Global Information Assurance Certification Paper

Internet Security: Focus On Internet Explorer

by Jason K. Zahn

GSEC Practical Assignment Version 1.2b

According to a recent estimate, approximately 58% of the Internet population is using Microsoft's Internet Explorer.[i] Given the popularity of this browser and the impact of Internet usage by end users on a business, it is critical to make sure that the browser is properly secured. This paper will explore three primary areas related to Microsoft's Internet Explorer: the overlying importance of an Internet Usage Policy, a high level view of Internet Explorer security features, and the critical importance of having a security awareness program in place, with a focus on Internet Explorer vulnerabilities.

I. Internet Usage Policy

For security professionals, this will come as no new news, but one would be surprised at how often a company will spend countless hours and dollars successfully configuring routers, firewalls, proxy servers, intrusion detection services, and implementing a VPN, only to neglect the most simple first step of Internet security: an Internet Usage Policy (IUP). It is not the purpose of this report to explain the full benefits of an IUP or provide a comprehensive explanation on how to create one. However, it should be noted that no amount of technical configuration would alleviate the many risks to an organization that does not set guidelines on Internet usage. For those who are skeptical of the risks, here are some interesting statistics. According to a 1999 survey of 1,800 workers:

- **55% of workers exchanged e-mail that could be considered racist, sexist, or otherwise politically incorrect.**
- **60% admitted to receiving or sending adult-oriented material.**
- **10% admitted to having received e-mail that contained company-confidential information.**
- **21% to 31% admitted to sending confidential information outside the company, including financial and product data.**
- **More than 85% of workers use office e-mail for personal use.[ii]**

These statistics illustrate the legal risk, not to mention the technical risk involved with users performing downloads, using popular file exchange services like Napster which consume bandwidth, and receiving questionable content over risky mediums such as JAVA and ActiveX.

An IUP should be clearly stated, frequently evaluated and updated, and distributed to everyone on a regular basis. There are several matters to consider in setting IUP policy, and some of the most important are the following:

1. **Restrict Internet access to users who require it for business purposes only.**

2. **Define appropriate use of the Internet, e-mail, and other electronic resources.**

3. **The company needs to state what the consequences are of breaking the policy.**

All of the work that is spent on creating an IUP is not merely extraneous paperwork but will provide real benefits to the company, some of which are:

1. **In the event of legal action against company, the IUP will assist in separating the company from the actions of individuals and show that the company has taken steps, as a means of due diligence, to have prevented the occurrence of the individual's actions.**

2. **It insures that those who decide to break the policy will do it consciously and independently rather than from ignorance.**

3. **It will help protect both the company and its employees from misuse of the Internet, e-mail, and other electronic resources.**

In conclusion, before a company takes the steps to configure their technical environment, including Internet Explorer, time should be invested in developing a comprehensive Internet Usage Policy.

II. IE Security Options

The next and most obvious step, to securing Internet Explorer (IE) is to properly configure the browser. In many ways, Internet Explorer is a safe browser. The last few versions of IE support Secure Socket Layer (SSL) 2.0/3.0, Private Communication Technology (PCT) 1.0, CryptoAPI, and VeriSign certificates. Additionally, it is possible to obtain a version that employs 128-bit encryption, one of the stronger forms of encryption available (commercially) for use over the Internet. To see which version of Internet Explorer you have, click on **Help** in your browser's top menu bar. Scroll down to "About Internet Explorer," and the top line of the resulting window displays your browser version. Those without the 128-bit browser should seriously consider upgrading, if company policy permits.

Secure Socket Layer (SSL) is a Netscape-developed protocol that has become a standard security

approach for World Wide Web (WWW) browsers and servers on the Internet. SSL provides a security "handshake" that is used to initiate the TCP/IP connection. As a result of this handshake, the client (browser) and server will agree on a security level and any authentication required for the connection. The SSL will then encrypt and decrypt the byte stream of the application protocol being used (for example, HTTP).[iii] This verifies that all the information in both the HTTP request and the HTTP response are fully encrypted, including the URL the browser is requesting, any submitted form contents (such as credit card numbers), any HTTP access authorization information (usernames and passwords), and all the data being returned to the browser from the server.

Private Communication Technology (PCT) is a Microsoft-developed security protocol available in IE only. According to the draft by Microsoft on Microsoft's TechNet:

> (PCT) protocol is designed to provide privacy between two communicating applications (a client and a server), and to authenticate the server and (optionally) the client. PCT assumes a reliable transport protocol (e.g., TCP) for data transmission and reception. The PCT protocol is application protocol-independent. A "higher level" application protocol (e.g., HTTP, FTP, TELNET, etc.) can layer on top of the PCT protocol transparently. The PCT protocol begins with a handshake phase that negotiates an encryption algorithm and (symmetric) session key as well as authenticating a server to the client (and, optionally, vice versa), based on certified asymmetric public keys. Once transmission of application protocol data begins, all data is encrypted using the session key negotiated during the handshake.[iv]

Safe communications and the ability to perform transactions without being overheard are of primary importance to a business. These protocols go a long way in supporting that need.

IE also supports server and client authentication by using digital certificates to identify users to web servers. Additionally, IE supports code signing with Authenticode, which assists in verifiying that downloaded code has not been modified from its original source. For more information on Authenticode, visit Microsoft's Authenticode page.[v]

CryptoAPI 1.0 provides the underlying security services for the *Microsoft Internet Security Framework*. CryptoAPI will allow developers to integrate cryptography into their applications. Microsoft has put a lot of work and planning into the security of their products, and some time spent browsing through the security section of TechNet is time well spent. From "security zones", which allow you to restrict browsing capabilities, to continued support of Authenticode, IE has many features that can assist in increasing browser security.

For example, a new feature in Internet Explorer 5.5 is increased cookie management capabilities. A summary of this feature was provided by Microsoft as follows:

- **Notify consumers of cookies.** The new enhancements will present consumers with a balanced description of cookies and their uses, clearly differentiating between first- and third-party cookies. Additionally, any time a persistent third-party cookie -- the kind of cookie that remains on a consumer's hard drive for a specified period of time and came from a site different from the one the user is currently visiting -- is being served or read on a consumer's machine, a default setting will alert the consumer, who can then make the most informed decision about accepting that type of cookie. The default response for all cookie confirmation prompts is for the cookie to be accepted, though consumers can easily refuse the cookie.

- **Provide additional controls over cookies.** Consumers who decide not to receive any of the customization that cookies provide can now easily delete all cookies from their hard drive. This "delete all cookies" button has been added on the primary Internet Options page of Internet Explorer. At the same time, previous features that allowed users to delete cookies selectively have been maintained.[vi]

In addition, one of the newly announced features of Internet Explorer 6.0 Beta is that it will use features from the industry-developed Platform for Privacy Preferences (P3P) specifications. P3P-compliant privacy policies can be read by a browser for ready comparison to a Web surfer's pre-set privacy settings. If the policy of a site conflicts with a surfer's pre-set privacy requirements, IE 6.0 will issue a warning to the user, and may block the site altogether.[vii]

Just like every software product, Microsoft's Internet Explorer does have vulnerabilities, and as discussed in the next section, many new areas of weakness are discovered on a periodic basis. In spite of this, it is still one of the more security robust browsers available, and system administrators, as well home users, should take the time to make sure they have explored the various security options inherent with this browser.

III. Security Awareness Program and Current Vulnerabilities

Within two weeks of this report's creation, there were two new vulnerabilities identified in Internet Explorer. The specifics of these vulnerabilities will be discussed in further detail later, however, this brings up another critical infrastructure issue that is often overlooked; the critical importance of having a security awareness program.

Again, it is not within the scope of this document to explain the details of setting up a comprehensive security awareness program, but it will be discussed at a high level. Specifically,

with regard to Internet Explorer, a system administrator or security staff should be reviewing Microsoft's TechNet on a regular basis. TechNet (http://www.microsoft.com/technet/security/current.asp), lists the latest vulnerabilities and patches, if available. To make things even simpler, one can even send an e-mail to microsoft_security-subscribe-request@announce.microsoft.com and they will be subscribed automatically to a notification list so that they receive all security notifications via e-mail. Great effort should be made to ensure that any critical vulnerabilities are properly and promptly addressed (whether this entails simply applying a patch or some other work around until a fix is available).

Many administrators incorrectly assume that time spent on TechNet is only to obtain functionality enhancements, but by looking at three vulnerabilities identified in the last few months, the importance of staying up-to-date on security issues should be clear.

First is a glitch in Internet Explorer (IE) browser versions 5.01 and 5.5. It will primarily affect applications that are using IE to parse incoming HTML data. The glitch, identified by Microsoft as (MS01-020), could potentially allow malicious users to access and run programs on users of the 5.01 and 5.5 browser. Reportedly, the glitch causes IE to automatically open specially-coded attachments in an e-mail without warning, possibly unleashing programs that could do anything from sending other users a message to deleting files from users computers, according to Microsoft. For example, if an attacker created a HTML e-mail containing an executable attachment, then modified the MIME header to indicate a type that IE handles incorrectly, then the attachment will be allowed to execute without the usual "save to disk" or "open" warning messages. Microsoft was quoted as saying, "This vulnerability could enable an attacker to potentially run a program of her choice on the machine of another user. Such a program would be capable of taking any action that the user himself could take on his machine, including adding, changing or deleting data, communicating with web sites, or reformatting the hard drive." [viii] This flaw, according to Microsoft's security group, is contained in "a few" out of several hundred Multipurpose Internet Mail Extensions, or MIMEs, which are used to encode files as e-mail attachments.[ix] An impractical solution to this would be to simply disable downloads under the "security/ trust zones" section of IE. Microsoft released a patch for this problem within a week of its publication (be aware that at as of this writing, there were issues with the initial patch issued). If a company were not actively monitoring security issues, they would have no knowledge of this weakness.

The next vulnerability, affecting IE 5.0 and up, was discovered within two weeks of the above security risk. It could lead to the disclosure of sensitive information and may assist in future attacks against the victim, if successfully exploited. One of the ways to submit information to external websites is through the INPUT type form options. Users can upload files to remote webservers with the input type=FILE option. Due to a design error in the INPUT TYPE=FILE variable, it is possible for a website operator to specify a known filename from the visitors

machine for upload to the website.

This vulnerability is only exploitable under certain circumstances. The filename would have to be known by the website operator, the amount of characters that exist in the filename would have to be the same amount of characters the user typed in the form, and the visiting user would need to have at least read access to the known file (which they most likely would on their own machine). This vulnerability did not appear to allow the website operator to delete or modify any files on the visitor's machine.[x] Within a week of identifying this vulnerability, a patch was made available from Microsoft for those who were aware of the weakness.

Lastly is a recent vulnerability that could enable a remote (probably hostile) user to invoke telnet on the client (browser) and execute arbitrary commands on a target machine via IE. This is primarily due to services for Unix 2.0 containing a client side logging option which records all information that is exchanged during a telnet session. It is exploited by crafting a URL composed of command line parameters (telnet:-f%20\file.txt%20host) to the telnet client, which would invoke 'telnet.exe'. Telnet would then connect to the host and initiate the logging of session information. Access to this file will allow an attacker to write and execute arbitrary commands that may also be executed later.[xi] Again, for those actively monitoring security issues, a patch was issued shortly after the publication of the vulnerability.

The importance of having an active security awareness program cannot be understated. The vulnerabilities identified above were merely identified a few months time. A brief glance at any reputable security site will identify many, many more vulnerabilities. A procedure should be developed and implemented to review CERT and other vendor advisories for new security exposures within the company's environment, including IE, on a proactive basis. Examples of some of these sites include:

http://www.cert.org
http://www.securityfocus.com
http://sans.org
http://microsoft.com/security

This security awareness program should also include coordination with vendors and service providers to insure that the company's infrastructure is adequately secured and risks related to known security vulnerabilities are mitigated.

Microsoft's Internet Explorer is the most popular browser today and will continue to grow in popularity as it appears that, barring a surprising court order, it will continue to be integrated with all future Microsoft product suites. As with any software product, it is important to properly configure the technical aspects, in accordance with all the security features available.

However, as it has been discussed here, if a company does not have the proper policies and procedures in place, no amount of technical wizardry can alleviate the risk to what may have appeared to be a technically "secure" environment.

LIST OF REFERENCES

[i] Nua Internet Surveys. "What browser are they using?" March 2000. URL: http://www.dreamink.com/design5.shtml (2 April 2001)
[ii] Baldas, Tresa. "Who's watching while you web wander?" 20 April 2000. URL: http://knowledgespace.arthurandersen.com/InternalAudit/ (2 April 2001)
[iii] Microsoft."The MS Internet Security Framework." 3 June 1996. URL: http://www.microsoft.com/technet/index/defaultHome.asp?url=/technet/security/prodtech.asp (2 April 2001)
[iv] Microsoft."The MS Internet Security Framework." 3 June 1996. URL: http://www.microsoft.com/technet/index/defaultHome.asp?url=/technet/security/prodtech.asp (2 April 2001)
[v] Schnoll, Scott."Safety and security on the Internet." 2000. URL: http://www.nwnetworks.com/sands.htm (2 April 2001)
[vi] Not available."Microsoft Announces New Cookie-Management Features to Help Consumers Protect Privacy Online." 20 July 2000. URL: http://www.microsoft.com/presspass/features/2000/jul00/07-20cookies.asp (3 April 2001)
[vii] Chidi Jr, George A. "Microsoft Beefs Up IE's Security." 21 March 2001. URL: http://www.pcworld.com/news/article/0,aid,45162,00.asp (3 April 2001)
[viii] Leyden, John."Lookout for Internet Explorer Bugs." 30 March 2001. URL: http://www.theregister.co.uk/content/8/17990.html (3 April 2001)
[ix] Not Available." Security defect found in Internet explorer browser 5.01 and 5.5." 02 April 2001. URL: http://www.accountingweb.com/cgi-bin/item.cgi?id=42882 (3 April 2001)
[x] Williamson, David."Microsoft Internet Explorer 'Input Type=File' Vulnerability." Unknown. URL: http://www.403-security.org/cgi-bin/news403/viewnews.cgi?newsid976013072,78957 (4 April 2001)
[xi] Friedrichs, Oliver."Microsoft IE Telnet Client File Overwrite Vulnerability." 19 March 2001. URL: http://www.securityfocus.com/vdb/bottom.html?vid=2463 (4 April 2001)