Sicurezza e Privacy

2 Crediti Formativi (CFU)

Corso di Laurea in Economia Aziendale

A.A. 2022/2023
Introduzione al Web

Ing. Paola Lapadula
Università degli Studi della Basilicata

Sommario

- Malware
  - Antivirus
- Tipi di attacchi, norme di sicurezza e sistemi di protezione
- E-mail e sicurezza
- Privacy
  - La legge, Privacy Policy, Cookie
- Diritti di autore e licenze software

Introduzione

- Un sistema informatico è sicuro se vengono garantite le seguenti caratteristiche:
- Integrità
  - le informazioni memorizzate sono protette da modifiche non desiderate
- Confidenzialità
  - le informazioni memorizzate sono protette da letture non autorizzate
- Disponibilità
  - le informazioni memorizzate sono disponibili quando se ne verifica il bisogno

Introduzione

- 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"

Malware

- Esistono diverse tipologie di malware:
  - Virus: programmi che infettano una macchina ospite, si riproducono e si propagano
    - Il meccanismo usato consiste nell'annidarsi all'interno di un programma (file eseguibile), modificandone il comportamento
  - TROJAN-HORSE
    - programmi apparentemente innocui che aprono delle falle nei sistemi informatici
  - **Spyware: raccoglie informazioni sugli utenti**

Malware

- Altre tipologie
  - Worm (rallentano il sistema con operazioni inutili o dannose)
  - Backdoor (consentono un accesso non autorizzato al sistema su cui sono in esecuzione)
  - Wabbit (esauriscono le risorse del computer creando copie di sé stessi, in memoria o su disco, a grande velocità)

Malware

- Altre tipologie
  - Batch: non sono file pericolosi ma assicurarsi che la fonte da cui proviene sia attendibile
    - Esempio: esegua il comando di formattare il pc (o altre cose dannose)
  - Keylogger: registrano i dati immessi da tastiera o copia e incolla rendendo possibile il furto di password
  - …

In dettaglio

- Un virus generalmente effettua:
  - un'azione che tende a favorire la diffusione dello stesso virus su altri computer
  - azioni collaterali di mascheramento (ad esempio assumere il nome di file non sospetti presenti nel sistema)
  - l'azione dannosa vera e propria (dalla cancellazione di tutti i file alla comparsa improvvisa di un messaggio di qualche genere)

In dettaglio

- Il cavallo di Troia è un altro veicolo di azioni dannose
  - è un particolare tipo di programma che l'utente scarica da Internet o riceve via mail e manda in esecuzione "volontariamente" all'interno del proprio sistema
  - una volta completata l'installazione, il nostro sistema diventa vulnerabile ad attacchi futuri
  - Il trojan horse entra nel nostro sistema fingendosi innocuo per poi distruggere le nostre difese dall'interno

In dettaglio

- Lo spyware è un software che viene utilizzato per raccogliere informazioni dal sistema su cui viene installato e per trasmetterle ad un destinatario interessato
- Le informazioni carpite possono andare dalle abitudini di navigazione fino alle password e alle chiavi crittografiche di un utente

Antivirus

- Sono programmi scritti per rilevare e, se possibile, cancellare i virus
- Una volta installati controllano continuamente e automaticamente tutti i file e programmi che vengono eseguiti sul computer
- Ogni giorno nascono nuovi virus e per poterli identificare gli antivirus necessitano di aggiornamenti continui (scaricabili da Internet)

Tipi di attacchi

- Un sistema Informatico può essere attaccato in vari modi
- Vediamone alcuni:
  - Social Engineering
  - Intercettazione
  - Denial of Service

Social Engineering

- Per Social Engineering si intende lo studio del comportamento individuale di una persona al fine di carpire informazioni
- Un ingegnere sociale (social engineer) per definirsi tale deve saper fingere, sapere ingannare gli altri
- Un social engineer è molto bravo a nascondere la propria identità, fingendosi un'altra persona:
  - riesce a ricavare informazioni che non potrebbe mai ottenere con la sua identità reale

Social Engineering

- Per esempio
  - L'intruso chiama il Centro di Calcolo dell'Università: "Buongiorno, sono il prof. Tizio. Ho dimenticato la mia password, potete modificarla in paperino?"
  - La password viene modificata
  - L'intruso può ora accedere con la password da lui decisa
  - Una volta recuperata la password, l'intruso si può connettere al sistema e ogni sua azione (con le conseguenti responsabilità) verrà fatta risalire al reale proprietario della password

Intercettazione

- La password ed ogni altra informazione che transita per la rete può essere intercettata da appositi programmi (sniffer)
- Un intruso potrebbe installare sul vostro computer un programma (keylogger) invisibile che si occupa di memorizzare in un file tutto ciò che si digita sulla tastiera e quindi anche le vostre password

Denial of Service

- L'obiettivo dell'intruso è saturare le possibili connessioni che un server è in grado di gestire verso l'esterno, con connessioni fasulle
- In questo modo il server non sarà più in grado di soddisfare le richieste dei propri utenti e sarà di fatto NON funzionante
- Per effettuare un attacco del genere è di solito necessaria la collaborazione di molti intrusi

Norme di sicurezza

- Non eseguire programmi di cui non si conosce la provenienza
- Non aprire direttamente gli allegati di posta elettronica, anche se provenienti da conoscenti
- Avere molta cautela nello scambio di file attraverso supporti mobili

Sistemi di protezione

- Hanno il compito di prevenire e rilevare le intrusioni e di farvi fronte
  - Firewall
  - Crittografia
  - Proxy per un Internet filtrato

Firewall

Uno dei possibili servizi dei router

- È un insieme di componenti hardware e software posto tra due reti di calcolatori
  - tutto il traffico tra le due reti deve passare attraverso il firewall
  - solo ai messaggi autorizzati è permesso di oltrepassare il firewall
- Il Firewall ("muro di fuoco") è a tutti gli effetti un filtro intelligente in grado anche di accorgersi di un possibile attacco in corso e di avvisare chi di dovere

Crittografia

- Il principio di base della crittografia è la trasformazione sistematica degli elementi che compongono le informazioni
- la trasformazione viene fatta utilizzando un dato codice (chiave)
- solo chi è in possesso della chiave può ricostruire l'informazione corretta
- in caso contrario l'informazione risulta illeggibile

Crittografia

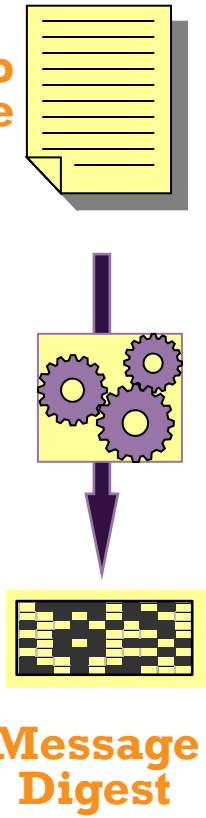
- Tipi di cifratura
  - Cifratura simmetrica: si usa la stessa chiave per cifrare e decifrare
  - Cifratura asimmetrica: si usa una chiave pubblica e una chiave privata
    - Tale tecnica è alla base dei messaggi segreti e della firma digitale >>
- Messaggi segreti
  - Se A vuole inviare un messaggio segreto a B, usa la chiave pubblica di B. Solo B lo può leggere con la sua chiave privata

Firma digitale: I suoi requisiti

- Integrità
  - Il contenuto del messaggio non deve essere alterato (verifica del digest >>)
- Autenticità
  - con un documento firmato digitalmente si può essere certi dell' identità del sottoscrittore
- Non ripudio
  - il documento informatico sottoscritto con firma digitale ha piena validità legale e non può essere ripudiato dal sottoscrittore

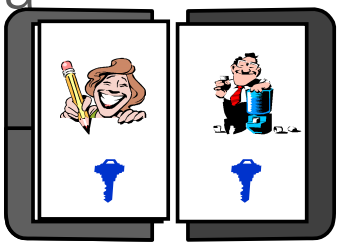
Impronta (digest)

- L'impronta dei dati (digest) è una sorta di "sintesi" dei dati generata mediante appositi algoritmi, detti algoritmi di hash
- La funzione di hash è una trasformazione dei dati di lunghezza arbitraria (un *messaggio*) in una stringa di dimensione fissa chiamata message digest:
  - dati due messaggi diversi (anche di un solo bit), la probabilità di ottenere lo stesso digest è estremamente bassa
  - la funzione è unidirezionale (non è possibile risalire al messaggio che lo ha generato)

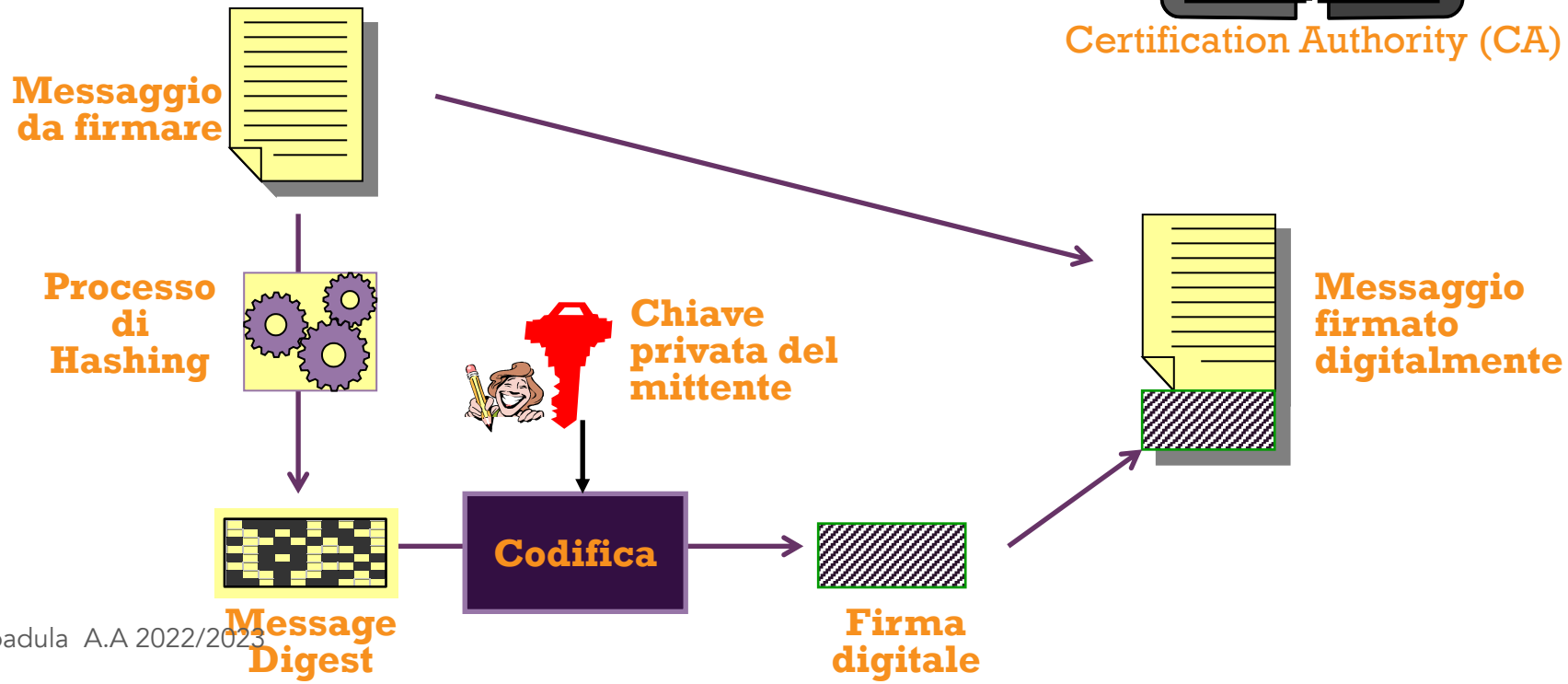


Impronta (digest)

- Il message digest è quindi crittografato con la chiave privata del mittente e aggiunto al messaggio originale (in chiaro)



Certification Authority (CA)

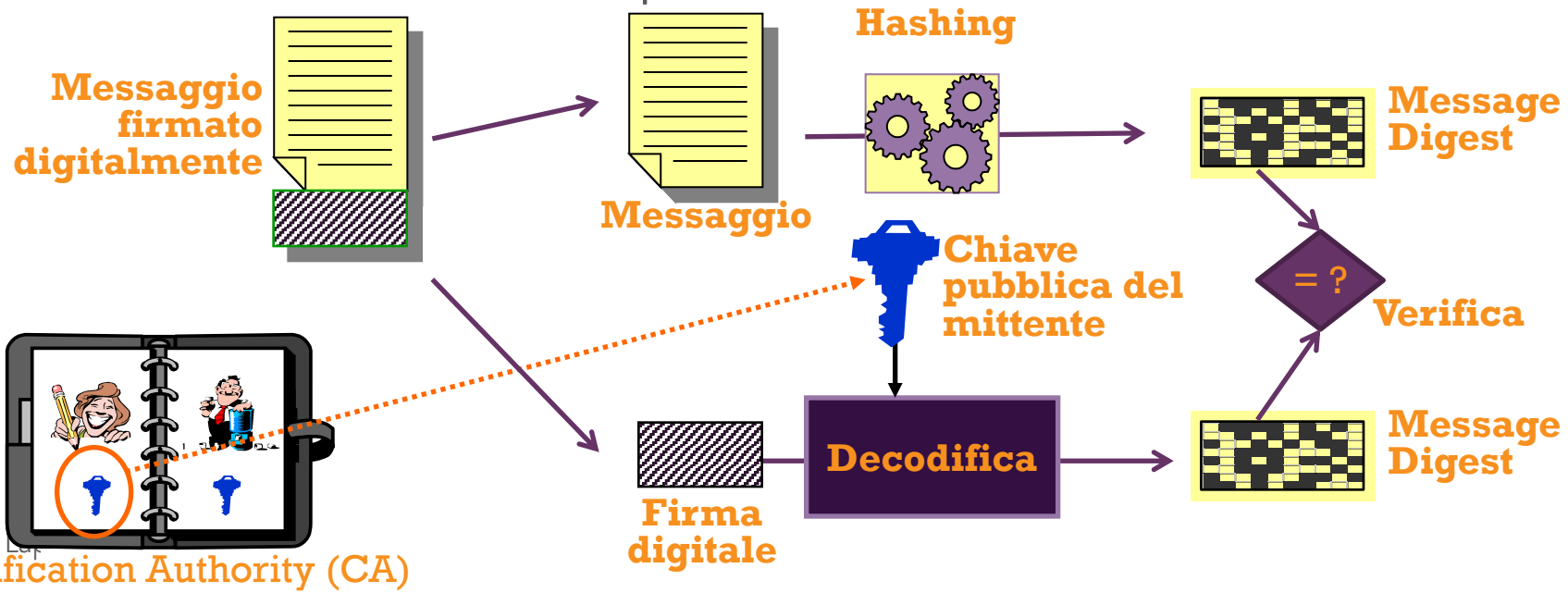


Impronta (digest)

- Per verificare che il messaggio ricevuto non è stato modificato durante la trasmissione e che il mittente è effettivamente chi dice di essere, il destinatario compie le seguenti operazioni:
  - usando lo stesso algoritmo di hashing, crea un message digest del documento ricevuto
  - usando la chiave pubblica del mittente (prelevata dalla Certification Authority (CA)), decodifica la firma digitale del mittente per ottenere il message digest del documento originale
    - la CA garantisce la titolarità della chiave pubblica mediante certificati

Impronta (digest)

- confronta i due message digest per verificare se essi coincidono: se i due message digest risultano diversi significa che il messaggio è stato modificato oppure il mittente non è chi dice di essere (ha firmato con una chiave privata diversa)



Firma digitale vs PEC

- La PEC può essere utilizzata per inviare i documenti e sostituisce i mezzi tradizionali quali la raccomandata A/R, il fax ed il corriere
- La firma digitale, viceversa, rappresenta il mezzo elettronico per apporre la propria firma ad un documento elettronico o ad una mail
  - In altre parole la firma digitale è il sostituto elettronico della firma autografa in calce ai documenti cartacei

Firma digitale vs PEC

- La PEC assicura che un messaggio arrivi a destinazione inalterato ed integro e garantisce l'identità del mittente
- con la firma digitale il mittente appone il proprio autografo al contenuto della mail e agli eventuali allegati, ad ulteriore garanzia della propria identità

Firma digitale vs PEC

- Chiaramente i due strumenti non sono in contrapposizione ma possono essere utilizzati insieme
- Per il funzionamento della PEC non è necessario alcun device, mentre per l'utilizzo della firma digitale è necessario dotarsi di un lettore di smartcard o di un token USB tra i molti disponibili in commercio

Proxy

- Si pone come intermediario tra client e server
- Tutto il traffico passa attraverso il proxy che diventa un collo di bottiglia se è inefficiente,
  - mentre può migliorare la navigazione se effettua il caching delle pagine web
- Può anche servire per obbligare tutta la rete a un servizio di filtraggio dei contenuti
- È possibile registrare la navigazione degli utenti a fini statistici o di controllo

Password: le linee guida

- Usare password
  - lunghe
  - non predicibili
  - non basate su nomi, date di nascita, ecc.
- Password diverse per servizi diversi
- Cambiare le password frequentemente
- Non scrivere le password su un foglietto attaccato al monitor (!)
- Non condividere password fra più utenti

Email e Sicurezza

- La posta elettronica è uno dei servizi di rete più diffusi. Per questo è uno di quelli con cui la gente mette più facilmente a repentaglio la propria sicurezza
- Due problemi sono:
  - L'esistenza di molti modi per mandare le mail con un mittente e/o un destinatario falso
  - Gli allegati delle e-mail hanno dimostrato di essere ideali per veicolare virus, anche perché l'e-mail è spesso percepita come qualcosa di personale, a cui si può dare fiducia

Spam e Phishing

- Lo spam e il phishing sono due grossi problemi che attanagliano il servizio di posta elettronica
- Lo spam è un insieme di e-mail indesiderate che vengono generate automaticamente e inviate a numerosi indirizzi di solito per pubblicità o truffa
- La peggiore idea che si possa avere riguardo allo spam è … rispondere
- Rispondendo ad una mail di spam si ha la garanzia che il proprio indirizzo e-mail venga inserito in liste di indirizzi noti, con conseguente copioso aumento dello spam stesso

Spam e Phishing

- Il phishing è una tecnica utilizzata per ottenere l'accesso ad informazioni personali usando l'ingegneria sociale
- Grazie a messaggi fatti ad hoc l'utente è portato a rivelare dati personali
- Per ovviare al phishing è necessaria soprattutto l'attenzione dell'utente, anche se molti programmi di posta e browser moderni hanno filtri anti-phishing,
  - Ossia sono in grado di rilevare e rimuovere in automatico le e-mail truffaldine

Esempio di Phishing

Gentile Cliente,
Ci è arrivata una segnalazione di accredito di Euro 129 ricevuta dal UFFICIO POSTALE di BRANDIZZO. L'accredito e stato temporaneamente bloccato a causa dell'incongruenza dei suoi dati, potrà ora verificare i suoi dati e successivamente sarà accreditato l'accredito ricevuto:
Acceda al servizio accrediti online di Poste.it e verifichi le sue operazioni »
*(*http://www.r-f-c.org/images/src.html *)*

Cordiali saluti,
Poste Italiane

TELEFONO
Numero gratuito 803.160 (dal lunedì al sabato dalle ore 8 alle ore 20).

Ti preghiamo di non inviare alcuna risposta a questo messaggio e-mail, poiché non verrà presa in considerazione.

Esempio di Phishing

- Il collegamento, arrivato con l'e-mail conduce ad un sito Web fasullo che assomiglia a quello vero.
- Una volta giunto a quel sito, sarà chiesto di rivelare informazioni personali quali Login, Password e codice PIN.
- Tali dati, naturalmente, vengono memorizzati su quel server fasullo e usati successivamente da truffatori per attacchi di phishing con i quali si appropriano della identità del malcapitato e prosciugano il suo conto

Privacy

- Inizialmente riferito alla sfera della vita privata, negli ultimi decenni ha subito un'evoluzione estensiva, arrivando a indicare il diritto al controllo sui propri dati personali
  - Privacy nelle fotografie
  - Privacy dei cellulari
  - Privacy del telemarketing
- *"È il diritto alla riservatezza delle informazioni personali e della propria vita privata".*

  (giurista statunitense Louis Brandeis)

Privacy

- La riservatezza dei dati personali nel settore dell'informazione è ancora oggi molto complessa
- Il settore dell'informazione è un settore interessato da una continua evoluzione e da una rilevante importanza sociale
  - Esempio: tutte le informazioni sottoforma di dati personali, abitudini e consumi dei clienti, che posseggono le aziende

Legge sulla privacy 675/1996

- Legge madre sulla protezione dei dati personali:
  - garantire "che il trattamento dei dati personali si svolga nel rispetto dei diritti, delle libertà fondamentali, nonché della dignità delle persone fisiche, con particolare riferimento alla riservatezza e all'identità personale". (art. 1 comma 1)
- Per il trattamento (raccolta, conservazione, utilizzazione) dei dati personali deve essere ottenuto il consenso esplicito dell'interessato
- Norme restrittive sui dati sensibili (abitudini sessuali, salute, opinioni politiche e religiose)

Legge sulla privacy 675/1996

- Con il tempo a tale norma si sono affiancate ulteriori diverse leggi, riguardanti singoli specifici aspetti del trattamento dei dati
- La complessità della situazione normativa venutasi a creare in seguito all'emanazione di norme integrative ha reso indispensabile provvedere al rilascio di un Testo Unico:
  - il Decreto legislativo 30 giugno 2003, n. 196, che ha riordinato la normativa, abrogando la L. n. 675/1996

D. lgs. N. 196 del 2003

- Entrato in vigore il 1° gennaio 2004:
  - Le finalità del d. lgs. 196/03 consistono nel riconoscimento del diritto del singolo sui propri dati personali e, conseguentemente, nella disciplina delle diverse operazioni di gestione (tecnicamente "trattamento") dei dati, riguardanti la raccolta, l'elaborazione, il raffronto, la cancellazione, la modificazione, la comunicazione o la diffusione degli stessi
- Lo scopo della legge non è quello di impedire il trattamento dei dati, ma di evitare che questo avvenga contro la volontà dell'avente diritto, ovvero secondo modalità pregiudizievoli

Dal D.lgs 196/2003 al Reg. 2016/679/UE: GDPR

- Consenso
- Interesse legittimo prevalente di un titolare o di un terzo - estensione del principio di "responsabilizzazione"
- Informativa
- Diritto di Accesso ai dati

Fonte https://www.cyberlaws.it/2018/gdpr-differenze-2016-679-ue-dlgs-196-2003/

Privacy e Web

- Come possiamo essere sicuri che i nostri dati personali non vengano usati impropriamente?
- Quando si visita un sito, il Web server conosce molte cose:
  - chi è il vostro Service Provider
  - quale browser e sistema operativo possedete
  - quali pagine visitate
  - il vostro indirizzo IP
- Ma non il vostro nome, cognome, e-mail … a meno che non siano esplicitamente richiesti

Privacy policy

- Se il sito raccoglie informazioni personali dovrebbe avere una politica di privacy dichiarata esplicitamente
- Questa dovrebbe dichiarare
  - quali dati vengono raccolti
  - come verranno trattati
  - per quale scopo
  - se verranno utilizzati da altri
  - per quanto tempo saranno mantenuti
  - se sono utilizzati cookie >>

Cookie

- Che cos'è un cookie?
  - è un frammento di informazione che il server memorizza sul disco del client (in un piccolo file di testo) per poterlo identificare
- quando si visita di nuovo quel sito, il cookie viene rimandato indietro in automatico dal vostro browser
- il tutto in maniera completamente invisibile

Cookie

- È pericoloso?
  - Assolutamente no.
  - È un semplice file di testo che permette al Server di “ricordarsi” di voi
- Esempio
  - Firefox -> Cookies
  - C:\Documents and Settings\[nomePC]\Cookies

Privacy e Cookie

- Possono i cookie costituire una violazione della privacy?
  - Ci sono casi di abuso dell'informazione raccolta con i cookie e di cause per violazione della privacy
- I cookie rispettano la legge sulla privacy?
  - Tipicamente no in quanto manca l'assenso informato

Copyright

- Il software è equiparato alle opere letterarie e artistiche e come tale, protetto dal copyright
- È punibili con pene pecuniarie e detenzione chi:
  - riproduce, detiene, distribuisce, vende, loca software non autorizzato

Classificazione Licenze Software

- Classificazione del software in base alla licenza:
  - Open Source, viene fornito il codice sorgente, l'utente può copiarlo, modificarlo e re-distrubuirlo
  - Pubblico dominio, software fornito senza copyright, l'utente può copiarlo e distribuirlo
  - …

Classificazione Licenze Software

- …
  - Freeware, software fornito gratuitamente, gli sviluppatori mantengono tutti i diritti
  - Shareware, software coperto da copyright, distribuito dietro piccola somma
  - Software con licenza d'uso, software coperto da copyright, distribuito dietro somma una tantum o canone periodico

Il diritto d'autore e il Web

- Legge n. 248/2000 da Diritto d'autore sul web:
  - Su Internet tutto è tutelato da copyright
  - Ogni opera creativa è automaticamente protetta da copyright
  - Copiare i testi è scorretto, disonesto, ma soprattutto è un reato
  - L'indicazione del copyright, completa di nome dell'autore e della data, rafforza ed esplicita meglio la protezione del testo, ma anche se non c'è, non si può copiare nulla

Legge sul diritto d'autore: suggerimenti

- Se volete riprodurre un testo, chiedete sempre il permesso all'autore
- Se tenete particolarmente al controllo dei vostri testi, dedicate una pagina del sito al copyright e scrivete chiaramente i termini e i limiti della riproduzione

Legge sul diritto d'autore: suggerimenti

- Si possono riprodurre dei passaggi, citando autore e fonte ma non per scopo commerciale
- Se vi accorgete di essere stati copiati, salvate il "corpo del reato", scrivete subito, invitate ad un accordo o a togliere la pagina incriminata

P2P: Decreto Urbani

- Il 02/03/2004 viene approvato il "decreto Urbani"
- Finanzia il cinema e introduce ulteriori misure contro la pirateria e la condivisione peer-to-peer di film
  - sanzioni per avere scaricato un film
    - ad uso personale: 1.500 euro
    - a scopo commerciale: dai 2.500 ai 15.000 euro, reclusione dai 6 mesi a 3 anni

Da decreto a legge

- Il decreto è stato convertito in Legge 22 maggio 2004, n. 128
  - con la promessa di modifiche in un futuro prossimo
  - con inasprimenti rispetto al decreto
  - non solo film, anche musica e programmi …
  - "fini di lucro" diventa "per trarne profitto"
- Le modifiche non sono arrivate …

Sommario

- Malware
  - Antivirus, tipi di attacchi, norme di sicurezza e sistemi di protezione
- E-mail e sicurezza
- Privacy
  - La legge, Privacy Policy, Cookie
- Diritti di autore e licenze software

- Ringraziamenti
  - Parte del materiale di questa lezione è stato sviluppato a partire dalle lezioni della Dott.ssa Vicari e della Dott.ssa Irina Coviello

Termini della Licenza

- This work is licensed under the Creative Commons Attribution-ShareAlike License. To view a copy of this license, visit http://creativecommons.org/licenses/by-sa/1.0/ or send a letter to Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.
- Questo lavoro viene concesso in uso secondo i termini della licenza "Attribution-ShareAlike" di Creative Commons. Per ottenere una copia della licenza, è possibile visitare http://creativecommons.org/licenses/by-sa/1.0/ oppure inviare una lettera all'indirizzo Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.