

Lezione 07

Dott. Francesco De Angelis

francesco.deangelis@unicam.it

<http://francescodeangelis.org>



Scuola di Scienze e Tecnologie - Sezione di Informatica
Università di Camerino

Agenda

- L'informatica e la legge [cap. 25]
- Il lavoro e l'informatica [cap. 26]
- L'informatica come fatto sociale [cap. 27]



Informatica di base 5e

Dennis P. Curtin, Kim Foley, Kunal Sen, Cathleen Morin.
A cura di Agostino Marengo

Copyright © 2012 – The McGraw-Hill Companies



**NOTA: LE SLIDE NON RAPPRESENTANO UNA
ALTERNATIVA AL LIBRO DI TESTO
O ALLE LEZIONI DEL DOCENTE**

Capitolo 25

L'informatica e la legge

Protezione dei dati

- I messaggi di posta elettronica sono come delle cartoline, che possono essere lette da tutti.
- Che accadrebbe se tutti pensassero che i cittadini onesti usano solo cartoline per la loro posta?
- Fortunatamente tutti proteggono la maggior parte della loro posta chiudendola in una busta.
- Sarebbe giusto se tutti usassero abitualmente la crittografia per la loro posta elettronica.
- Privacy; D.L. 30/6/2003 n 156 (“Legge sulla privacy”).

Cosa vuol dire sicurezza informatica

Sicurezza "interna"

- Accesso sicuro ai propri dati, alle proprie informazioni.
- Copia delle informazioni importanti.
- Gestione di login, nickname e password personali.

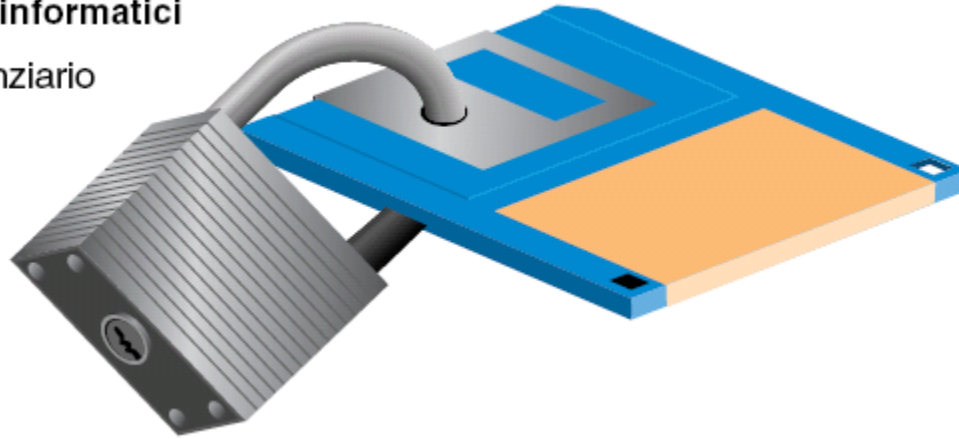
Sicurezza "esterna"

- Certezza sul trattamento dei dati sensibili.
- Difesa dagli attacchi da virus e altro malware.
- Non commettere reati inconsapevolmente.

Crimini e criminali informatici

Le motivazioni dei criminali informatici

- Tornaconto personale o finanziario
- Divertimento
- Vendetta
- Favore personale
- Sfida
- Incidente
- Vandalismo



Tipi di *crimine* informatico

- Furti e manipolazioni dei dati
- Accessi abusivi a informazioni
- Attacchi "Denial of Service"
- Violazioni del copyright

Tipi di *criminale* informatico

- Cracker
- Dipendenti delle aziende colpite
- Persone in genere non autorizzate a svolgere determinate operazioni

Virus, tecniche di attacco, malware

Tipi di virus

- Cavallo di Troia
- Worm
- Exploit (es. Backdoor)
- Hoax
- Macro Virus

Malware

- Dialer
- Spyware
- e tutti i virus...

Tecniche di attacco

- *Sniffing*
- *Spoofing*
- *Phishing* (con la collaborazione dell'utente...)

La crittografia

- La crittografia è l'**arte di progettare algoritmi** (o **cifrari**) per crittografare un messaggio rendendolo incomprensibile a tutti tranne al suo destinatario
- Il destinatario, con un algoritmo simile deve essere in grado di decodificarlo, attraverso un parametro segreto detto **chiave** (usato in precedenza anche dal mittente per la cifratura).

Tecniche di crittografia

- Crittografia a chiave singola (c. simmetrica)

La stessa chiave codifica e decodifica i messaggi.

- Crittografia a chiave pubblica

Una chiave pubblica e una privata cifrano e decifrano i messaggi, in modo che nemmeno il mittente può decifrare il proprio messaggio, una volta codificato.

- Firma digitale

Il destinatario chiede al mittente di apporre con la sua chiave privata una "firma digitale" al documento. Attraverso quella pubblica il destinatario può riconoscere senza ombra di dubbio il file del mittente come fatto da lui.

- Chiave di sessione

Il messaggio viene cifrato con una chiave singola - generata casualmente per quella sola trasmissione - e questa a sua volta cifrata con una chiave pubblica.

Algoritmo di crittografia

- Un algoritmo di crittografia riceve un testo da codificare (detto **testo in chiaro**) e lo trasforma, attraverso la chiave, in un testo cifrato apparentemente incomprensibile.
- La sicurezza di un sistema di crittografia risiede solo ed esclusivamente nella **segretezza della chiave** e non dell'algoritmo che è opportuno far conoscere alla pubblica analisi, in modo che se ne possano scoprire eventuali punti deboli in tempo.

Lunghezza della chiave

- La **lunghezza della chiave** utilizzata è uno dei fattori più importanti per la segretezza del testo:
 - evita infatti che possa essere decifrato per tentativi
- Provare tutte le possibili combinazioni di caratteri che potrebbero formare una chiave è un problema che gli analisti definiscono a **complessità computazionale esponenziale**:
 - basta aggiungere una sola lettera alla chiave per aumentare in modo vertiginoso il numero di possibili combinazioni che possono essere ottenute.

Il cifrato di Cesare

- Per comunicare con i suoi generali, Giulio Cesare sostituiva ad ogni lettera del messaggio un'altra lettera un certo numero di posizioni più avanti nell'alfabeto.
- Per l'esattezza utilizzava la **chiave "3"**, tutte le lettere venivano scalate di tre cifre: la A diventava D, la B diventava E, la C diventava F e così via.
- Con questo metodo la frase:

PROVA DI CIFRATURA

diventa

SURYD GL FLIUDWXUD

Crittografia a chiave segreta

- Tutti i sistemi di cifratura visti fino a questo punto sono detti **a chiave segreta** ed utilizzano la stessa chiave sia per cifrare che per decifrare.
- Le due parti devono riuscire in qualche modo a scambiarsi la chiave con la certezza che nessuno ne venga a conoscenza, un problema non indifferente.
- La soluzione a questo tipo di problema fu proposta nel 1975 da Whitfield Diffie e Martin Hellman, che ebbero un'intuizione che rivoluzionò il mondo della crittografia.

La crittografia a chiave pubblica: le chiavi asimmetriche

- 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.
- 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;
 - quella privata deve essere conosciuta solo da una persona.

La firma digitale

- La **firma digitale** viene da molti considerata uno dei migliori mezzi possibili per ridurre drasticamente i problemi di sicurezza relativi alla trasmissione di documenti per via telematica.
- Tale sistema permette di semplificare sia i rapporti tra **imprese e/o privati** che quelli tra **cittadini e pubblica amministrazione**.

Che cos'è la firma digitale?

La legge la definisce il risultato di una **procedura informatica – validazione** – che attraverso un procedimento crittografico a **chiavi asimmetriche**, permette di identificare il reale mittente di un documento informatico verificandone l'autenticità.

Messaggi a firma digitale

Come viene inviato un messaggio?

Tre diversi modi:

- il **mittente** in possesso della chiave pubblica del destinatario cifra con essa il messaggio; il **destinatario** attraverso la propria chiave privata può decifrarlo;
- è il **mittente** a rendere cifrato il messaggio con la propria chiave privata, in questo caso **chiunque** sia in possesso della chiave pubblica del mittente può decifrarlo (in questo modo viene assicurata la reale identità del mittente);
- il **mittente** cifra il proprio messaggio con la chiave pubblica del **destinatario** e con la **propria chiave privata**; il ricevente dovrà decifrare il testo sia con la propria chiave privata che con quella pubblica del mittente. In questo modo oltre alla segretezza del messaggio dovrebbe essere garantita anche l'autenticità della provenienza.

Il certificatore

Ma come essere sicuri che la chiave pubblica non sia stata contraffatta e provenga effettivamente dall'utente-titolare?

Per garantire trasparenza e sicurezza la legge ha creato la figura del **CERTIFICATORE**:

"il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna gli elenchi dei certificati sospesi e revocati"
(D.P.R. 513/97, art.1).

Capitolo 26

Il lavoro e l'informatica

Gli specialisti dell'informatica

- Operatori di computer
- Bibliotecari informatici
- Programmatori
- Sistemisti
- Responsabili dei sistemi informativi
- Addestratori
- Esperti di microcomputer
- Supporto tecnico
- Redattori di testi tecnici
- Consulenti
- Gestori di microcomputer
- Webmaster

Come aggiornarsi?

- Internet è la più ampia fonte di informazioni *su se stesso*.
- I gruppi d'utenza sono libere organizzazioni di utenti, e ne esistono per qualunque hardware o software prodotto.
- Le organizzazioni professionali hanno servizi esclusivi per i loro soci, ma sono in genere aperte alla consultazione pubblica e offrono informazioni preziose. Nel settore informatico:
 - *Educom*;
 - *Infoworld*;
 - *Computerworld*.

Prepararsi per tempo ai cambiamenti tecnologici

È importante ricordare che:

- maggiori conoscenze informatiche si hanno, più facile sarà *adattarsi ai cambiamenti* che inevitabilmente subiranno gli strumenti che usiamo;
- va bene *tenersi al corrente* dei prossimi arrivi sul mercato informatico, ma non serve correre freneticamente dietro alla tecnologia;
- il futuro del proprio lavoro va *immaginato*, e non subito.

Capitolo 27

L'informatica come fatto sociale

Ergonomia

L'ergonomia è la scienza che studia l'interazione tra uomo e macchina.

Alcuni consigli per affrontare il lavoro davanti al PC

- Illuminare l'ambiente meno rispetto alla luminosità dello schermo.
- Attenzione ai riflessi, alla posizione delle fonti di luce e agli oggetti o vestiti chiari.
- I caratteri devono essere ben nitidi rispetto allo sfondo.
- Sedia regolabile in altezza.
- Documenti da consultare alla stessa distanza dagli occhi che ha lo schermo.
- Una pausa raccomandata:
 - se il meno del 60% del tempo si fissa lo schermo = ¼ d'ora ogni due ore;
 - se oltre il 60% del tempo si fissa lo schermo = ¼ d'ora ogni ora.

Le questioni scottanti

- Il trattamento dei dati personali: utilità ed efficienza pubblica *contro* diritto privato alla privacy.
- Il supervisore elettronico: migliore gestione aziendale *contro* controllo dei dipendenti.
- La censura: difesa dei più vulnerabili *contro* controllo generalizzato della rete.
- *Privacy nelle comunicazioni*: controllo possibile per l'autorità contro garanzia di inviolabilità.
- *Digital divide*: l'accesso alle nuove tecnologie, possibile solo ai ricchi, aumenta il divario economico e sociale con i paesi poveri.



Windows o Linux?

- Windows tecnicamente nasce negli anni '80, prima che la rete sia diffusa al grande pubblico.
- Windows è fin dall'inizio venduto come un servizio fornito da un'azienda.
- Lo sviluppo di Windows è garantito, ed è praticamente obbligatorio seguirlo da parte dei suoi clienti.
- Windows ha bisogno di componenti aggiuntivi per difendersi dagli attacchi dalla rete.
- Linux nasce negli anni '90 grazie alla collaborazione spontanea di programmatori convocati in rete.
- Linux è distribuito gratuitamente e si affida a spontanee comunità di utenti che si mettono al servizio di altri.
- Le versioni di Linux progrediscono solo grazie a un lavoro non retribuito; le nuove non sostituiscono necessariamente le precedenti.
- Linux non conosce il problema dei virus.