www.aesf.org

Website of the American Electroplaters and Surface Finishers Society

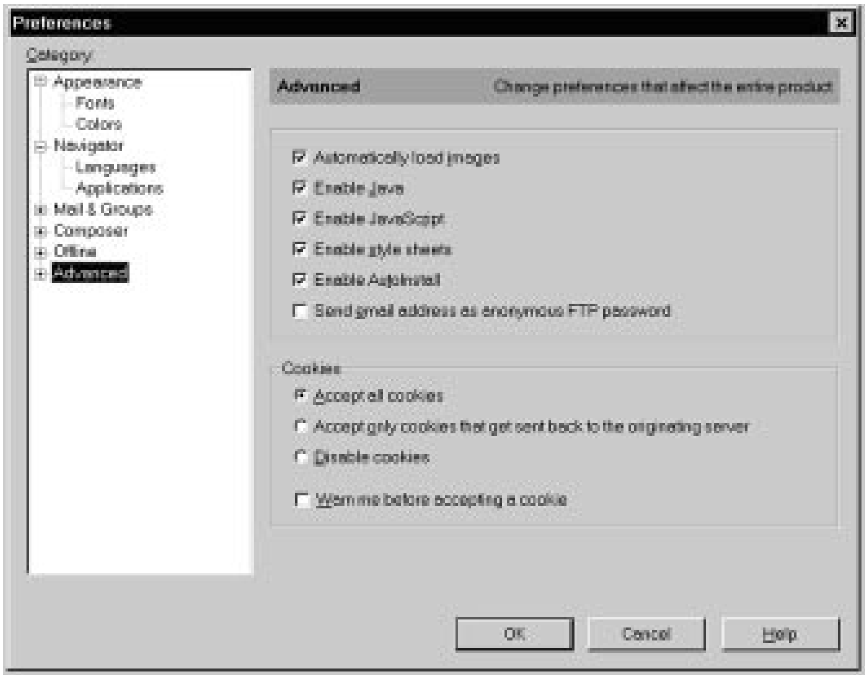
Ted Witt, CEF
AESF Executive Director
12644 Research Parkway
Orlando, FL 32826-3298
e-mail: ted@aesf.org

Maintaining Security & Privacy on the Internet

Most computer users have some concerns about the Internet with regard to security and privacy, especially when it involves monetary transactions or transfer of confidential data. Many of us don't like the idea of anyone monitoring what we view on the Internet or the records we keep. These concerns are valid. If we understand how the technology works and what controls are available to them, however, the process is much less worrisome. This month's column looks at two aspects of Internet security and privacy: Secure servers for monetary transactions and "cookies."

What Is a Secure Server? How Secure Is It?

When you arrive at a common Internet web page, your browser (*e.g.*, Netscape, Internet Explorer) communicates with the host server by sending and receiving plain text messages. Information travelling between your computer and a server uses a routing process that can extend over many computer systems. However unlikely, a hacker could potentially intercept the information and read it.[1] Eavesdroppers can operate from any point on the path between your browser and the server, including the network on the browser side, the network on the server side, the end user's Internet service provider (ISP), or the server's ISP. For this reason, any information that you want to keep private should only be transmitted over a **secure server**. With a secure server, information sent by both your browser and the server are "encrypted." This is done using public key algorithms, introduced by Netscape in a protocol called SSL (Secure Sockets Layer Protocol).[2]



Advanced — Change preferences that affect the entire product

☑ Automatically load images
☑ Enable Java
☑ Enable JavaScript
☑ Enable style sheets
☑ Enable AutoInstall
☐ Send email address as anonymous FTP password

Cookies
● Accept all cookies
○ Accept only cookies that get sent back to the originating server
○ Disable cookies

☐ Warn me before accepting a cookie

Netscape controls for "cookies."

Early encryption technology was based on a 40-bit secret key. In 1995, a French researcher used a network of workstations to crack a 40-bit encrypted message in a little over a week. Newer technology, like that used on the AESF website,[3] employs the more secure 128-bit secret key. To crack a message with such a key would take significantly longer than the age of the universe, using conventional technology.

How Do I Know If a Website Is Secure?

In Netscape, you can tell what kind of encryption is in use for a particular document by looking at the "document information" screen accessible from the file menu. The little key in the lower left-hand corner of the Netscape window also indicates this information. A solid key with three teeth means 128-bit encryption, a solid key with two teeth means 40-bit encryption, and a broken key means no encryption. Visit and click on "join the AESF right now with this secure online application form." The web page that appears is a secure form (128-bit).

With Microsoft Internet Explorer, a solid padlock will appear on the bottom right of the screen when

[1] *Secure communication does not eliminate all of an Internet user's concerns. The greatest threat for using a credit card over the Internet is not with hackers, but rather with the person and company to whom you have entrusted your card information. Of course, this concern is not limited to the Internet. Anytime you hand your credit card to a waiter or sales clerk, you run a risk of losing money. Security technology does not protect you from disreputable or careless people with whom you choose to do business.*

[2] *http://www.netscape.com/assist/security/ssl/howitworks.html*

[3] *AESF employs a secure server for any business transactions performed on the website. For example, the AESF membership form is located on the secure server.*

encryption is in use. To determine whether 40-bit or 128-bit encryption is in effect, open the document information page using File, Properties. This will indicate whether "weak" or "strong" encryption is in use.

What Are Cookies?

The cookie was developed by Netscape to improve the service capabilities of websites. Normally, each time a browser requests the URL of a page from a web server, the request is treated as a completely new and anonymous undertaking. In most cases, this process does not cause any difficulties, and is actually desirable. Users of certain websites can benefit, however, from being recognized by the server. For example, users can be provided with personalized information or helped with on-line sales/services. Cookies are the means by which a server can "mark" visitors so that they can recognize them in the future. A cookie is a piece of information that is delivered to your computer and, if accepted, is stored on your hard disk. The browser returns a copy of the cookie to the server each time it connects.

Consider this simple example: You fill out a form on a server giving your favorite color, a server can turn this information into a cookie and send it to your browser. The next time you visit the site, your browser will return the cookie, allowing the server to alter the background color of its pages to suit your preferences.

Cookies are supported by most versions of Netscape, Internet Explorer, and other browsers. Users have control, however, over whether or not cookies are accepted. Without acceptance, the exchange never occurs. Current versions of browsers offer the option of alerting you whenever a server attempts to give your browser a cookie. If you turn this option on, you always have the ability to refuse cookies.

You can avoid the situation entirely by completely turning off cookie acceptance. With Netscape, the controls can be located from the top menu [pull down "file" and select "preferences," and then "advanced" (see the figure)].

As originally designed, cookies were to be of benefit to the user. Most likely, they were intended to be limited to communications between one user and one server. Although most of time they are used in a positive way, there is also a dark side to cookies.

Because cookies can be matched to a user's preferences and browsing habits, they can become a potential tool for targeted advertising. Moreover, they can be used to develop detailed profiles of users. Currently, this information is primarily used for targeted advertising (banners). The possibility exists, however, for these profiles to be sold and resold to other commercial interests.

You can check your hard drive to find out which cookies you have stored away. The easiest way to do this is to use the "find" feature and search your drive for "cookies." Internet Explorer saves cookies in the Cookies sub-folder, usually under the Windows folder. Netscape stores cookies in the file "cookie.txt." Open the file, and you can usually decipher the origin of any cookies.[4] **P&SF**

CSI Strategic Goals Website

A new website has been developed by the NMFRC for the CSI Strategic Goals program. This site provides background information on the program, a sign-up sheet, participant directory, electronic reporting for participants and access to facility data. Also, there is a benchmarking tool available to participants that allows you to compare your shop's water use, energy use, and sludge generation rate.

[4] *Incidentally, you will not find "cookie" files from aesf.org or the nmfrc.org.*

East Meets West In Hawaii at the "Advanced Surface Technology" Forum

October 8–9 • Hilton Waikoloa Village • Kamuela, Hawaii

Think about putting a "good finish" on 1998 by attending the first-time-ever Forum sponsored by the Surface Finishing Society of Japan and the AESF. You'll be able to combine the best of both worlds: Get an update in surface finishing, environmental and management technologies while enjoying the tropical paradise setting of Hawaii.

Diversified Conference Program

- 12 presentations from AESF ("western" authors)
- 12 presentations from the SFSJ ("eastern" authors)
- Proceedings will include all 24 presentations
- Papers will be presented and printed in English
- Poster session (more than 20 papers are lined up now; others welcome)
- Golf
- Social Events
- Light Metals Finishing Course (October 7–9)

Conference Organizers

For AESF: Tam Van Tran, Ionics, Inc., Watertown, MA

For SFSJ: Dr. Tetsuya Osaka, Waseda University

Head Communication Officer for Conference: Kazuyoshi Okuno, Okuno Chemical Industries Co., Ltd., Osaka, Japan

For more information call
AESF at 407/281-6441