Unità E2

Sicurezza e privacy

Obiettivi

- Conoscere il concetto di crittografia e i principali algoritmi di crittazione
- Apprendere il concetto di firma digitale
- Conoscere le leggi sulla privacy
- Conoscere i concetti di base sulla sicurezza dei sistemi
- Conoscere i tipi di minacce che possono provenire dal mondo esterno
- Conoscere la differenza tra minacce sui dati e basate sull' infrastruttura
- Conoscere alcuni strumenti per la sicurezza, come i firewall

Terminologia

- **Steganografia**: occultamento del messaggio
- **Crittografia**: occultamento del significato del messaggio
- **Messaggio in chiaro**: testo da crittare
- **Chiave**: informazione usata come parametro in un algoritmo crittografico
- **Crittoanalisi**: scienza dell' interpretazione del messaggio di cui si ignora la chiave

Steganografia

- Il termine steganografia è composto dalle parole greche στεγανός (nascosto) e γραφία (scrittura) e individua una tecnica risalente all'antica Grecia che si prefigge di nascondere la comunicazione tra due interlocutori, e fu teorizzata dall'abate Tritemio attorno al 1500 nell'omonimo libro.
- La steganografia si pone come obiettivo di mantenere nascosta l'esistenza di dati a chi non conosce la chiave atta ad estrarli.
- Un esempio: LSB (least significant bit, bit meno significativo) è la tipologia di steganografia più diffusa. Si basa sulla teoria secondo la quale l'aspetto di un'immagine digitale ad alta definizione non cambia se i colori vengono modificati in modo impercettibile.
- Ogni pixel è rappresentato da un colore differente, cambiando il bit meno significativo di ogni pixel, il singolo colore non risulterà variato e il contenuto dell'immagine sarà preservato nonostante questa manipolazione…

Wikipedia

Crittografia

- La parola crittografia deriva dall'unione di due parole greche: κρυπτός (kryptós) che significa "nascosto", e γραφία (graphía) che significa "scrittura".
- La crittografia tratta delle "scritture nascoste", ovvero dei metodi per rendere un messaggio "offuscato" in modo da non essere comprensibile a persone non autorizzate a leggerlo.
- Un tale messaggio si chiama comunemente crittogramma.
- Lo studio della crittografia e della crittanalisi si chiama comunemente crittologia.

Wikipedia

Chiave

- In crittografia una chiave è un'informazione usata come parametro in un algoritmo crittografico.
- Le chiavi sono utilizzate in molte applicazioni crittografiche e sono l'unico dato che è davvero necessario tenere segreto.
- La dimensione della chiave, generalmente misurata in bit, dipende dal particolare algoritmo usato.
- Esiste un metodo per stimare la lunghezza minima della chiave da utilizzare e si basa sulla simulazione di un attacco di forza bruta: una chiave di n bit avrà 2^n chiavi distinte e non conoscendo quale chiave sia stata usata bisognerà provarle tutte fino ad individuare la chiave giusta.

Wikipedia

Crittoanalisi

- Per crittoanalisi (dal greco kryptós, "nascosto", e analýein, "scomporre") si intende lo studio dei metodi per ottenere il significato di informazioni cifrate senza avere accesso all'informazione segreta che è di solito richiesta per effettuare l'operazione.
- Tipicamente si tratta di trovare una chiave segreta. La crittoanalisi è la "controparte" della crittografia, vale a dire lo studio delle tecniche per occultare un messaggio, ed assieme formano la crittologia, la scienza delle scritture nascoste.

Wikipedia

Storia della crittografia

Crittografia classica

(dall'antichità al 1975)

- I metodi più antichi di cui abbiamo notizia sono
  - la skytala lacedemone,
  - la scacchiera di Polibio,
  - il codice atbash
  - il codice di Giulio Cesare.
- I successivi risalgono al Rinascimento:
  - Leon Battista Alberti (inventore della cifra polialfabetica e forse dell'analisi di frequenza),
  - Blaise Vigenère
  - Giovanni Battista Bellaso
- Nel ventesimo secolo sono stati sviluppati
  - la macchina Enigma (usata dai tedeschi durante la Seconda Guerra Mondiale),
  - il DES (Data Encryption Standard)

Crittografia Moderna

- La crittografia moderna nasce nel 1975 con un articolo di Diffie & Hellman nel quale si proponeva un nuovo protocollo per lo scambio delle chiavi, che è e rimane il vero tallone d'Achille della crittografia classica.
- Un aspetto fondamentale è la possibilità dell'applicazione alla trasmissione sicura di dati fra entità che non hanno concordato preventivamente le chiavi, e che non necessariamente si fidano l'una dell'altra.
- Esempi:
  - DES
  - doppio lucchetto
  - RSA

Crittografia Classica

500-600 a.c. cifrario ATBASH

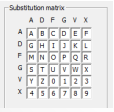
- L'atbash è un semplice cifrario a sostituzione monoalfabetica in cui la prima lettera dell'alfabeto è sostituita con l'ultima, la seconda con la penultima, e così via, "invertendo" l'ordine alfabetico delle lettere.
- Testo in chiaro:
  - a b c d e f g h i l m n o p q r s t u v z
- Testo cifrato:
  - Z V U T S R Q P O N M L I H G F E D C B A
- Un esempio:
  - PIANO LAUREE SCIENTIFICHE
  - KRZML OZFIVV HXRVMGRURXSV

400 a.c. Scitala spartana

- Una scitala (dal greco σ κ υ τ ά λ η = bastone) era una piccola bacchetta utilizzata dagli Spartani per trasmettere messaggi segreti.
- Il messaggio veniva scritto su di una striscia di pelle arrotolata attorno alla scitala, come se fosse stata una superficie continua.
- Una volta srotolata e tolta dalla scitala la striscia di pelle, era impossibile capire il messaggio.
- La decifrazione era invece possibile se si aveva una bacchetta identica alla scitala del mittente: vi si arrotolava nuovamente la striscia di pelle ricostruendo la primitiva posizione.
- Si tratta del più antico metodo di crittografia per trasposizione conosciuto.

150 a.c. Scacchiera di Polibio

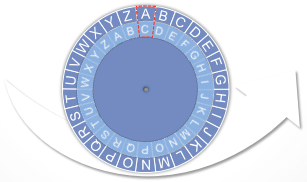
- La scacchiera originale è costituita da una griglia composta da 25 caselle ordinate in 5 righe ed altrettante colonne.
- Le lettere dell'alfabeto vengono inserite da sinistra a destra e dall'alto in basso.
- Le righe e le colonne sono numerate: tali numeri sono gli indici o "coordinate" delle lettere costituenti il messaggio in chiaro.
- Esempio
  - PIANO LAUREE SCIENTIFICHE
  - FGDFAAFDFFDXAAGFFXAVAVGAAFDFAVFDGDDFAXDFAFDDAV



50-60 a.c. Il metodo di Cesare

- Il cifrario di Cesare è un cifrario a sostituzione monoalfabetica in cui ogni lettera del testo in chiaro è sostituita nel testo cifrato dalla lettera che si trova un certo numero di posizioni dopo nell'alfabeto.
- Questi tipi di cifrari sono detti anche cifrari a sostituzione o cifrari a scorrimento a causa del loro modo di operare: la sostituzione avviene lettera per lettera, scorrendo il testo dall'inizio alla fine.
- In particolare, Cesare utilizzava uno spostamento di 3 posizioni (la chiave era dunque 3).
- Un esempio:
  - PIANO LAUREE SCIENTIFICHE
  - RKCPQ NCWTGG UEKGPVKHKEJG

Cifrari a scorrimento



Debolezze del metodo di Cesare

- Il metodo di Cesare ha due principali debolezze:
  - è sensibile all'analisi di frequenza
  - sono possibili solo poche codifiche diverse (n – 1) se n è il numero di caratteri dell'alfabeto.
- Chi intercetta un messaggio cifrato con il metodo di Cesare può limitarsi a provare successivamente tutte le possibili chiavi di cifratura e trovare il testo in chiaro in un tempo ragionevolmente breve (attacco a forza bruta).

1586 Il cifrario di Vigenère

- E' il più semplice dei cifrari polialfabetici.
- Pubblicato nel 1586, il cifrario di Blaise de Vigenère fu ritenuto per secoli inattaccabile.
- Si può considerare una generalizzazione del cifrario di Cesare: invece di spostare sempre dello stesso numero di posti la lettera da cifrare, questa viene spostata di un numero di posti variabile ma ripetuto, determinato in base ad una parola chiave da scrivere ripetutamente sotto il messaggio, carattere per carattere.
- Un esempio:
  - PIANO LAUREE SCIENTIFICHE
  - ITIS
  - XBIFW EIMZXM KKBMFBBNAKAM

Vigenère - Cesare

- Il metodo di Vigenère rendere impossibile l'analisi di frequenza perchè le lettere più frequenti saranno codificate con lettere diverse da colonna a colonna, con il risultato di rendere quasi uguali le frequenze relative delle lettere del testo cifrato.
- Il metodo di Vigenère sembra essere molto più robusto di quello di Cesare perché il crittografo ha due problemi:
  - determinare la lunghezza k della chiave
  - e poi la chiave stessa.
- Se l'alfabeto ha n caratteri, vi sono n^k possibili chiavi di cifratura, mentre sono solo $n!/(n-k)!$ se vogliamo che i caratteri siano tutti diversi fra loro.
- Anche da questo punto di vista il metodo di Vigenère è migliore di quello di Cesare.

Cryptographia ad usum Delphini – A.Zaccagnini

Debolezza del metodo di Vigenère

- Questo metodo è stato considerato sicuro per alcuni secoli, finche un'analisi statistica più raffinata, di Kasinski, mostrò che è possibile "indovinare" la lunghezza k della chiave di cifratura, riducendo il problema della decifratura a k problemi di decifratura del metodo di Cesare.
- L'analisi si basa sul fatto che in ogni lingua vi sono alcune combinazioni di due lettere piuttosto frequenti: se due istanze di questa coppia di lettere compaiono nel testo in chiaro ad una distanza che è un multiplo della lunghezza della chiave, saranno cifrate allo stesso modo, perché vanno a finire nelle stesse colonne.

Cryptographia ad usum Delphini – A. Zaccagnini

Un esempio di steganografia

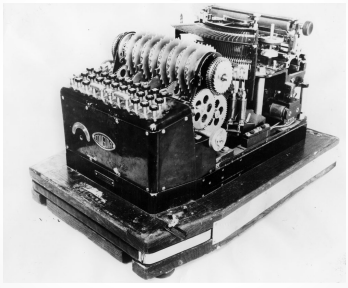
Per il timore di ciascuna di queste cose [Aristagora]meditava una rivolta. Accadde anche che gli arrivasse da Susa, da parte di Istieo, un uomo con la testa tatuata che gli annunciava di ribellarsi al re. Infatti Istieo, volendo segnalare ad Aristagora di ribellarsi, non aveva d'altra parte nessun modo sicuro per farlo, dal momento che le strade erano sorvegliate e quindi, avendo rasato il capo del più fedele dei servi, vi incise dei segni, e attese che gli ricrescessero i capelli; e non appena gli furono cresciuti lo mandava a Mileto, ordinandogli soltanto, una volta giunto a Mileto, di dire ad Aristagora di guardare sul suo capo dopo avergli rasato i capelli. E i segni indicavano, come ho detto prima, rivolta.

Erodoto, Storie

La macchina Enigma

- L'ultimo passo prima della così detta crittografia moderna è costituito dalla costruzione dalla macchina elettromeccanica tedesca ENIGMA usata nella seconda guerra mondiale.
- Essa era composta da ruote con i caratteri incisi sul bordo, e con contatti elettrici in corrispondenza delle lettere in entrambi i lati.
- Il testo in chiaro, digitato su una tastiera, veniva riprodotto utilizzando i caratteri della prima ruota, la quale a sua volta costruiva un nuovo alfabeto utilizzando i caratteri della seconda, e poi della terza, e così via ... Tutte le ruote, e potevano essere parecchie, venivano "scalate", in modo che la sostituzione delle lettere fosse ogni volta diversa.
- La chiave consisteva nel settaggio iniziale delle ruote, che potevano essere posizionate in una quantità di posizioni diverse tanto alta quante più erano le ruote utilizzate.
- Questo meccanismo è facile da costruire via software e abbastanza sicuro, può tuttavia essere infranto. Fu brillantemente attaccato dal matematico polacco Marin Rejewsky che con il suo lavoro permise di decifrare numerosi messaggi militari tedeschi, un fattore che probabilmente contribuì alla vittoria finale degli alleati.

Enigma



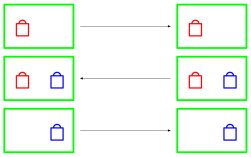
Crittografia Moderna

1975 Diffie-Hellman-Merkle

- Tutti i sistemi di cifratura classici sono detti a chiave segreta ed utilizzano la stessa chiave sia per cifrare che per decifrare.
- Questo costituisce un problema non indifferente se pensiamo all'utilizzo della crittografia per la comunicazione a distanza, infatti le due parti devono riuscire in qualche modo a scambiarsi la chiave con la certezza che nessuno ne venga a conoscenza.
- La soluzione a questo tipo di problema fu proposta nel 1975 da Whitfield Diffie e Martin Hellman, col tributo di Ralph C. Merkle, che ebbero un'intuizione che rivoluzionò il mondo della crittografia.

Il protocollo del doppio lucchetto

- A mette il suo messaggio per B in una scatola, che chiude con un lucchetto e invia a B.
- B mette il suo lucchetto alla scatola e la rispedisce ad A.
- A toglie il suo lucchetto e rispedisce la scatola a B.
- B toglie il suo lucchetto e legge il messaggio.
- La scatola non viaggia mai senza lucchetto
- Ne A ne B ha dovuto inviare all'altro la chiave del proprio lucchetto.
- E' possibile comunicare con sicurezza **senza** dover effettuare un preventivo **scambio delle chiavi**



Crittografia a chiave pubblica

- Diffie ed Hellman pensarono ad un sistema **asimmetrico**, basato su l'uso di due chiavi generate in modo che sia impossibile ricavarne una dall'altra.
- Le due chiavi vengono chiamate **pubblica** e **privata**: la prima serve per cifrare e la seconda per decifrare.
- Una persona che deve comunicare con un'altra persona non deve far altro che cifrare il messaggio con la chiave pubblica del destinatario, che una volta ricevuto il messaggio non dovrà fare altro che decifrarlo con la chiave segreta personale.
- Ogni persona con questo sistema possiede quindi una coppia di chiavi, quella pubblica può essere tranquillamente distribuita e resa di pubblico dominio perché consente solo di cifrare il messaggio, mentre quella privata deve essere conosciuta solo da una persona.
- In questo modo lo scambio di chiavi è assolutamente sicuro.
- Il problema è quello di trovare il modo di implementare matematicamente questo sistema, riuscire cioè a creare due chiavi per cui **non fosse possibile dedurre quella privata conoscendo quella pubblica**.

Il meccanismo in azione

1976 DES

- Il Data Encryption Standard (DES) è un algoritmo di cifratura scelto come standard per il governo degli Stati Uniti d'America nel 1976 e in seguito diventato di utilizzo internazionale.
- Il DES divenne uno standard nel Novembre del 1976 e fu reso pubblico il 15 Gennaio 1977 col nome di FIPS PUB 46.
- Si basa su un algoritmo a chiave **simmetrica** con chiave a 56 bit.

Sicurezza di DES

- Il DES è un sistema molto utilizzato, ma allo stesso tempo insicuro.
- Insicuro in quanto la lunghezza della chiave (solamente 56 bit) consente, tramite attacchi a forza bruta (ovvero tramite tentativi), di scovarla in maniera abbastanza rapida.
- Vi sono diversi sistemi creati per aggirare il DES (DES cracker, COPACOBANA) i quali sono comunque molto costosi partendo dagli 8.000€ arrivando ai 250.000€.
- Vi sono comunque algoritmi che utilizzano chiavi associate ad un numero maggiore di bit, tali da rendere più difficili l'attacco (3DES, IDEA ecc.).

1977 RSA

- L'algoritmo a **chiave asimmetrica** è stato pubblicamente descritto nel 1977 da Ron **Rivest**, Adi **Shamir** e Leonard **Adleman** al **M**assachusetts **I**nstitute of **T**echnology. La sigla RSA deriva dalle iniziali dei cognomi dei tre creatori.
- L'algoritmo è basato su particolari proprietà formali dei numeri primi con alcune centinaia di cifre.
- Non è sicuro da un punto di vista matematico teorico, in quanto esiste la possibilità che tramite la conoscenza della chiave pubblica si possa decrittare un messaggio, ma l'enorme mole di calcoli e l'enorme dispendio in termini di tempo necessario per trovare la soluzione, fa di questo algoritmo un sistema di affidabilità pressoché assoluta.
- Una variante del sistema RSA è utilizzato nel pacchetto di crittografia Pretty Good Privacy (PGP).
- L'algoritmo RSA costituisce la base dei sistemi crittografici su cui si fondano i sistemi di sicurezza informatici utilizzati sulla rete Internet per autentificare gli utenti.

RSA Funzionamento (semplificato)

- A deve spedire un messaggio segreto a B.
- B sceglie due numeri primi molto grandi (per esempio da 300 cifre) e li moltiplica con il suo computer (impiegando meno di un secondo).
- B invia il numero che ha ottenuto ad A. *Chiunque può vedere questo numero.*
- A usa questo numero per cifrare il messaggio
- A manda il messaggio cifrato a B, *chiunque può vederlo ma non decifrarlo*
- B riceve il messaggio e utilizzando i due fattori primi che solo lui conosce lo decifra.
- A e B hanno impiegato pochi secondi a cifrare e decifrare, ma chiunque avesse intercettato le loro comunicazioni impiegherebbe troppo tempo per scoprire i due fattori primi, con cui si può decifrare il messaggio.
- In realtà A e B si scambieranno con questo sistema una chiave segreta (che non occupa molto spazio), che poi useranno per comunicare tra loro usando un sistema a crittografia simmetrica, più semplice e veloce.

Sicurezza di RSA

- Per quanto riguarda l'algoritmo RSA l'attacco a forza bruta (ovvero ottenere i due numeri primi usati per creare la chiave pubblica), è una procedura lentissima.
- L'attacco più veloce è durato 5 mesi utilizzando 80 processori da 2,2GHz
- Questi dati consentono di dire che l'algoritmo è sufficientemente sicuro.

Sicurezza nel mondo internet

1994 - SSL (Secure Socket Layer)

- Transport Layer Security (TLS) e il suo predecessore Secure Sockets Layer (SSL) sono dei protocolli crittografici che permettono una comunicazione sicura e una integrità dei dati su reti TCP/IP come, ad esempio, internet.
- TLS e SSL cifrano la comunicazione dalla sorgente alla destinazione (end-to-end) sul livello di trasporto.
- Diverse versioni del protocollo sono ampiamente utilizzate in applicazioni come i browser, l'E-mail, messaggistica istantanea e VOIP.
- TLS è un protocollo standard IETF che è sviluppato sulla base del precedente protocollo SSL da Netscape

1999 - WEP (Wired Equivalent Privacy)

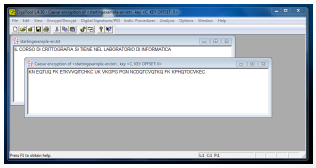
- Il Wired Equivalent Privacy è parte dello standard IEEE 802.11 (ratificato nel 1999) e in particolare è quella parte dello standard che specifica il protocollo utilizzato per rendere sicure le trasmissioni radio delle reti Wi-Fi.
- WEP è stato progettato per fornire una sicurezza comparabile a quelle delle normali LAN basate su cavo.
- WEP adesso viene considerato un sottoinsieme del più sicuro standard Wi-Fi Protected Access (WPA) rilasciato nel 2003 e facente parte dell'IEEE 802.11i.
- Il WEP viene ritenuto il minimo indispensabile per impedire a un utente casuale di accedere alla rete locale.

2003 - WPA (Wi-fi Protected Access)

- Wi-Fi Protected Access (WPA) è un protocollo per la sicurezza delle reti senza filo Wi-Fi creato nel 2003 per tamponare i problemi di scarsa sicurezza del precedente protocollo di sicurezza, il WEP.
- Studi sul WEP avevano individuato delle falle nella sicurezza talmente gravi da renderlo quasi inutile.
- Il WPA implementa parte del protocollo IEEE 802.11i e rappresenta un passaggio intermedio per il raggiungimento della piena sicurezza.
- Questa verrà raggiunta quando i dispositivi implementeranno completamente lo standard IEEE 802.11i.

CrypTool

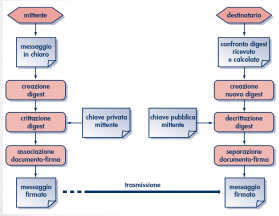
- CrypTool è un software libero e open source di e-learning per Microsoft Windows che illustra i concetti fondamentali della crittografia in via pratica.
- Scritto in C++, è disponibile in inglese, in tedesco, in spagnolo e in polacco.
- La versione scritta in Java, che prende il nome di JCrypTool, è disponibile da agosto 2007.
- http://www.cryptool.de/index.php/en



Firma digitale

- La **firma digitale** consente di certificare la provenienza di un documento
- È un modo per avere la certezza che un determinato messaggio o documento sia stato inviato da una specifica persona.
- Il sistema si basa su una crittazione a **chiavi asimmetriche**, dove ogni utente dispone di due chiavi, quella **pubblica** e quella **privata**.
- La chiave pubblica è tale in quanto non viene mantenuta segreta, ma anzi "pubblicata" dall' utente.
- La chiave privata, invece, non deve assolutamente essere divulgata, ed è lo strumento utilizzato dall'utente per firmare il documento o messaggio da spedire.

Uso della firma digitale



- Mittente:
  - Attraverso un algoritmo di hash crea un' impronta digitale del documento (*digest*), una stringa di dimensione fissa che riassume le informazioni presenti nel documento.
  - Il digest viene crittato utilizzando la chiave privata.
  - La firma viene allegata al documento.
- Destinatario:
  - Decodifica la firma del documento utilizzando la chiave pubblica del mittente.
  - Crea un nuovo digest sul documento in chiaro.
  - Se i due digest sono identici, significa che il documento è autentico.

Firma digitale e firma autografa

- Secondo l' ordinamento giuridico italiano, la firma digitale a crittografia asimmetrica è riconosciuta ed equiparata a tutti gli effetti alla firma autografa su carta.
- La qualifica della firma avviene attraverso un ente certificatore che si occupa di mantenerne un registro di chiavi pubbliche.
- Un esempio di ente certificatore sono le Poste Italiane.

Leggi sulla privacy

- La legge n. 675 dell' 8 gennaio 1997 è relativa al trattamento dei dati personali e alla **privacy**.
- L' intento è quello di disciplinare l' utilizzo dei dati personali che aziende e organizzazioni raccolgono.
- Lo scopo è quello di **evitare** l' utilizzo **improprio** o non autorizzato di queste informazioni, per esempio per ricerche di mercato o proposte commerciali.
- È previsto che l' interessato dia **esplicito consenso** all' azienda di mantenere i suoi dati, con la possibilità di consentire o meno l' utilizzo dei dati a fini diversi, come quelli pubblicitari.
- Il rispetto di questa legge è affidato a un organismo statale chiamato **Garante della Privacy**.

Hacker

- Gli **hacker** vengono normalmente identificati con "criminali informatici".
- Negli anni Sessanta gli hacker erano in realtà **esperti di computer** che raggiungevano obiettivi insperati grazie alla loro originalità e creatività. Persone con la passione dell' informatica e dei computer che consideravano prioritaria l' apertura di questi nuovi ritrovati della tecnica a tutti, indistintamente.
- Un **hacking** era una **soluzione geniale** a un problema ostico.
- L' hacker era un intelligente e acuto appassionato di tecnologie.
- Il termine ha quindi in origine un' accezione ben diversa da quella comunemente in uso.

Tipi di minacce

- **Ingegneria sociale**. Attacchi non tanto diretti ai sistemi informatici, quanto alle persone. Sono inganni perpetrati per profitto, o anche solo per scherzo.
  - Es.: *phishing (password fishing)* per "rubare" la password di un utente.
- **Sostituzione di persona**. L' hacker si impadronisce delle credenziali di un utente, per entrare nel sistema con le mentite spoglie di un altro utente (furto di "identità").
- **Exploit**. Sfruttamento di una vulnerabilità di un programma, sistema operativo o dispositivo di rete, al fine di ottenere dati riservati.
- **Transitive trust**. Acquisire il controllo di un server o di un' intera rete sfruttando l' accesso a una singola stazione di lavoro.
- **Minacce basate sui dati**. Troiani, virus e altri software malevoli.
- **DoS** (*Denial of Dervice*). Rendere inoperativo un determinato sistema.
  - Es.: si bombarda di richieste un server web, in modo da saturare le sue capacità di risposta; il server non sarà più in grado di rispondere neanche alle richieste dei normali utenti.

Virus *(da Wikipedia)*

- *Nell'ambito dell'informatica un virus è un software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente.*
- *I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.*
- *Come regola generale si assume che un virus possa **danneggiare** direttamente solo il **software** della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di raffreddamento.*

Minacce basate sui dati - Virus

- Un virus cerca di installarsi nel sistema dell' utente e di diffondersi direttamente verso altri file nel sistema.
- L' elemento attivo di un virus può causare danni di vario tipo, da semplici scherzi ad azioni distruttive.
- I virus per diffondersi si basano sull' apporto dell' utente. Se i file infetti non sono trasferiti, tramite dischi o posta elettronica, l' infezione non procede.

Malware

- *Nell'uso comune il termine virus viene frequentemente ed impropriamente usato come sinonimo di **malware**, indicando quindi di volta in volta anche categorie di "infestanti" diverse, come ad esempio worm, trojan o dialer.*
- *Si definisce **malware** un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi **malicious** e **software** e ha dunque il significato letterale di "**programma malvagio**"; in italiano è detto anche codice maligno.*

Minacce basate sui dati - Worm

- Un verme (worm) è molto simile a un virus, con la differenza fondamentale che il verme cerca di propagarsi senza l' apporto dell' utente.
- Il worm affida la propria diffusione solo a comunicazioni di rete iniziate in modo autonomo, per esempio utilizzando a supporto la posta elettronica.
- L' azione tipica intrapresa da questi fastidiosi programmi è quella di eseguire una scansione di altri computer per intercettare specifiche vulnerabilità.

Minacce basate sui dati - Trojan

- I troiani (trojan)derivano il proprio nome dal Cavallo di Troia della mitologia greca.
- Sono software che possono apparire normali, in realtà nascondono pezzi di codice come virus o spyware.
- I cavalli di troia possono nascondersi in tutti i tipi di software, dai giochi agli screen saver, oppure in software commerciali craccati.
- Possono avere diversi scopi, come la realizzazione di una backdoor sul sistema ospite.

Spyware – Scanner - Sniffer

- Uno **Spyware** si installa sul computer dell' ignaro utente fornendo un accesso in rete ai malintenzionati.
  - Sono chiamati anche *back door* (porta sul retro), e possono garantire un numero maggiore di accessi rispetto a quelli del normale utente.
  - Quando un computer è infettato da spyware ed è connesso in rete i malintenzionati possono spiare il contenuto dell' hard disk e addirittura eseguire operazioni sul computer.
- Uno **Scanner** è un software progettato per recuperare informazioni da computer accessibili via Internet sulla tipologia e versione del software che è in esecuzione sul computer stesso.
  - Ci sono una varietà di scanner diversi: alcuni semplicemente controllano la presenza di una macchina, altri verificano quali porte sono aperte, altri si accertano della presenza di vulnerabilità in particolari servizi, oppure dell' esistenza di spyware.
- Uno **Sniffer** è un programma che cattura le password e altre informazioni.
  - Gli analizzatori di rete(sniffer ethernet) sono programmi che possono vedere all' interno del traffico in transito su una rete.

Minacce basate sull' infrastruttura

- **Buffer overrun**
  - Viene fornito al software un input più lungo di quanto previsto.
  - È sfruttato per passare comandi al computer remoto quali, per esempio, di lettura del file di password del computer o di apertura di una determinata porta.
- **Heap overflows**.
  - È molto simile al buffer overrun, ma non si applica ai buffer per i dati di input quanto alle zone di memoria utilizzate dall' applicazione.
- In entrambe le tecniche lo scopo è quello di inserire piccoli programmi assembler (*shellcode*) che eseguono una shell (come **/bin/sh** su Unix o **command.com** su DOS e Windows) nella memoria del computer e di fare in modo che vengano eseguiti dal computer sotto attacco.

Antivirus

- Un antivirus è un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi (malware.
- Tecniche usate dagli antivirus:
  - **Monitoraggio**: prevenire un'infezione mediante il controllo di attività sospette (ad esempio, la richiesta di formattazione di un disco oppure l'accesso a zone privilegiate di memoria).
  - **Scanner**: confronto tra le firme memorizzate in un **database interno**, con quelle, eventualmente, contenute nei file infetti (importantissimo l' aggiornamento del database dei virus);
  - **Verifica dell'integrità**: calcolano l'hash dei file da confrontare successivamente coi nuovi valori risultanti da un nuovo calcolo per verificare che i file non abbiano subito modifiche nel frattempo.

firewall

- I **firewall** ("muro tagliafuoco") sono dispositivi hardware/software di difesa del perimetro di una rete di computer.
- La loro funzione è quella di isolare la rete interna da quella esterna, generalmente rappresentata da Internet.
- Filtrano la comunicazione tra rete esterna e interna, per limitare la comunicazione solo a messaggi che non rappresentino un rischio di sicurezza.
- I pacchetti di rete in transito sono monitorati, controllati e verificati per individuare messaggi potenzialmente maligni, o tentativi di connessione da parte di computer o sottoreti non autorizzate, oppure su porte non consentite.
- Possono essere di due tipi:
  - **completamente software**.
  - **hardware/software**. Sono in pratica computer su cui è in esecuzione un software di firewall, completamente dedicati allo scopo.
- Altre funzionalità dei firewall sono:
  - funzionalità di routing, che consente di interfacciare due reti diverse, come Internet e la rete locale;
  - filtro sui contenuti, come quelli necessari a limitare la visione di materiale per adulti.

SQL injection

- E' una tecnica dell'hacking mirata a colpire le applicazioni web che si appoggiano su un database di tipo SQL.
- Sfrutta l'inefficienza dei controlli sui dati ricevuti in input ed inserisce codice maligno all'interno di una query SQL.
- Le conseguenze prodotte sono imprevedibili per il programmatore: l'Sql Injection permette al malintenzionato di autenticarsi con ampi privilegi in aree protette del sito (ovviamente, anche senza essere in possesso delle credenziali d'accesso) e di visualizzare e/o alterare dati sensibili.

Esempio SqL injection

- login.html

```
<form action='login.php' method='post'>
   Username: <input type='text' name='user' />
   Password: <input type='password' name='pwd' />
   <input type='submit' value='Login' />
</form>
```

- login.php

```
<?php
$query = "SELECT * FROM users WHERE user='".$_POST['user']."' AND pwd='".$_POST['pwd']."'";
$sql = mysql_query($query,$db);
if(mysql_affected_rows($sql)>0)
{
//ok utente loggato
?>
```

- se l'utente immette come user **`jack`**
- e come password **`' OR user='jack`**
- La stringa SQL diventa

```
SELECT * FROM users WHERE user='jack' AND pwd='' OR user='jack'
```