Classificazione delle informazioni
 - Registrazione e identificazione degli utenti
 - Privilegi accordati agli utenti

Integrità

- I dati non devono essere modificati (direttamente o indirettamente) da:
 - Utenti non autorizzati (intrusi)
 - Incidenti (crash, rottura di dispositivi)
- Deve essere sempre possibile controllare se i dati siano stati modificati
- Deve essere possibile ripristinare l'integrità dei dati, in seguito alla scoperta di azioni non autorizzate
- Occorre avere una politica sistematica di backup
- Protezione dell'informazione tramite duplicazione

Autenticazione

- Verificare l'identità di una persona o dell'origine dei dati
- Il sistema deve controllare che l'utente sia veramente la persona che pretende di essere
- Travestimento: un intruso cerca di impersonare un utente registrato per sfruttarne i privilegi
- Problema arduo nei sistemi distribuiti
 - Nessun contatto diretto con l'utente
 - L'informazione di autenticazione viaggia sulla rete

Non ripudio

- L'originatore (responsabile) di ogni azione specifica deve essere identificato ed autenticato
- Il sistema deve raccogliere informazioni tali da impedire al responsabile di negarne in seguito la paternità
- Autenticazione dell'informazione
 - Firma digitale
 - Certificati
 - Marcatura temporale

Attacchi attivi e passivi

- Attacchi passivi
 - Tesi ad intercettare dati ed a carpirne il contenuto
 - Violano solo la confidenzialità
- Attacchi attivi
 - Tesi a modificare le comunicazioni ed i dati
 - Più difficili da attuare, ma molto pericolosi
- Obiettivi
 - Dispositivi e computer connessi alla rete
 - Pacchetti che transitano sulla rete
 - Procedure: procedure di autenticazione, protocolli

Tipologie di intrusi

- Utenti casuali
 - Connessi ai sistemi e mossi dalla curiosità
- Insiders
 - Sistemisti, operatori etc, abilità e senso della sfida
- Criminali
 - Almeno hanno una motivazione seria (il denaro)
- Spie
 - Spionaggio sia militare che industriale
- Sabotatori
 - Distruggere informazioni e colpire la capacità operativa
 - Minaccia spesso sottovalutata

Sniffing e spoofing

- Sniffing
 - Analisi del traffico tramite installazione di programmi ad hoc (sniffer), ad es. Su una LAN
 - Tramite lo sniffing gli hacker si procurano informazioni preziose, tipicamente le password
- Spoofing
 - Simulazione del comportamento di un host e invio di messaggi che simulano quelli veri
 - Gli utenti autorizzati cadono nella trappola e forniscono informazioni riservate

Backdoor e Cavalli di Troia

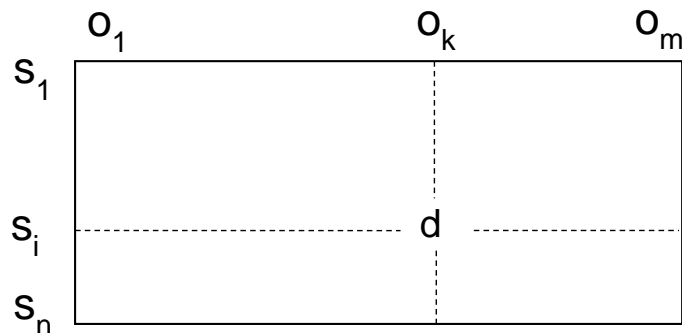
- Backdoor
 - Punto di entrata ‘non ufficiale’ nel sistema
 - Predisposte dagli sviluppatori software (*just-in-case*)
 - Dovrebbero rimanere segrete: a volte non lo restano
- Cavalli di Troia
 - Programmi che imitano applicazioni ben note all’utente
 - Ad es. MS office, Explorer, ecc.
 - Compiono anche alcune azioni ‘extra’
 - Ad es. Comunicano al loro ‘padrone’ le password di sistema ogni volta che vengono cambiate

Controllo degli accessi

- Soggetti
 - Utenti del sistema e processi
 - Chiedono di accedere agli oggetti
- Oggetti
 - Dati, programmi, risorse del sistema
- Operazioni
 - Tipi di accesso agli oggetti: es. read, write, execute

Diritto: privilegio concesso ad un soggetto di effettuare una data operazione su di un dato oggetto

Matrice degli accessi



- Righe: *soggetti*
- Colonne: *oggetti*
- Elementi: *diritti*

Access list e capability list

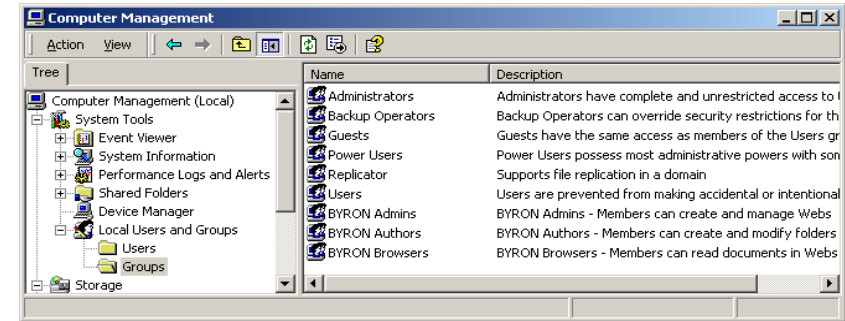
- La matrice degli accessi è in genere molto sparsa
- Utilizzate rappresentazioni equivalenti
- Access list:
 - Una per ogni oggetto
 - Lista tutti i soggetti che detengono diritti sull’oggetto
- Capability list:
 - Una per ogni soggetto
 - Lista tutti gli oggetti su cui il soggetto detiene diritti

Politiche di sicurezza

Regolano i criteri di concessione dei diritti

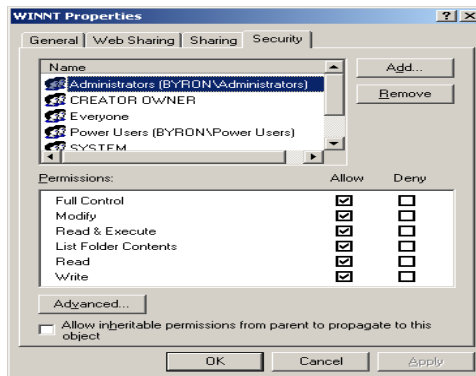
- Massimo privilegio
 - È permesso tutto ciò che non è esplicitamente vietato
 - Massima disponibilità dei dati
 - Tipica degli ambienti 'aperti'
- Minimo privilegio
 - È vietato tutto ciò che non è esplicitamente permesso
 - Minima disponibilità dei dati
 - Detta anche 'need-to-know policy'
 - Tipica degli ambienti militari

Utenti e Gruppi in NT



- Utenti: registrati e identificati tramite password
- Gruppi: gruppi di utenti cui sono associati diritti di accesso
- Un utente può appartenere a più gruppi ed eredita i diritti di accesso dei gruppi ai quali appartiene

Controllo degli accessi in NTFS



- Ciascun oggetto ha un proprietario (*owner*)
- L'owner può assegnare diritti di accesso differenziati ai vari utenti e gruppi nel sistema
- Possibile un *audit* selettivo che tiene traccia degli accessi

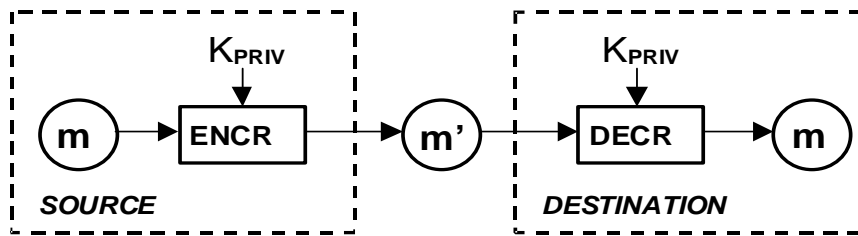
Cifratura dell'informazione

$$E(m, k_E) = m' \quad , \quad D(m', k_D) = m$$

m : messaggio
 m' : messaggio cifrato
 E : funzione di cifratura
 D : funzione di decifratura
 k_E : chiave di cifratura
 k_D : chiave di decifratura

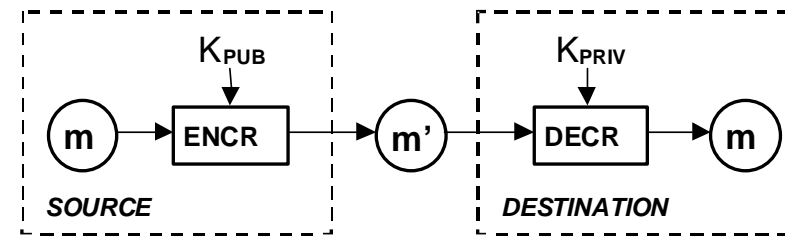
- L'informazione può essere protetta tramite *cifratura*
- Scema validi sia per trasmissione, che per memorizzazione/rilettura
- Vari problemi fra cui lo scambio e la conservazione delle chiavi

Codici a chiave privata



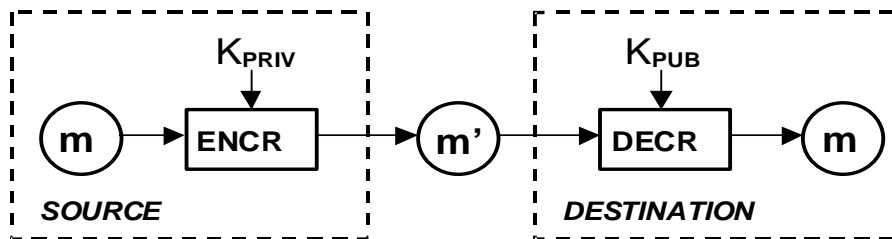
- La chiave di cifratura coincide con quella di decifratura in un'unica chiave K_{PRIV}
- Problema: i corrispondenti devono scambiarsi la chiave
- Entrambi la devono conservare con cura
- La conoscenza della chiave compromette il codice

Codici a chiave pubblica



- Codifica effettuata con la *chiave pubblica* K_{PUB} , nota a tutti
- Decodifica effettuata con la *chiave privata* K_{PRIV}
- La chiave pubblica non consente di decodificare i messaggi
- Nessun problema nella distribuzione della chiave pubblica
- Per comunicare nei due sensi occorrono due coppie di chiavi

Autenticazione

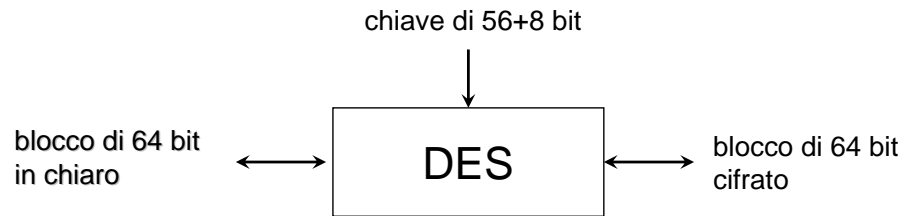


- Codifica effettuata con la chiave privata
- Il possessore della chiave privata firma il messaggio
- Chiunque, con la chiave pubblica può verificare se il messaggio è stato effettivamente cifrato dal possessore della chiave privata
- Meccanismo largamente utilizzato su Internet
- Necessaria una *terza parte* che garantisca l'autenticità delle chiavi

DES (Data Encryption Standard)

- Standard di cifratura a chiave privata usato dall'amministrazione federale degli USA
- Non abbastanza per la sicurezza nazionale: può essere decifrato dalla NSA (*National Security Agency*)
- Molto diffuso, è diventato uno standard *de facto*
- Codifica molto efficiente, anche su un PC
- Due varianti
 - *Normal DES*
 - *Triple DES, con chiavi da 112 bit*
 - *Triple DES è richiesto nelle applicazioni commerciali*

DES: cifratura del blocco



- *Cifrario a blocchi*: opera su blocchi elementari di 64 bit, tramite l'uso di una chiave di 56 bit, più 8 bit di parità
- Sequenza di numerosi round elementari, di cifratura debole (trasposizioni ecc.)
- Dopo ciascun round il blocco viene diviso in due e le due metà scambiate

Triple-DES (TDES o 3DES)

- Una chiave di 56 bit non è ormai più inviolabile
 - 2^{56} è 'poco più' di 76 milioni di miliardi
- Nel Triple-DES, si applica l'algoritmo DES per tre volte consecutive, usando tre chiavi differenti
 - Tre chiavi di 56 bit ciascuna per un totale di 168 bit
 - Livello di sicurezza inferiore a quello di DES con una chiave a 168 bit
 - Livello di sicurezza pari a quello che sarebbe garantito da DES utilizzando una chiave a 112 bit (risultato matematico, non intuitivo)

RSA (Rivest, Shamir e Adleman)

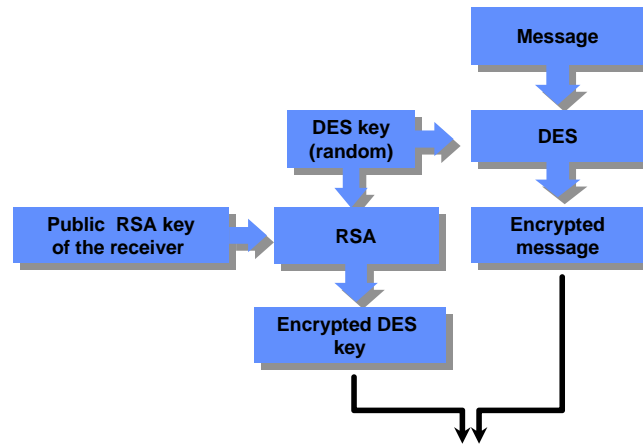
- Algoritmo di cifratura a chiave pubblica
- Brevettato nel 1978, RSA è diventato uno standard *de facto* per la cifratura a chiave pubblica
- Basato sulla *difficoltà di fattorizzare un intero*
 - Non esistono algoritmi efficienti per interi grandi
- Diverse lunghezze di chiave
 - Chiavi più lunghe: maggiore sicurezza, ma maggiore costo di elaborazione
 - Chiavi di 512 -1024 bit sono accettabili per la maggior parte delle applicazioni

Cifratura con RSA e DES

- Se il messaggio è lungo RSA può essere troppo lento
- RSA e DES possono essere usati insieme
 - Il mittente genera una chiave DES
 - Cifra il messaggio con DES
 - Invia il messaggio con DES
 - Invia la chiave DES usando RSA (cifrando con la chiave pubblica del destinatario)
 - Il destinatario decifra la chiave DES usando la sua chiave privata RSA
 - Il destinatario usa la chiave DES per decifrare il messaggio

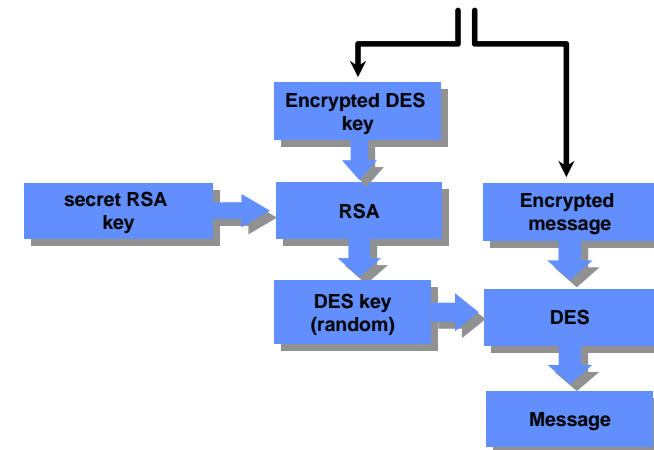
Cifratura con RSA e DES

LATO MITTENTE



Cifratura con RSA e DES (2)

LATO DESTINATARIO



Digest

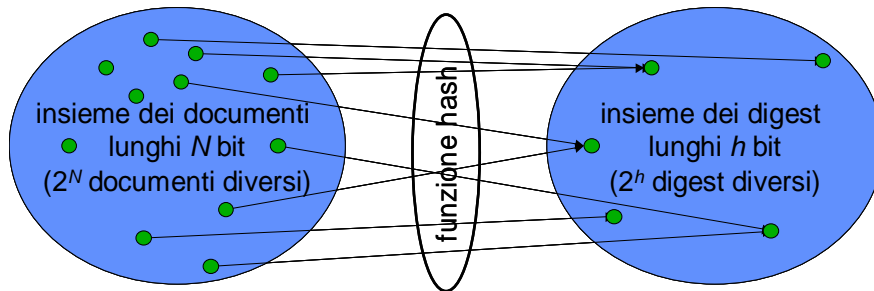
- Un digest è un piccolo file estratto da un grosso documento con proprietà molto particolari
- Dato un documento D, un *metodo di hashing* consente di ottenere un breve digest di lunghezza fissa
- Documenti diversi generano digest diversi
- Il processo non è *reversibile*
 - Dato un documento è facile ottenere il digest
 - Dato un digest è praticamente impossibile ottenere un documento che corrisponde a quel digest
- Se il documento è modificato il digest cambia

Calcolo di un digest

- Proposti molti metodi
- Solo un paio sono usati come standard
- **SHA** genera un digest di 160 bit
- **MD5** genera un digest di 128 bit

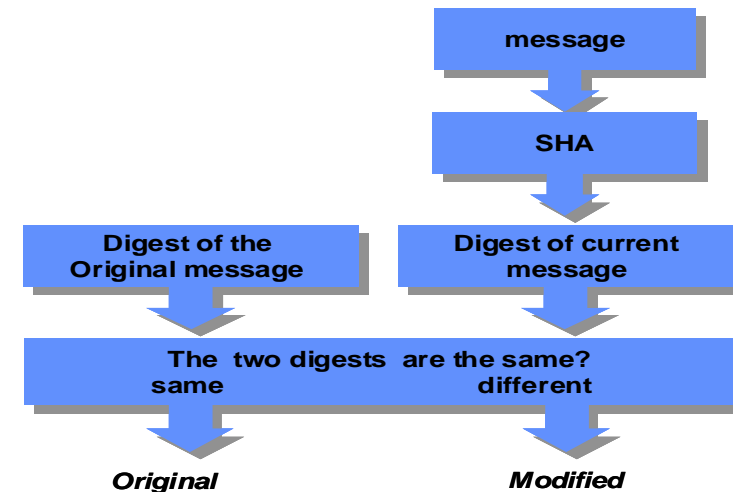
Conservando in modo sicuro il digest di un documento è sempre possibile controllare se è stato modificato (non è necessario conservare in modo sicuro l'intero documento).

Invertibilità del digest



- Se $N \gg h$: fenomeni di collisione sono inevitabili
- Esistono digest corrispondenti a più di un documento
- La funzione hash dunque è non iniettiva e non invertibile

Controllo dell'integrità



Firma digitale

- La firma digitale è una sequenza di bit che dipende dal firmatario e dai dati che sono firmati
- Chiunque può facilmente controllare la firma
- La firma non può essere falsificata, anche da un attaccante che conosca la firma su altri documenti
- Il firmatario non è in condizione di poter ripudiare la firma da lui apposta ad un documento
- La procedura di firma è semplice e veloce
- La procedura di controllo della firma è semplice e non richiede contatto diretto col firmatario

Specifiche della firma digitale

- La firma digitale è una funzione del messaggio firmato e della chiave segreta del firmatario
- Firme della stessa persona su documenti diversi devono essere diverse
- La conoscenza anche di molte firme del firmatario non è di utilità nella contraffazione
- Solo il detentore della chiave può firmare
- Se qualcuno falsifica la mia firma, questo significa che conosce la mia chiave segreta

Generazione della firma digitale

- Un semplice metodo di firma digitale è basato su RSA e funzioni di hashing

PASSO 1

- Calcolare il digest del messaggio tramite una funzione di hashing

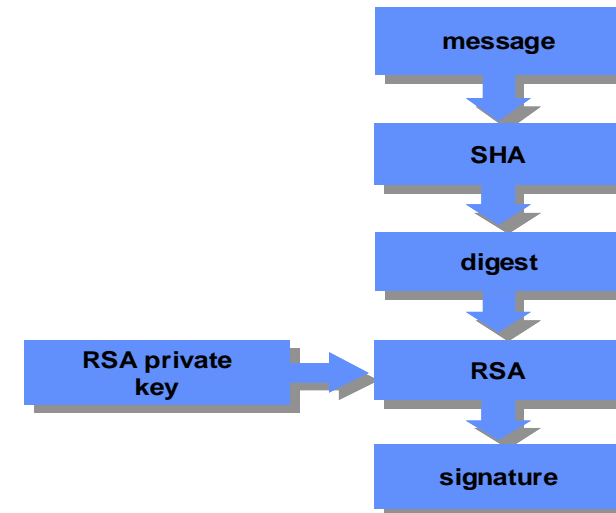
PASSO 2

- Cifrare il digest con RSA usando la propria chiave privata

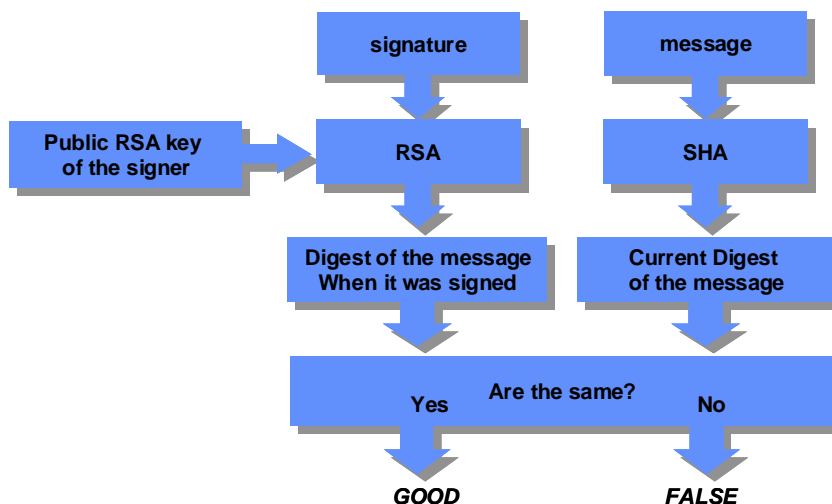
PASSO 3

- Chiunque può controllare la firma usando la chiave pubblica del firmatario

Generazione della firma



Verifica della firma



Certification Authority

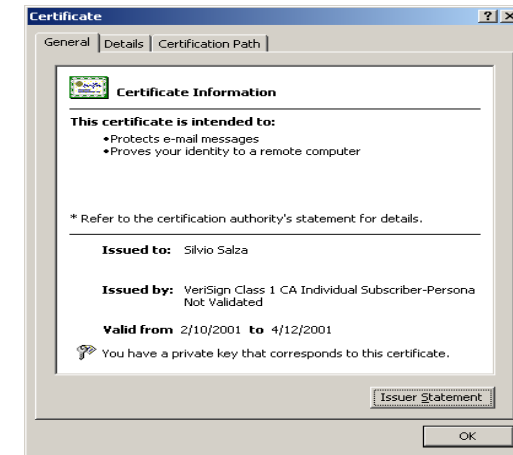
- Come mi procuro la chiave pubblica del firmatario?
- Occorre un'autorità credibile e *super partes*
- Una Certification Authority (CA)
 - Identifica ed autentica gli utenti
 - Conserva le chiavi pubbliche
 - È ritenuta credibile da tutti gli utenti
 - Fornisce a richiesta le chiavi pubbliche

Certificati digitali

- La CA pubblica i certificati firmandolo con la propria chiave privata
- Ciascun certificato include
 - Nome della Certification Authority
 - *Timestamp* di validità del certificato
 - Nome e dati dell'utente
 - La chiave pubblica dell'utente



Certificati digitali (ITU X-509)



- ITU (*International Telecommunication Union*) X-509
- IETF (*Internet Engineering Task Force*) RFC 1422

Verifica della firma digitale

- Include i seguenti passi
 - Chiedere alla CA la chiave pubblica del firmatario
 - La CA invia il certificato firmato con la sua chiave
 - La CA garantisce la validità della chiave pubblica
 - Effettuare la comparazione
- Procedura svolta automaticamente dal software

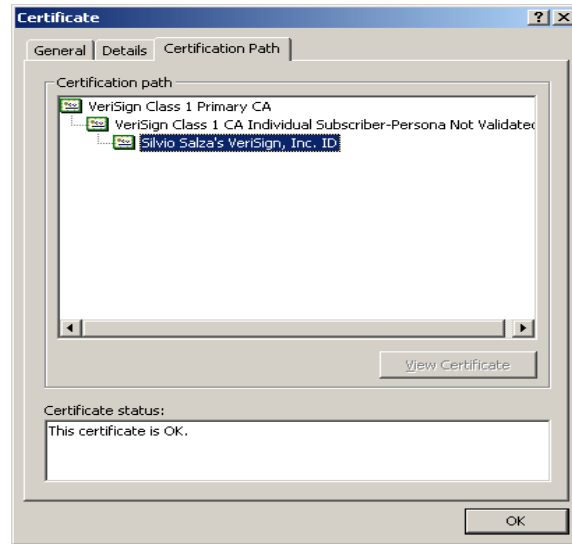
Es. Basta installare i certificati (incluso il proprio) ed Outlook Express gestisce posta cifrata ed autenticata

Quis custodiet custodes

- Perché devo fidarmi della firma della CA?
- Regolamenti nazionali ed internazionali sulle CA
- Il certificato della CA è firmato da una CA di livello più alto
- Posso seguire la 'chain of trust'
- Molto software può fare direttamente questi controlli

Alla fine ci possiamo fidare di Microsoft?

Chain of trust



Identificazione e autenticazione

- Identificare li utenti all'atto dell'accesso al sistema
- Autenticare l'identificazione per mezzo di oggetti o informazioni posseduti o conosciuti dall'utente
- Informazioni conosciute
 - Password
 - Query/answer
- Oggetti posseduti
 - Token di vario tipo
 - Smartcard
- Caratteristiche dell'utente
 - Impronte digitali e vocali
 - Impronte retiniche

Autenticazione tramite password

- L'utente sceglie la password e la comunica in chiaro al sistema
- Il sistema la cifra e la conserva in forma cifrata in un apposito file, il *password file*
- Negli accessi successivi l'utente esibisce la password in chiaro
- Il sistema la ricifra e la confronta con quella cifrata conservata nel password file
- Anche chi si impossessasse del *password file* non può risalire alle password in chiaro
- L'algoritmo di cifratura è noto, si può quindi provare ad indovinare

Rottura delle password

- Gli utenti hanno poca fantasia nella scelta delle password
- In qualsiasi sistema esiste un numero adeguato di cretini (*legge di Cipolla*)
- L'attaccante per prima cosa si impossessa del *password file*
- Questo contiene le password di tutti gli utenti *in forma cifrata*
- L'attaccante possiede un *dizionario di password 'probabili'*, tutte già cifrate
- Deve solo confrontare il *dizionario delle password cifrate e password file*
- Funziona in un numero sorprendente di casi

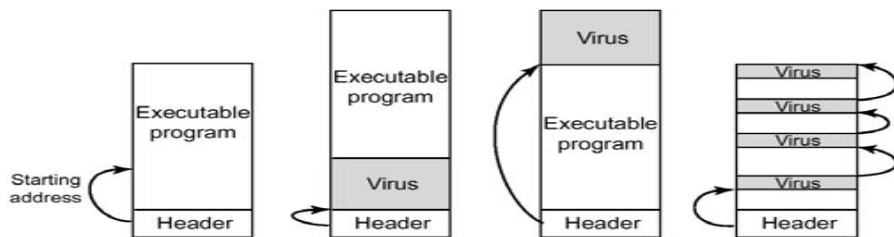
Gestione delle password

- Il SO operativo permette di mettere vincoli sulla forma delle password
- Altri vincoli possono essere messi sulla scadenza e sull'impossibilità di riutilizzare vecchie password
- Situazione particolarmente delicata nel caso di reti: occorre evitare che le password viaggino in chiaro
- One-time password: ogni utente ha una lista di password che possono essere usata ciascuna una volta sola
- Comunicazione sicura: collegamento tramite software client-server che apre una sessione cifrata con doppia coppia di chiavi asimmetriche

Virus

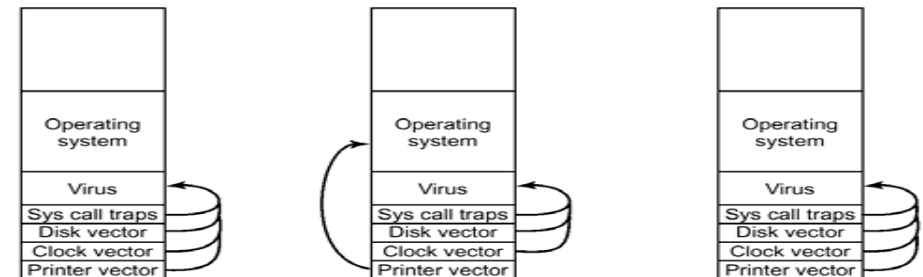
- Programmi *malintenzionati* scritti allo scopo di:
 - Distruggere informazioni
 - Rendere indisponibili servizi
 - Propagarsi ad altri sistemi
- Rientrano nella categoria dei sabotaggi
- Cominciato per gioco (e finito male!)
- Possono causare danni enormi
- I LOVE YOU: 1 miliardo di dollari
- Azioni criminali: ricatto
- Sabotaggio militare
- Più spesso semplicemente vendetta e/o vandalismo
- Problema moltiplicato con Internet
- Anche danni hardware, es. la flash ROM della scheda madre

Virus parassiti



- Si attaccano ad un programma eseguibile, e ne precedono l'esecuzione
- Posizionamento all'inizio o alla fine (piggybacking)
- Possono andare ad occupare spazi liberi nel file (cavity virus)
- Quando vanno in esecuzione:
 - infettano tutti i programmi che trovano
 - svolgono azioni dannose, a volte in tempi ritardati

Boot Sector virus



- Si insediano nel *boot sector*: si attivano prima del boot
- Si installano in memoria centrale nella zona delle routine di interruzione, *prima* che il sistema operativo parta
- Si aggiungono alla routine che serve la trap di sistema
- Vengono attivati ad ogni system call

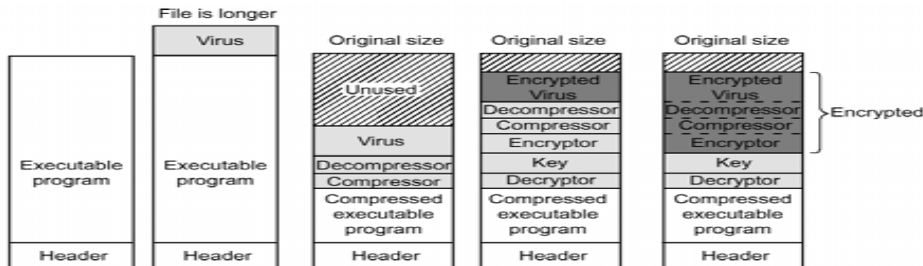
Macro virus

- Si insediano nelle macro che alcune applicazioni permettono di definire
- Le macro sono programmi a tutti gli effetti, e quindi possono far danno
- Il Virus Melissa si inserisce come macro in documenti Office
- Office avverte che il file contiene una macro, ma molti utenti...
- Il documento viene spedito per e-mail
- La macro si attiva quando il documento viene aperto e infetta tutti i documenti dello stesso tipo che trova

Tecniche antivirus

- Scanning
si confronta il codice di tutti i programmi eseguibili con un database di segmenti di codice di virus noti,
- Integrity Checking
si creano impronte dei file (quando sono sani!) e si verifica che non cambino
- Behavioral Checking
si sorveglia il comportamento dei programmi, controllando che non facciano azioni strane, accedere al boot sector etc.
- Prevenzione
 - Installare software antivirus
 - Cautela nell'aprire attachment di e-mail
 - Controllare dischetti ignoti e software pirata

Tecniche anti-antivirus



- Ripristino della lunghezza originale tramite compressione
- Cifratura del virus per evitare lo *scanning*
- Chiave di cifratura sempre diversa
- Cifrato anche tutto il resto, escluso il *decicifratore*
- Il software antivirus può individuare il decifratore, rimasto fuori

Virus polimorfici

- Per ingannare gli scanner il virus cambia la parte visibile del suo codice ogni volta che si riproduce
- Permutazione delle istruzioni lasciando inalterata la funzionalità
- Il virus contiene un *mutation engine* che genera mutazioni in un esteso insieme:
 - Il mutation engine è contenuto nella parte cifrata del virus, e non può essere scoperto
 - Il decifratore è l'unica parte visibile ma cambia in continuazione e non può essere scoperto

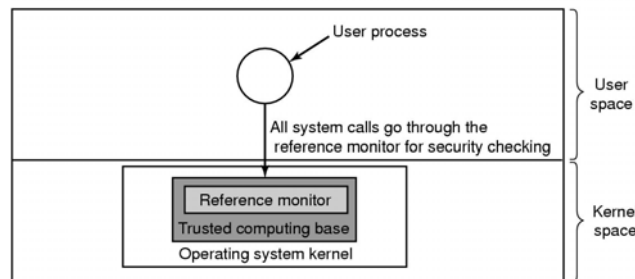
Standard per la sicurezza

- Livelli di sicurezza attribuibili ai sistemi informatici sulla base di criteri predefiniti
- TCSEC (Trusted Computer System Evaluation Criteria)
 - Introdotti dal DoD (Department of Defense)
 - “Orange Book”, dal colore della copertina
 - Adottato nell’85 dal DoD come standard
- Procedure di controllo e certificazione
 - Introdotte dall’amministrazione federale USA
 - Riconosciute come standard de facto
- Certificazione di prodotti commerciali

Orange book (TCSEC)

- D, sicurezza assente
- C, sicurezza media
 - C1, sicurezza discrezionale
 - C2, sicurezza obbligatoria
- B, sicurezza media-alta
 - B1, non consente di modificare i permessi di accesso ai file
 - B2, classificazione del livello di sicurezza dei dispositivi HW
 - B3, usa HW specifico per proteggere risorse importanti
- A, sicurezza massima – certificata
 - per ora, mai raggiunta

Architettura dei sistemi sicuri



- **Trusted computing base**: cuore del sistema che verifica la sicurezza, ed il cui funzionamento è garantito formalmente
- Include un insieme di funzioni cruciali del kernel
- **Reference monitor**: controlla tutte le richieste dei processi critiche da un punto di vista della sicurezza

Orange Book: criteri e classi

Criterion	D	C1	C2	B1	B2	B3	A1
Security policy							
Discretionary access control		X	X	→	→	X	→
Object reuse			X	→	→	→	→
Labels				X	X	→	→
Label integrity				X	→	→	→
Exportation of labeled information				X	→	→	→
Labeling human readable output				X	→	→	→
Mandatory access control				X	X	→	→
Subject sensitivity labels					X	→	→
Device labels					X	→	→
Accountability							
Identification and authentication		X	X	X	→	→	→
Audit			X	X	X	X	→
Trusted path					X	X	→

→ : come la classe inferiore

X : ulteriori restrizioni

Orange Book: criteri e classi (2)

Criterion	D	C1	C2	B1	B2	B3	A1
Assurance							
System architecture		X	X	X	X	X	→
System integrity		X	→	→	→	→	→
Security testing		X	X	X	X	X	X
Design specification and verification				X	X	X	X
Covert channel analysis					X	X	X
Trusted facility management					X	X	→
Configuration management					X	→	X
Trusted recovery						X	→
Trusted distribution							X
Documentation							
Security features user's guide		X	→	→	→	→	→
Trusted facility manual		X	X	X	X	X	→
Test documentation		X	→	→	X	→	X
Design documentation		X	→	X	X	X	X

→ : come la classe inferiore

X : ulteriori restrizioni

Altri standard di sicurezza

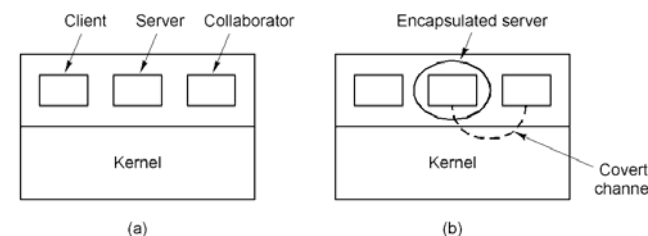
- ITSEC, 1991, Europa
 - Francia, Germania, Olanda e Regno Unito
- CTCPEC, 1993, Canada
 - TCSEC + ITSEC = CTCPEC
- 1993, inizia negli USA la “fusione” degli standard...
- CCITSE (Common Criteria for Information Technology Security Evaluation), 1996, noti più semplicemente come “Common Criteria”
 - ISO/ICI 15408
 - 7 livelli di sicurezza, EAL1...EAL7, approssimativamente corrispondenti ai livelli TCSEC

Normativa italiana

- Legge 675/96
 - “Privacy” nel trattamento di dati personali
- Art. 15, comma 2, legge 15-3-1997, n. 59
 - Atti e documenti elettronici
- DPR 513-97
 - Regolamento per attuazione firma elettronica
- DPCM 8-2-1999
 - Formazione, trasmissione e gestione dei documenti informatici
- DPR 318-99
 - Misure minime di sicurezza per il trattamento dei dati personali
- DPCM 31-10-2000
 - regole tecniche per il protocollo informatico

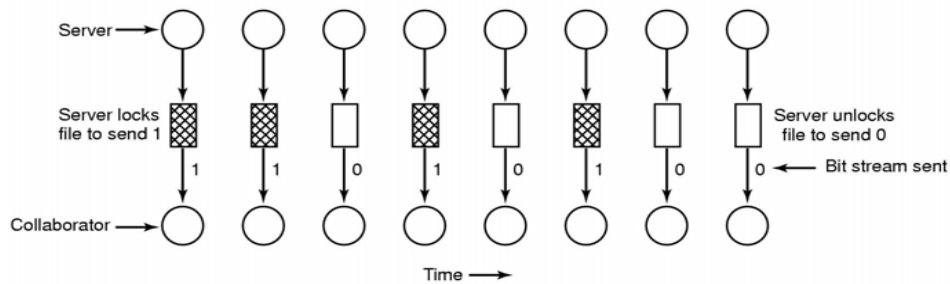
Documentazione alla URL <http://www.cnipa.it>

Covert channel



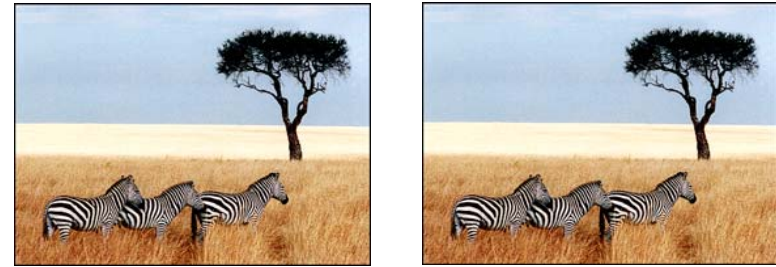
- Sistemi sicuri impediscono il passaggio dell'informazione riservata, di un soggetto *client*, verso l'esterno
- La barriera può essere aggirata tramite un *covert channel*
- Collaborazione di un soggetto interno (*server*)
- Metodo di comunicazione: il complice (*collaborator*) riceve l'informazione osservando “fenomeni” apparentemente scorrelati

Covert channel: file locking



- L'informazione viene trasmessa dal *server* effettuando il blocco e lo sblocco di un file
- Il *collaboratore*, provando ad accedere al file ricava il messaggio come sequenza di 0 e 1
- Comunicazione lenta, canale rumoroso

Covert channel: codifica segreta



- La foto di sinistra contiene nascoste 5 opere di Shakespeare
- Foto di 1024 x 768, nella codifica RGB tre byte per pixel
- Si sfruttano i 3 bit meno significativi di ogni pixel
- 'Rumore' impercettibile nella foto
- Circa 300 Kbyte di informazione segreta, usati per il testo compresso delle 5 opere