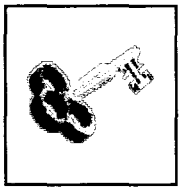

SEGURIDAD DEL CLIENTE EN EL SERVICIO WORLD WIDE WEB

Felipe Moreno Strauch

Estudiante de la ETSETB, UPC y socio colaborador de BJT.
felipe@bjt.upc.es

INTRODUCCIÓN

El World Wide Web empezó como una forma sencilla de distribuir información, pero ahora se ha transformado en algo que va mucho mas allá. A medida que el Web se ha ido desarrollando las herramientas involucradas en el proceso de creación de las páginas también lo han hecho. Al lenguaje HTML se han añadido nuevas tecnologías como el JavaScript, el Java o el Active-X y los navegadores han aumentado en tamaño para ofrecer más funcionalidad.

Los navegadores ahora son programas complejos, con muchas líneas de código y esto tiene dos consecuencias en cuanto a la seguridad: a medida que aumentan sus prestaciones se vuelven más difíciles de configurar y a medida que su código se vuelve más complejo, son más susceptibles a tener fallos. Por ello, es muy importante dedicar algún tiempo a estudiar la configuración de estos programas y mantenerse informado sobre las posibles vulnerabilidades que pueden tener.

En este artículo, aclararemos algunos conceptos relativos su configuración que están relacionados con la seguridad, veremos algunos de los fallos conocidos más importantes que poseen los dos navegadores de uso mas extendido y propondremos algunas soluciones para navegar de forma más segura.

Cuando hablamos de seguridad en el navegador hablamos básicamente de dos puntos: la privacidad del usuario que navega y la integridad de su máquina. En cuanto a privacidad, nos referimos a navegar de forma anónima, divulgando la mínima información posible a la red y en cuanto a integridad, al acceso que los programas o scripts contenidos en las páginas Web pueden tener a los recursos de la máquina.

1. Helper Applications

Para ampliar la funcionalidad del navegador podemos configurar aplicaciones externas como «helper applications» y asociarlas a tipos MIME que el navegador no sea capaz de tratar por sí mismo. De esta forma al recibir un documento de tipo desconocido, este consulta la lista de «helper applications» y si encuentra alguna aplicación asociada al tipo recibido la ejecuta y le pasa el documento.

En cuanto a seguridad es importante controlar que aplicaciones están configuradas como «helper applications» ya que esto puede suponer una posible vulnerabilidad. Por ejemplo si se configurará una shell «command.com» como «helper application» de un tipo MIME application/x-bat seria posible llegar a ejecutar archivos por lotes («.bat») enviados desde un servidor Web. Lo que debemos hacer es controlar a aquellas aplicaciones que son capaces de ejecutar macros o scripts y que están configuradas como «helper applications» (por ejemplo el Microsoft Word o el Microsoft Excel).

En general basta con configurar el navegador de forma que NUNCA se ejecuten aplicaciones externas de forma automática sino que se pregunte siempre antes (la típica ventana de «ejecutar» o «grabar en disco») para que el usuario siempre tenga la ultima palabra.

2. Plug-ins

Los plug-ins, como las «helper applications» sirven para ampliar la funcionalidad del navegador permitiéndole que interprete documentos de tipos que antes desconocía. La diferencia es que en lugar de aplicaciones externas, son módulos que se instalan sobre el propio navegador. El funcionamiento es muy parecido: al recibir un documento de tipo desconocido se consulta la lista de plug-ins instalados y se ejecuta el adecuado.

En cuanto a seguridad es importante tener en cuenta que no se debe instalar un plug-in si no se sabe exactamente para que sirve y que puede hacer. Además es recomendable instalar solamente plug-ins desarrollados por empresas conocidas como: Macromedia (Flash o Shockwave), RealNetworks

(Real Player), etc. Ya que en este caso la marca supone cierta garantía.

3. Cookies

Los «cookies» son pequeños trozos de información enviados por un servidor de páginas Web y almacenados por el navegador en el disco duro. El objetivo es subsanar la falta de estado del protocolo HTTP y permitir crear la ilusión de una sesión a lo largo de varias páginas visitadas (por ejemplo, para que el usuario solamente tenga que autentificarse una vez). El navegador controla el envío de los cookies hacia los servidores en función del atributo «dominio». De esta forma, el cookie solo puede ser enviado hacia un servidor en el mismo dominio del que lo ha generado (para evitar que un determinado dominio tenga acceso a cookies creados por servidores de otros dominios). Un mecanismo de control impide que se establezcan cookies con atributo «dominio» con dominios de alto nivel («top level domains») como el «.com».

Los cookies están muy relacionados con la privacidad, ya que muchos sitios los utilizan para hacer un seguimiento de las acciones del usuario. Por ejemplo, los buscadores como el Yahoo o el Altavista guardan todas las búsquedas realizadas por un usuario en una base de datos que utilizan para realizar marketing personalizado (la publicidad aparece en función de los intereses del usuario). Para poder realizar este seguimiento establecen un cookie en cada cliente donde almacenan un número identificador que sirve de índice en esta base de datos.

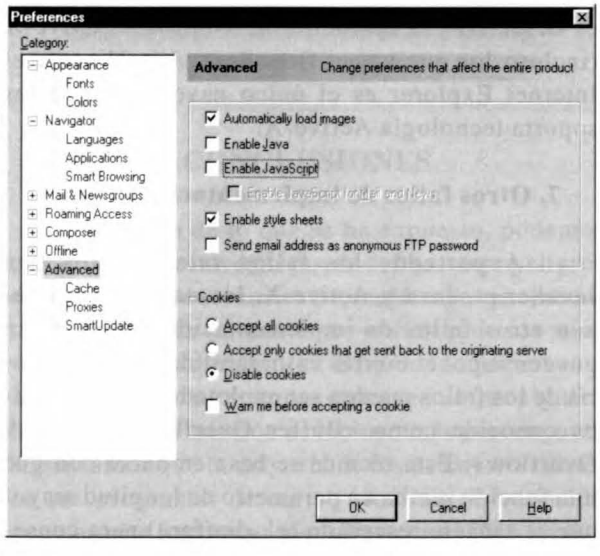

Figura1. Pantalla de configuración del Netscape Communicator (File-Preferences).

Para evitar este tipo de acciones lo más eficaz es desactivar la aceptación de cookies o al menos configurar el navegador para pedir una confirmación al usuario antes de aceptar uno. Por defecto, los navegadores tienen activada la opción de aceptar los cookies activada.

4. JavaScript

El JavaScript es un lenguaje de scripts desarrollado por Netscape para añadir mas interactividad a las páginas Web. A principio se incorporaba solamente a sus navegadores pero a medida que aumentó su popularidad, Microsoft lo incorporó también al Internet Explorer (en la versión 3.0).

La historia de JavaScript esta llena de ejemplos de agujeros de seguridad, pero dada la propia característica de ese lenguaje (no se puede cambiar la información almacenada en el disco) los fallos repercuten casi siempre en perdida de privacidad.

Algunas de las vulnerabilidades relacionadas con JavaScript permiten obtener información sobre las páginas visitadas como por ejemplo el «JavaScript Cache Browsing Bug» (versiones Windows de Netscape 3.04, 4.07 y 4.5) que permite que un script sea capaz de leer la información almacenada en la memoria cache; o obtener información sobre la configuración del navegador como la «Preferences Bug» (versiones 4.0 a 4.04 de Netscape en todas las plataformas) que permite acceder al fichero «prefs.js» y obtener la dirección de email, servidores de correos y noticias, contraseña de correo y de FTP, etc.

Otros fallos de seguridad más importantes permiten que un script pueda acceder (lectura solamente) a los ficheros del disco duro de la máquina cliente. El «Injection Bug» (versiones 4.0 a 4.07 y 4.5PR de Netscape en todas las plataformas) permite acceder a la información almacenada en los cookies, determinar otras páginas visitadas y obtener listados de ficheros y directorios. Otros fallos permiten el envío de ficheros al servidor como el «The Cuartango Hole» o el «The Son of Cuartango Hole» que afectan a las versiones de Netscape 4.0 y 4.01 así como la versión preview del Internet Explorer 5. Otros fallos parecidos afectan también a la versión 4.0 del Internet Explorer. Estos tipos de fallos suelen utilizar formularios en frames ocultos para enviar los ficheros a un CGI mediante elementos de tipo «file» (INPUT TYPE=FILE). Para evitar la restricción de acceso que tienen los scripts a estos elementos se suele utilizar el método de «copiar-y-pegar».

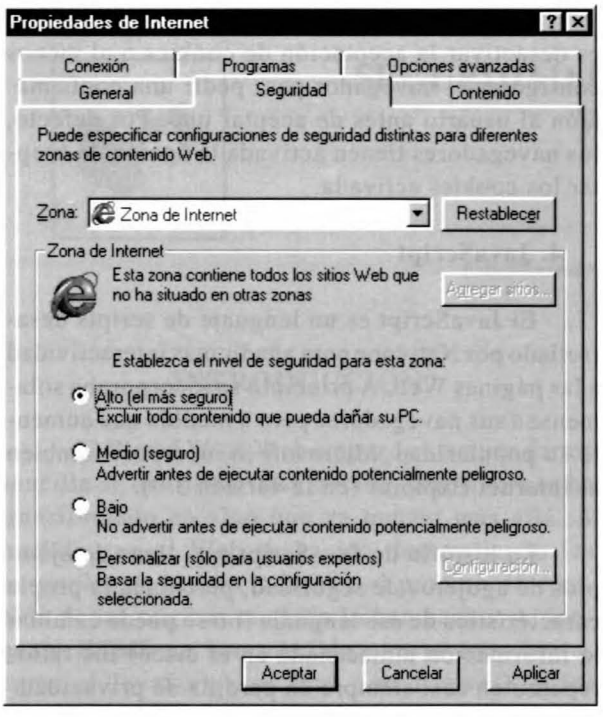

Fig.2 - Opciones de seguridad en «Panel de Control» - «Configuración de Internet».

5. Java

Aunque Java es un lenguaje de programación en todos sus aspectos, los programas hechos para su utilización en las páginas Web, los applets, tienen fuertes restricciones. Estas restricciones las controla un objeto «security manager» creado por el navegador que impide al applet ejecutar ciertos comandos de sistema, cargar ciertas librerías, acceder a ciertos recursos como el sistema de ficheros o establecer conexiones con otros servidores en la red a parte de su servidor de origen.

A pesar de ser seguro en la teoría, los fallos de implementación hacen con que en la práctica un applet pueda generar efectos desastrosos. Casi todas las vulnerabilidades relacionadas con Java permiten burlar al «security manager» y obtener acceso total a la máquina como el «Java Security Vulnerability» (Netscape 4.0 a 4.5 en todas las plataformas) del 29/03/99; el «Classloader Java Vulnerability» (Netscape 4.0 a 4.05 en todas las plataformas) del 14/08/98 o el «Virtual Machine SandBox Vulnerability» (Explorer 4.0 y 5.0) del 25/08/99. Este ultimo, al afectar la implementación de la máquina virtual de Java (JVM) puede ser explotado desde todos los programas de Microsoft que la utilizan (como el Outlook por ejemplo).

En caso de utilizar Internet Explorer es muy recomendable obtener la versión corregida de la JVM de Microsoft, que se puede bajar de Internet.

6. Controles Active-X

El Active-X es una tecnología desarrollada por Microsoft para distribuir software por Internet. De la misma forma que un applet de Java, un control Active-X puede ser incluido en un página Web. Los controles son distribuidos en código binario y por tanto han de ser compilados para cada posible plataforma cliente a diferencia del código precompilado de Java.

El modelo de seguridad utilizado por Microsoft para el Active-X es bastante diferente del modelo de Java. No hay ninguna restricción sobre que puede hacer un control sino que se permite que cada control sea «firmado» digitalmente utilizando un sistema llamado «Authenticode». De esta forma se puede comprobar el origen del control comprobando la firma y la autenticidad del certificado utilizado mediante una Autoridad de Certificación (los applets de Java también pueden «firmarse» mediante un mecanismo parecido).

El «Scriptlet.typelib/Eyedog Vulnerability» del 31/08/99 que afecta las versiones 4.0 y 5.0 de Internet Explorer permite explotar el fallo de dos controles Active-X (el «scriptlet.typelib» y el «eyedog») para crear y modificar ficheros, acceder al registro de Windows e incluso permitir la ejecución de código (realizando un ataque de «Buffer Overflow» sobre los métodos del control «eyedog»). Para corregir este problema se puede descargar un parche desde Microsoft, pero lo más recomendable es desactivar la ejecución de controles Active-X (incluso los que vayan firmados). Actualmente el Internet Explorer es el único navegador que los soporta tecnología Active-X.

7. Otros fallos de implementación.

A parte de los fallos relacionados con JavaScript, Java y Active-X, los navegadores tienen otros fallos de implementación que también pueden suponer ciertas vulnerabilidades. La mayoría de los fallos pueden ser explotados con la técnica conocida como «Buffer Overflow» o «Stack Overflow». Esta técnica se basa en hacer con que una función reciba un parámetro de longitud mayor que el espacio reservado (el «buffer») para conse-

guir sobrescribir la dirección de retorno almacenada en la pila («stack»). Así se puede sustituir esta dirección por la de otro punto de la memoria (en general un punto dentro del propio buffer) donde se pone el código a ejecutar.

El Internet Explorer 4.0 y 4.01 contiene varios de estos fallos relacionados con URLs o elementos HTML de longitud muy larga y el Netscape 4.03 y 4.04 presenta problemas al almacenar páginas con títulos muy largos en los bookmarks. El «Long Filename Mail Vulnerability» (Netscape 4.0 a 4.05 y PR1) es otro caso de «Buffer Overflow» y se puede explotar si un mensaje de email o news contiene como attachment un fichero con un nombre muy largo.

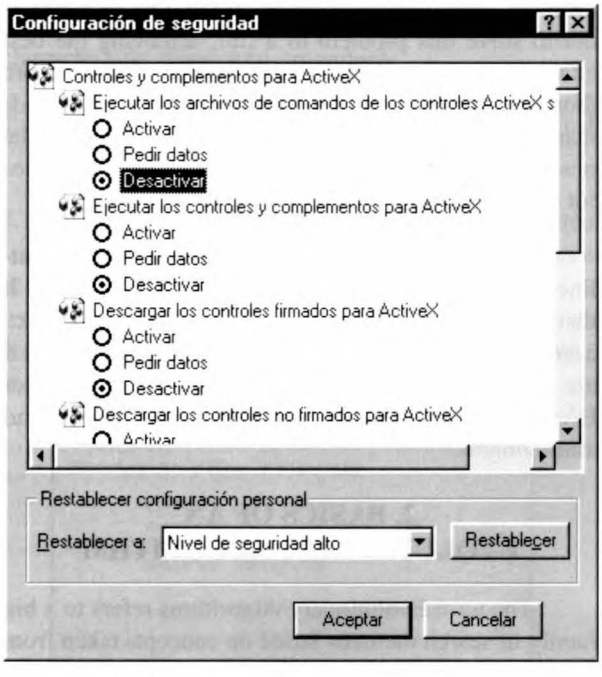

Fig.3 - Configuración de la opción Personalizar donde se puede cambiar los parámetros de Java, JavaScript y Active-X.

CONCLUSIONES

En vista de lo que se ha expuesto, podemos comprobar que navegar puede ser bastante peligroso. No debemos sentirnos protegidos por el aparente anonimato de ser uno entre millones de usuarios ya que estos ataques no van dirigidos a una persona, sino que son como trampas esperando a que alguien las active. La situación es incluso más preocupante si pensamos que la mayoría de los usuarios utilizan en sus programas de correo electrónico la opción que permite formatear mensajes con HTML ya que entonces las páginas «trampa» se pueden enviar por email y para activarlas basta con abrir el mensaje.

El resultado de conseguir ejecutar código en la máquina cliente puede tener serias consecuencias, no solo para la máquina local (borrar el disco duro, cambiar la configuración del sistema operativo, obtener información sobre el usuario), sino incluso para la propia red donde esta está conectada (obtener ficheros de password, contaminarla con virus, o instalar programas de control remoto o «sniffers»). Como la mayoría de los sistemas de firewall habilitan el tráfico HTTP, se podría atacar a una máquina utilizando uno de los fallos de los navegadores para instalar en ella un programa. Este programa podría funcionar como un cliente HTTP «especial» que se utilizaría para intercambiar datos con el exterior anulando el firewall. Sería una forma de salida para la información obtenida dentro de la red (ficheros, contraseñas, nombres de servidores) y además se podría utilizar como forma de entrada para realizar ataques dentro de la red (podríamos por ejemplo llegar a montar una sesión de Telnet por encima del HTTP).

Para evitar estos problemas, es necesario tener siempre las ultimas versiones de los navegadores (4.7 para el Netscape Communicator y 5.0 para el Internet Explorer). De esta forma aunque no se podrá asegurar invulnerabilidad (incluso las ultimas versiones tienen fallos), podemos garantizar que estamos protegidos de los fallos conocidos y difundidos por Internet, que son los más peligrosos. Además es necesario configurar adecuadamente el navegador y si se navega por páginas «potencialmente peligrosas», desactivar la ejecución de JavaScript, Java, Active-X y deshabilitar los cookies. Por ultimo, también es importante, estar siempre informado de los fallos encontrados y de sus posibles soluciones o parches, lo que se puede hacer consultando los boletines de seguridad a través de Internet en las páginas de los propios navegadores.

PARA MÁS INFORMACIÓN

[1] Página de seguridad de Netscape: http://home.netscape.com/security/notes/index.html

[2] Página de seguridad de Internet Explorer: http://www.microsoft.com/windows/ie/security/default.asp

[3] FAQ sobre seguridad del World Wide Web Consortium: http://www.w3.org/Security/faq/www-security-faq.html

[4] Secure Internet Programming Laboratory - Princeton University: http://www.cs.princeton.edu/sip/