Il problema della sicurezza nel Commercio Elettronico

Moreno Marzolla
Dipartimento di Informatica
Università Ca' Foscari di Venezia
marzolla@dsi.unive.it
http://www.dsi.unive.it/~marzolla

Introduzione / 1

- Il 3 novembre 1988 il 10% dei calcolatori connessi alla rete Internet furono infestati da un "parassita" (*worm*)
  - Un numero elevato di programmi che assorbivano tutte le risorse del calcolatore infetto rendendolo di fatto inutilizzabile
- Il programma incriminato era stato scritto da uno studente, e si propagava da un computer all'altro sfruttando una falla del programma per l'inoltro della posta elettronica sendmail

Introduzione / 2

- Temendo di essere contagiati, altri siti decisero di scollegare i propri calcolatori dalla rete
- Il fermo durò fino a che la natura del "contagio" fu chiarita e il programma sendmail riparato
- I costi del fermo sono difficili da quantificare
  - Si parla di 24 milioni di dollari per il fermo delle macchine
  - Più 40 milioni di dollari per far ripartire i sistemi infetti e riparare il programma sendmail

La posta elettronica

- E' chiaramente uno degli strumenti più utilizzati su Internet, ma presenta molti porblemi
  - **Integrità**: Se scrivete un messaggio di posta elettronica per effettuare un ordine, siete sicuri che qualcuno non possa intercettare il messaggio e alterarlo prima dell'arrivo al fornitore?
  - **Privatezza**: Se il messaggio contiene informazioni confidenziali (il numero della vostra carta di credito) siete sicuri che nessuno lo possa leggere?
  - **Identificazione**: Siete sicuri che il destinatario del vostro messaggio sia chi dice di essere, e non un estraneo che ha preso il suo posto? Il destinatario è sicuro che il mittente sia chi dice di essere?

La posta elettronica

- Non molti ci pensano, ma la posta elettronica che tutti noi utilizziamo non garantisce nessuna delle proprietà precedenti
  - E' come scrivere su un foglio il nome del destinatario e il testo del messaggio, dare il foglio in mano ad un estraneo di cui non sappiamo assolutamente nulla e dirgli “fai avere questo messaggio al destinatario”
    - Il foglio è il messaggio di e-mail. La posta elettronica viaggia “in chiaro” sulla rete, non dentro una busta come la corrispondenza tradizionale
    - L'estraneo è qualunque dei router intermedi che instradano il nostro messaggio al destinatario. Ricordiamoci come funziona la rete Internet

La sicurezza e l'ECommerce

- Chiaramente nessuno sarebbe disposto a fare affari senza godere di alcuna sicurezza
  - Sia a tutela del compratore che del venditore
- Non è una sorpresa che il campo della sicurezza informatica sia uno dei più attivi negli ultimi anni
- La sicurezza è inevitabilmente un compromesso
  - *“Il PC più sicuro è quello spento, scollegato dalla rete Internet e chiuso a chiave in una stanza”*
  - Ovviamente un tale PC non è di molto uso
  - D'altra parte, non esiste un sistema *totalmente* sicuro

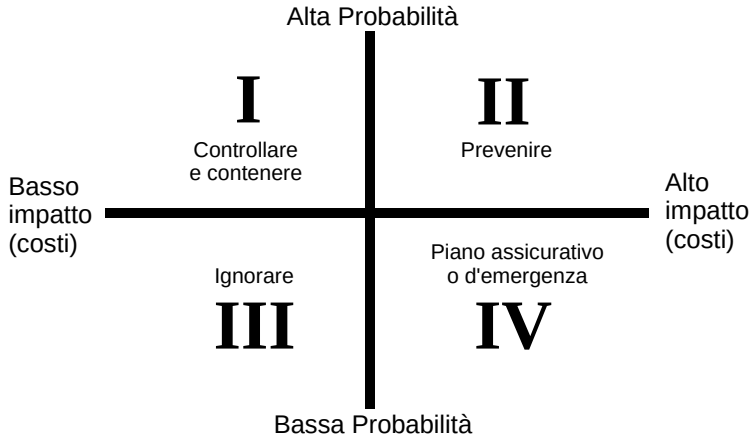
La Sicurezza Informatica

- La sicurezza informatica è la protezione delle risorse dall'accesso, utilizzo, alterazione o distruzione non autorizzati
- Due tipi di sicurezza
  - Fisica: protezione dei dispositivi fisici tramite allarmi, antifurto, porte ignifughe, casseforti...
  - Logica: protezione delle informazioni tramite risorse non fisiche (crittografia, firma elettronica...)

Minaccia

- Ogni azione o oggetto che costituisce un pericolo per una risorsa informatica è detta *minaccia*
- Le procedure fisiche e logiche per riconoscere, ridurre o eliminare una minaccia sono dette *contromisure*
  - Le contromisure variano in base all'importanza della risorsa a rischio
- Minacce poco rischiose possono essere ignorate quando il costo per proteggersi dal pericolo supera il valore di ciò che si deve proteggere

Modello di gestione dei rischi



Sicurezza informatica: classificazione

- Segretezza
  - Impedire la divulgazione non autorizzata di dati e garanzia di autenticità della fonte
  - Es: Notizie riservate che diventano di dominio pubblico, numeri di carta di credito in vendita su Internet...
- Integrità
  - Impedire le modifiche non autorizzate ai dati
  - Es: Manipolazioni del contenute delle email,
- Disponibilità
  - Impedire ritardi nella diffusione dei dati o la prevenzione della indisponibilità (rimozione dei dati)
  - Es: Attacchi *Denial of Service* (DOS)

Sicurezza informatica: classificazione

- Non repudiabilità
  - Impedire che la controparte possa negare una sua azione (firma elettronica)
  - Es: impedire che un cliente che ha inviato l'ordine possa in futuro negare di averlo mai fatto e rifiutarsi di pagare

Politiche di gestione della sicurezza

- E' un documento scritto che descrive
  - Quali risorse devono essere protette
  - Perché devono essere protette
  - Quali comportamenti sono accettabili e quali no
- Si deve occupare di
  - Sicurezza fisica
  - Sicurezza della rete
  - Autorizzazioni all'accesso
  - Protezione da virus e simili
  - *Disaster Recovery* (politiche per recuperare i dati a seguito di disastri quali rotture del sistema o cancellazioni accidentali o volontarie)

Pericoli per i clienti

- Gli utenti del WEB usano il proprio browser per navigare e accedere ai siti. Che pericoli corrono?
- Contenuti attivi
  - Sono programmi incorporati nelle pagine WEB
    - Controlli ActiveX, JavaScript, VBScript...
  - Possono essere usati per mostrare oggetti in movimento, scaricare file audio, effettuare calcoli su pagine WEB...
  - Sono molto usati dagli sviluppatori perché permettono di fare cose che con HTML da solo non risultano possibili
  - Consentono di far eseguire alcune computazioni sul computer dell'utente anziché sul server WEB

Contenuti attivi

- Possono anche essere nascosti sotto forma di istruzioni eseguibili contenuti in file binari
  - Certi tipi di immagini, formati o altri documenti di cui il browser effettua automaticamente l'anteprima a video
- I contenuti attivi sono potenzialmente molto pericolosi, per due ragioni
  - Vengono eseguiti di solito in modo totalmente trasparente all'utente
  - Essendo programmi eseguibili, in teoria non ci sono limiti a quello che possono fare, incluso ogni genere di danno

Java, applet Java e JavaScript

- Java è un linguaggio di programmazione inventato da Sun Microsystems
  - Originariamente nato per essere usato in prodotti "*embedded*" (elettrodomestici, dispositivi industriali...)
- Le applet Java sono applicazioni scritte in linguaggio Java che possono venire trasferite dai server WEB ai browser degli utenti assieme alle pagine che questi ultimi trasferiscono

Come funziona una applet Java

- Vediamo un esempio tratto da http://java.sun.com/applets/other/BouncingHeads/index.html

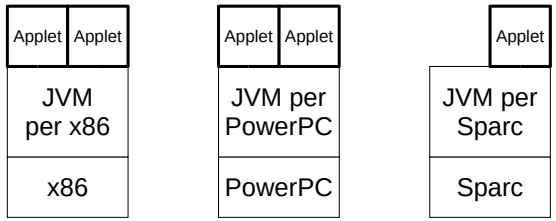
```
<html>
<head>
<title>Bouncing Heads</title>
</head>
<body>
<h1>Bouncing Heads</h1>
<hr>
<applet codebase="classes" code="BounceItem" width=500 height=300>
alt="Your browser understands the &lt;APPLET&gt; tag but isn't running the
applet, for some reason."
Your browser is completely ignoring the &lt;APPLET&gt; tag!
</applet>
<hr>
<a href="src/BounceItem.java">The source</a>.
</body>
</html>
```

Viene caricato ed eseguito il programma *BounceItem*

Caratteristiche di Java

- I programmi Java vengono compilati in istruzioni di basso livello
- Esiste un programma chiamato Java Virtual Machine, che funziona sul vostro PC ed esegue le istruzioni di basso livello
  - Esistono tante versioni della Java Virtual Machine, ciascuna funziona su un diverso microprocessore
  - PC, Mac, Sparc, Alpha, PowerPC...
- In questo modo la stessa applet Java funziona su tutti i calcolatori per i quali esiste una Java Virtual Machine

JVM



Sicurezza nelle applet Java

- Quando le applet giungono nel browser, vengono mandate in esecuzione in un ambiente “sicuro” (*Java Sandbox*)
  - Le azioni che le applet possono eseguire sono limitate
  - Quindi non possono causare danni
- Solo alle applet “certificate” possono essere concessi maggiori privilegi
  - Il certificato assicura che l'applet sia stata prodotta da un certo autore o compagnia
  - Se l'utente ha fiducia di chi ha prodotto l'applet, è ragionevole che possa concedere ad essa tutti i privilegi

JavaScript

- JavaScript è stato sviluppato da Netscape per consentire agli sviluppatori di pagine WEB di inserire dei contenuti attivi
- E' supportato dai browser più comuni
- Condivide molte delle caratteristiche di Java
  - E molte delle caratteristiche negative
  - Anche con JavaScript è possibile portare dei seri attacchi alla privacy o sottrarre dati sensibili dal PC dell'utente ignaro

ActiveX

- ActiveX è disponibile solo su calcolatori che utilizzano il SO Windows e solo su browser che li supportano
- Gli sviluppatori possono scrivere programmi utilizzando un qualsiasi linguaggio di programmazione
  - C, C++, Java, Visual Basic...
- I programmi vengono “impacchettati” in un controllo ActiveX e lo inseriscono in una pagina WEB
- Il controllo ActiveX viene trasferito sul PC dell'utente e il suo contenuto eseguito

Sicurezza dei controlli ActiveX

- Il problema è che, a differenza di Java, i controlli ActiveX una volta scaricati vengono eseguiti come qualsiasi altro programma
  - Hanno pieno accesso a tutte le risorse del sistema
  - Possono compiere qualsiasi operazione su tali risorse
  - Un controllo ActiveX nocivo potrebbe addirittura formattare l'hard disk o spegnere il vostro PC
- Per questa ragione possono generare violazioni di segretezza, integrità e disponibilità
  - Vedremo in seguito come proteggersi

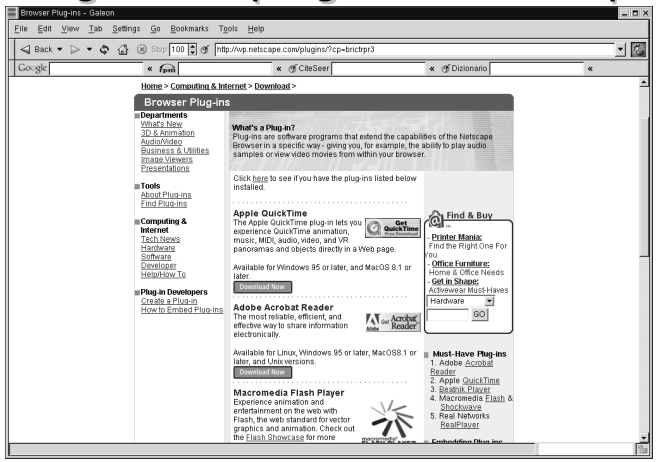
Immagini, plug-in e allegati di Email

- Certi tipi di file possono contenere (direttamente o indirettamente) dei programmi eseguibili
  - Direttamente: programmi che vengono eseguiti
  - Indirettamente: istruzioni che vengono passate al programma che visualizza quel tipo di file
- Gli allegati di Email sono un problema tristemente famoso
  - Gli allegati consentono di inviare informazioni non testuali in un sistema (la posta elettronica) che gestisce solo testo
  - Quando ricevono un allegato, i programmi di posta elettronica di solito ne mostrano l'anteprima...
  - ...ossia, eseguono l'applicazione che ha creato l'allegato

Problema con gli allegati

- Aprire un documento Word, di per sé, non è un problema per la sicurezza
- Il problema è che i documenti Word (o Excel o di altri tipi) possono contenere delle *macro*
  - Una macro altro non è che una sequenza di comandi, cioè un vero e proprio programma
- I linguaggi per scrivere macro (di solito VBscript) sono sufficientemente potenti e versatili che *qualunque* cosa si può fare tramite una macro
  - Compreso scrivere virus...
  - Molti virus basati su macro Word o Excel sono in circolazione

Pagine dei plugins di Netscape



La sicurezza del canale di comunicazione

- Internet non è nata con l'idea di garantire la sicurezza dei canali
  - Internet è originata dalla rete militare ARPANET
  - Lo scopo di ARPANET era di fornire percorsi diversi per comunicare, in modo da resistere ad attacchi
- I pacchetti viaggiano lungo percorsi apparentemente “casuali”
  - Non è possibile decidere a priori il tragitto
  - Non è possibile garantire che nessuno dei nodi attraversati sia ostile
  - Non è possibile garantire che nessuno dei nodi attraversati legga i messaggi in transito

Segretezza e privacy

- Segretezza
  - Evitare di divulgare una informazione
  - Può essere garantita con mezzi tecnici (crittografia principalmente)
- Privacy
  - Diritto individuale di impedire che certe informazioni vengano divulgati
  - Spesso i mezzi tecnici non bastano. Deve intervenire una tutela legislativa

Segretezza e privacy nella posta elettronica

- Segretezza
  - Si ottiene cifrando il testo del messaggio in modo tale che solo il destinatario autorizzato è in grado di decifrarlo
- Privacy
  - Impedire che il datore di lavoro possa leggere la mail dei dipendenti
  - Chi è il proprietario della mail? L'azienda o il dipendente che l'ha inviata?

Segretezza nel commercio elettronico

- L'aspetto più importante nell'ECommerce è la segretezza
  - Impedire che terze parti possano intercettare il contenuto delle transazioni (nomi, numeri di carta di credito, preferenze personali...)
  - Un furto di dati può teoricamente avvenire ogni volta che si compila e spedisce un form via Internet
  - I dati del form viaggiano “in chiaro” dal browser di chi li compila fino al sito WEB che li riceve. Ogni nodo intermedio può in teoria intercettare e/o alterare i dati

Uno scenario possibile / 2

- Vi collegate ad un sito, www.compratutto.com, ed effettuate degli acquisti compilando un form
- Il sito potrebbe accodare i dati del form nell'indirizzo della pagina a cui vanno spediti
  - Es. http://www.compratutto.com/invia.php?nome=Mario&cognome=Rossi&numerocc=123456789

Uno scenario possibile / 2

- A questo punto vi collegate ad un altro sito, www.altrosito.it
- Ad ogni nuova pagina cui accedete, il browser comunica anche l'indirizzo WEB da cui provenite
  - All'insaputa dell'utente!
  - Però questo è il comportamento definito nello standard del protocollo HTTP
- Quindi, il gestore di www.altrosito.it sa che voi provenite da:

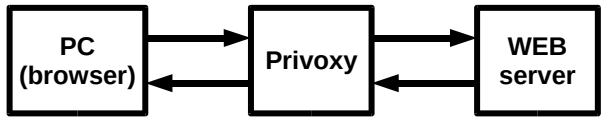
  http://www.compratutto.com/invia.php?nome=Mario&cognome=Rossi&numerocc=123456789

Uno scenario possibile / 3

- (vedi esempio pratico di lettura del referer)

Soluzioni possibili www.privoxy.org

- privoxy è un programma che potete installare sul vostro PC
  - Può eliminare dalle richieste le informazioni personali
  - E' in grado di filtrare le immagini che corrispondono a banner pubblicitari che non volete vengano mostrati



Minacce all'integrità

- Si verifica quando un soggetto non autorizzato può alterare le informazioni
- Integrità e segretezza non sono la stessa cosa!
  - Posso modificare un messaggio senza necessariamente doverne conoscere il contenuto
  - Es: Supponiamo di sapere che il messaggio cifrato XSHDG 9087 è l'ordine di un prodotto di cui la prima parola è il codice e la seconda la quantità
  - Se lo modifico a casaccio, ad esempio JIUYR 1092, magari corrisponde all'ordine di un'altra quantità di un altro prodotto
  - Può essere sufficiente se voglio fare un dispetto ad un concorrente...

Minacce alla disponibilità

- Due tipi di minacce:
  - Ritardo di servizio (delay threat)
  - Interruzione di servizio (denial threat)
- La disponibilità è importante!
  - Un servizio troppo lento non viene usato da nessuno
- Denial of Service Attack
  - “Bombardare” un sito web di richieste in modo da rallentarlo fino a renderlo inutilizzabile

In rete, nessuno sa se...

- ...Sei un criminale
  - Siti creati apposta per raccogliere numeri di carta di credito dei clienti, e poi sparire
- ...Sei qualcun altro
  - Hai preso il posto di un server WEB legittimo
  - Hai preso il posto di un utente legittimo
- ...Hai dipendenti disonesti
- ...Quanto il tuo sito è sicuro
  - E soprattutto, quanto sono al sicuro i dati dei tuoi clienti che sono memorizzati lì!

In rete, tutti sanno che...

- Molti (quasi tutti) gli utenti sono un po' sprovveduti
  - Faranno tutto quello che il loro computer dirà loro di fare
- Molti utenti eseguono programmi difettosi
  - Sono troppo pigri o non sanno che è necessario aggiornarli
- Non ci si può aspettare che gli utenti conoscano i protocolli di Internet
  - Non controllano se la transazione è sicura oppure no
- Gli utenti configurano il loro sistema
  - Con il minimo sforzo
  - Per massimizzare la facilità d'uso

Punti di attacco comuni

- Sul protocollo di commercio
  - Intercettare password degli utenti e numeri di carta di credito
  - Intercettare i dati ritornati agli utenti
  - Intercettare e manipolare le connessioni
- Al server
  - Ci sono tanti modi per entrare in un server
  - Una volta che si è dentro, tutte le difese sono inutile
- Al client
  - Il gestore del server ovviamente non ha alcun controllo del sistema usato dagli utenti

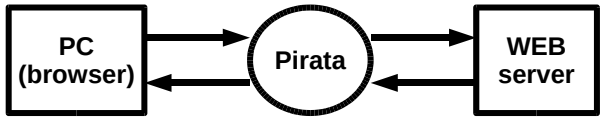
Contromisure

- Politiche di sicurezza
- Compartimentazione
- Firewalls
- Sicurezza del calcolatore
- Crittografia
- Autenticazione
- Tecniche per rilevare accessi non autorizzati
- Usare configurazioni appropriate, ed educare gli utenti a fare altrettanto

Politiche di sicurezza

- A quali dati gli utenti hanno accesso
  - Quali dati accedono in lettura, quali in scrittura
- Come autenticare gli utenti
  - Possibilmente in modo diverso in base a cosa devono fare
- Quanto proteggere i dati in transito
  - Possibilmente in misura diversa in base alla loro importanza
- Quali servizi si usano
  - E quanto ci si può fidare di loro

Tipi di attacchi



- Può fare molte cose
  - Intercettare i messaggi
  - Modificare i messaggi del server
  - Modificare i messaggi del client
- Contromisure
  - Non inviare nulla di importante; in questo caso non si corrono rischi perché nessuno è interessato
  - Usare la crittografia per tutto il resto

Crittografia

- Poteggere i dati inviati al server WEB
  - Es. contenuto del form con i dati personali del cliente e il numero della carta di credito
- Protegge i dati restituiti dal server
  - Potrebbero contenere informazioni sensibili
  - Inoltre, viene garantita l'integrità dei dati
- Le prestazioni e la reale sicurezza dei protocolli crittografici sono un problema
  - Protocolli che richiedono processori molto veloci non sono destinati ad avere consenso
  - E' impossibile *dimostrare* che un protocollo crittografico è veramente sicuro

La crittografia non è la soluzione di tutti i problemi!

- I dati sono cifrati sono cifrati prima di essere trasmessi, e vengono decodificati appena ricevuti
- I dati sono disponibili “in chiaro” (non cifrati):
  - Nel computer dell'utente che li ha inviati
  - Nel server WEB che li ha ricevuti
- Se qualcuno ha accesso al computer di una delle due parti, le informazioni sono *comunque* compromesse

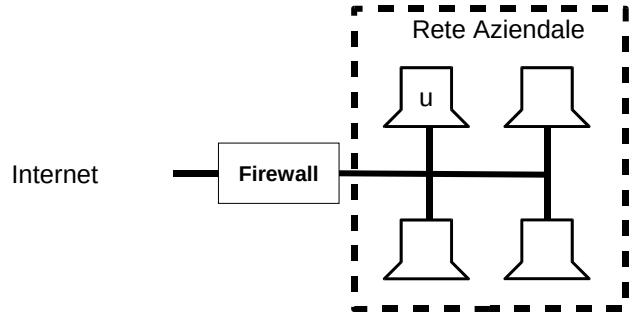
Un ostacolo

- Gli utenti sono restii a comunicare i propri dati in rete
  - *“Non dovete preoccuparvi a fare acquisti presso di noi, dato che le comunicazioni sono cifrate con il protocollo XYZ a 1024 bit”*
- Ma che succede una volta che i dati sono arrivati?
  - Il server è sicuro?
  - Gli impiegati che maneggiano i miei dati sono fidati?

Firewall / 1

- Sono dispositivi inseriti nel punto di collegamento tra la rete aziendale e Internet
- Il loro scopo è esaminare il traffico in ingresso e in uscita
  - Tutto il traffico in ingresso e in uscita deve passare attraverso il firewall
  - Il firewall deve essere sicuro
  - L'accesso può essere ristretto solo ad un certo tipo di traffico
    - Verso certi server
    - Verso certi servizi
    - Solo utilizzando un certo protocollo...

Firewall / 2



Sicurezza del server

- Il server di ECommerce deve essere sicuro
  - Possibilmente dietro un firewall
  - Ma il firewall non può bloccare ogni tipo di traffico. Gli utenti devono potersi connettere al server!
  - Il firewall può limitare l'accesso dall'esterno al solo servizio WEB
- Il programma di WEB server può essere insicuro
  - Delle falle nel software possono consentire a utenti esterni l'accesso non autorizzato ai dati

Attacchi DOS

- DOS=Denial Of Service
  - Interruzione del servizio
- Inondare il server con una marea di richieste, molte più di quelle che è in grado di soddisfare
- Non ci sono metodi efficaci per proteggersi
  - L'attacco può essere rilevato, e la fonte delle richieste può essere filtrata...
  - ...però l'attacco può essere distribuito, nel senso che molteplici sorgenti inondano il server. Spesso queste sorgenti sono PC di ignari utenti sotto il controllo di virus o cavalli di Troia.

Consigli pratici per rendere il server meno insicuro

- Disattivare tutti i programmi inutili che girano sul server (soprattutto i servizi)
  - FTP, Posta, Gopher...
- Fare in modo che il programma di server WEB non abbia privilegi particolari
  - Se qualcuno dovesse forzare il programma di server WEB acquisirebbe i suoi stessi privilegi
- Configurare correttamente il server WEB
- Utilizzare software in grado di accorgersi se il sistema è stato compromesso
  - Allertare gli amministratori immediatamente!

Attacchi al cliente / 1

- Se il server di ECommerce è sicuro, e il canale di comunicazione è protetto, il punto debole può diventare la macchina del cliente
  - Il cliente è la parte più difficile da “rendere sicura”
- Molte cose possono capitare
  - Rubare le password
  - Monitorare i tasti premuti sulla tastiera
  - Intercettare i dati in transito *prima* che siano codificati (o dopo che sono stati decodificati)

Attacchi al cliente / 2

- Difetti (bug) dei browser possono consentire
  - L'installazione di virus sul pc
  - L'esecuzione di codice arbitrario
  - Codice malevolo (JavaScript) che manda informazioni sensibili a terzi
  - L'esecuzione di applet Java che scrivono/leggono cosa non dovrebbero

Come proteggere il cliente?

- Sandbox
  - Eseguire i programmi in ambienti “protetti” che impedi-scono danni e consentono solo certi comportamenti
- Firme digitali
  - Vengono utilizzate per certificare l'origine dei programmi che si scaricano dalla rete. Solo programmi che proven-gono da fonti sicure dovrebbero essere eseguiti
- Configurare correttamente
  - Disabilitare Java, JavaScript, ActiveX, cookies e tutto quello che non serve
  - Usare programmi per filtrare informazioni sensibili

Altri meccanismi di protezione

- Watermark
  - Si tratta di nascondere delle informazioni all'interno di file normali (tipicamente audio o immagini statiche) in modo che non siano visibili (o udibili) nel file originario
  - Perché funziona? Audio e immagini contengono informazioni superflue che possono essere alterate senza compromettere l'aspetto del file
  - E' in queste informazioni superflue che può essere nasco-sto il watermark
- A cosa serve?
  - In tutti i casi in cui serve una sorta di “filigrana digitale”
  - Proteggere la proprietà intellettuale