Global Information Assurance Certification Paper

Microsoft Internet Explorer Web Browser: Pandora's Box of Attack Vectors

Abstract: The rise of internet usage among home and corporate users has lead to many new attacks that are propagated using the victim's web browser. These browser attacks can be anything from malicious code to privacy violations, and are becoming difficult to prevent. The widespread use of Internet Explorer leverages a common, well known code base with a mix of users content to stay within the default, insecure settings. Combine this with the marriage of the browser to the operating system, and the result is a miasma of security flaws, with an almost endless string of possible attacks. This paper explains just a few of the attacks and their theory, and explains how to best defend against them.

The World Wide Web (WWW, the Web) is, in it's barest form, a method for creating linked text. As the popularity of the Internet increased, web browsing has become the primary method for people to use Internet resources, and accounts for most of the traffic on the Internet today. The rise in popularity of the web has fueled a rise in the complexity of web pages. Active content, scripting, Flash animations, and Java applets are the norm for any well designed site. The black hat community hasn't been far behind, and every week brings new browser-based attack vectors. From manipulated MIME types to annoying scripting, the attacks can be harmless or can wipe out a system. A good study of these types of attacks is found in the O'Reilly book "Malicious Mobile Code" (see http://www.oreilly.com/catalog/malmobcode/index.html). It is important to look at why these types of attacks are successful, and what makes them so difficult to stop.

The internet was designed to be open, and was built on a trust model. Security was second to convenience. As the system scaled up, security could not keep pace with the newest technologies. Recent advances in browsers, scripting languages and applets have kept up the trend of convenience over security; Microsoft's marriage of the web browser to the operating system is the most obvious example. In an attempt to tie everything to the core OS, Microsoft opened a Pandora's box of attack vectors, leaving end users with a choice of either limited functionality (by disabling the "bells and whistles" that many sites depend on) or limited security. Internet Explorer includes security settings that allow the end user to make a few adjustments to browser behavior (see http://support.microsoft.com/default.aspx?scid=kb;EN-US;q174360 which describes how to use the security "zone" settings). This can include disabling scripting and active content, refusing cookies, and not accepting applets based on signature and trust level. The settings are, at best, confusing for the average home user. At worst, the end user may be given a false sense of security, believing that their browser is not going to allow malicious code to affect their system. A quick look at the NTBugTraq archives (http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A1=ind0111&L=ntbugtraq) will reveal the flaw in this thinking. The NTBugTraq list server was created for security conscious members of the Internet community to discuss security flaws in Microsoft operating systems. Lately, the discussion has been centering

around IIS (Internet Information Server, the web server on Microsoft server platforms) and Internet Explorer-based vulnerabilities.

The latest strain of attacks includes some theoretical attack methods based on the MIME type handling of the browser. MIME stands for Multi-purpose Internet Mail Extensions, and as the name implies is an extension of the original Internet email protocol (see http://www.webopedia.com/TERM/M/MIME.html for a complete definition). MIME objects are "embedded" in a web page, and the server tells the browser (via a tag or a document header) what MIME type is being served. Each browser includes a set of instructions (user settable) that point the browser to the appropriate response for a given MIME type. In the case of a .WAV audio file, the MIME type is identified as "x-audio\wav" for the object. This type is looked up by the browser, and is then handed off to the appropriate handler (in this case, on a Windows machine, it is handed off to Microsoft's media player). There are some default behaviors that Microsoft's Internet Explorer exhibits, in the guise of "ease of use." This includes default methods for handling known MIME types, such as email messages. In one of the simplest forms of a MIME type attack, Juan Carlos Cuartango found that some versions of Internet Explorer would allow a malicious "cut and paste" operation, which enabled the attacker to steal data from the system as long as the data was in a known location (such as the SAM, or password files from an NT machine). In the Cuartango version of what came to be known as an Untrusted Scripted Paste attack, an email message was sent formatted in HTML. This message is parsed by the HTML handler (Internet Explorer) which allowed the malicious code to perform cut and paste operations with data from the "local" or "intranet" zone, rather than passing it thru the more stringent "Internet Zone" security rules. Thus it was possible to get any information from the victim machine, and execute other malicious code. For a more detailed explanation of the early forms of the attack, see http://archives.indenial.com/hypermail/ntbugtraq/1998/October1998/0008.html. An interesting side effect to this was that many users of Microsoft's browsers tried to patch their installations, only to have the patch engine tell them that the update was not needed. The resulting confusion (see http://www.wired.com/news/technology/0,1282,42771,00.html, a Wired article titled "A Glitch in the Patch") led many users to leave their browsers insecure.

Microsoft released a patch for this flaw, but others are being found on a regular basis. Some of the latest include "extension spoofing." Nothing in the browser will "check" to make sure the MIME type tag matches the payload. Most browsers use the document's Content Type header to determine which application will be best suited to interpret the document. In some specific cases, Internet Explorer will use the 3 letter file extension to determine which application to use. In these cases (easy enough for the black hat to reproduce), Internet Explorer simply runs the application or script regardless of the security "zone" setting, since these settings seem to apply more to the Content Type header. Even if the file in question is not run, the user will be given the option to Open or Save the file. This type of attack is gaining much discussion on popular web logs such as Slashdot (see http://slashdot.org/article.pl?sid=01/12/11/2125224, an

article titled “Another Gaping Microsoft Security Hole Goes Unpatched”), and has some members of the security community rightfully frightened. In one attack, the user’s browser is handed a MIME type of "text/html", but the page contains an embedded .eml file which is downloaded and opened by Outlook Express. Outlook Express then parses an embedded .vbs (vbscript) file in the .eml message, (in some cases the user is prompted to either Open or Save the object, depending on version and patch level). The attacker is depending on the user to run the object, and has given instructions on the malicious web site to that effect. Once the program is run, a trojan is put in place, and the user’s machine is compromised.
Utilizing this inherent behavior maliciously is both easy to do and frustratingly difficult to detect (thankfully, Microsoft created a patch for this flaw while this text was being prepared, see http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-058.asp for the patch and information about what it fixes).

These attacks depend on several things. First and foremost, they depend on the user to be unaware of the malicious intent of the payload. Second, they depend on un-patched systems, as patches are created regularly by the vendor. Third, they rely on anti-virus software being either out-of-date or nonexistent (and some work around this by presenting scripting that most anti-virus programs will not catch). This may seem like a lot of dependencies, but most attacks rely on the end user being the weak link. Users look for convenience, functionality, and assume a lot of trust. The psychology involved with browser attacks is simple: make the payload seem either necessary or worthwhile. While more users are aware of browser related security flaws, the majority will accept content from any site, regardless. This leads to the possibility of creating an entire site (hanging off a DSL connection, for instance) that appears to be a legitimate source of information or entertainment, but in actuality is used as a delivery point of malicious code.

Malicious MIME types are just one of the attack vectors that attackers have concentrated on recently. Other attacks involve a wider scope of working around the default “security zone” settings in IE. Security zones are defined by the user (though defaults exist), and can be customized to disallow the parsing of any scripts or executables within a web site. This limits the functionality of most sites, but is flexible enough to correctly handle the majority of sites by placing them in the “Internet Zone,” a by default “medium” security setting that gives the user “safe browsing” but remains “functional” (Microsoft’s words). Unsigned ActiveX (scripts and applets) are not allowed, and the user is prompted before downloading potentially inappropriate content. The default setting for the “local zone” is “medium,” as well, but allows content to be saved or opened without prompting, and assumes trust from the (assumed intranet) site. There is a flaw, however: using malformed dotless IP numbering as the URL, the browser can be fooled into accepting content from an Internet site as if it were in an Intranet “local zone.” This allows the malicious site to automatically download applets and run them, a very bad thing. A “dotless IP address” relies on the browser openly accepting any type of information as a URL. The URL field will accept

names, IP addresses, or addresses that are numerically the same as the IP address but formed with any 32 bit number instead of dotted-quad. In the case of a dotless IP address, the IP address 207.46.131.13 would be entered into the browser as 031713501415. The browser then applies the security zone settings to the address, and does not read the dotless IP as an Internet address. Rather, it is read as a local, Intranet address, which bypasses the security zone settings. Since the default security zone setting for Intranets allows unsigned applets to be run, the malicious user can embed an application that would normally not be run by the browser. The application is silently run, and the user's machine is compromised. For a complete description of this flaw, see http://www.estreet.com/escihome2/support/WindowsArticles/WhataboutttheInternetExplo.html. Thought he flaw has been patched by Microsoft, the attack shows how obscure some of the settings are with regards to security "zones," and how a user can have a false sense of security with properly configured "zones."

There are also ways in which secure sessions can be hijacked (or at least compromised). A recent NTBugTraq post by Stephen Thair (see message titled "ASP Session ID's, SSL and a potential major security hole," December 2001 NTBugTraq archives) proposes a theoretical attack based on the use of session IDs for state information on an IIS server. The method that IIS uses to attach session IDs to Active Server Pages has two flaws. One is that an Active Server Page (ASP) SessionID is created by the system no matter what (even if the ASP specifically sets this session state to "false"). The second is that this same ASP session ID is shared by both http and https (secure http) connections. This means that the ASP session ID may be sent in clear text over the wire, resulting in the possibility of the Session ID being stolen. With this session ID and some creative Initial Sequence Number guessing, the session can be hijacked. However (and far more easy), the use of an improperly configured caching proxy server can lead to the session being "shared" by two different source IPs. If the malicious user hits the same URL (at the same time) as the legitimate user, the session ID cookie may get sent back to both of the users, allowing the malicious user access to the secure session. This example can occur with any browser that accepts and parses Active Server Pages and session cookies.

Finally, there is the "X factor," a term used to describe the unknown attack. As this is being written, several theoretical attacks based on MIME type handling and bypassing of Internet Explorer security zones are being worked on by several groups. While these groups are "gray hats," and report their findings to NTBugTraq (and other listservs), the attacks they demonstrate are often already in use by the time news reaches the Infosec community. The latest versions of Internet Explorer have proven just as susceptible to attacks from known methods (see http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-058.asp with information about a new patch and the old Frame Domain Verification flaw seen in security bulletin MS01-015), leading the informed Infosec person to believe that past patches and fixes aren't being engineered into new products. Newer methods will probably involve properly signed applets using faked Verisign-type certificates; one such certificate was recently granted

to an unknown entity with the title “Dell Software,” someone posing as Dell Computer Corp. Though the certificates were revoked, malicious coders will find another way. In the early days of L0pht Heavy Industries (a gray hat group that became @stake, http://www.@stake.com), the tagline was “Making the Theoretical Practical Since 1992.” This same credo is carried on by many in the black hat community.

Less malicious uses of the Internet trust model include attempts by marketing firms to gather data about browsing habits and ad penetration. The most obvious (and most vilified in some circles) example was the Comet Cursor, used by some web sites unintentionally as a means of making their site more aesthetically pleasing. The Comet Cursor was a signed applet that would install a small program that changed the mouse cursor to a comet at certain participating sites, which hardly seems malicious. In fact, the program also installed another applet that tracked web site usage and user profiles based on a unique identifier. There is an excellent article describing it’s almost virus like behavior at ZDNet, http://www.zdnet.com/anchordesk/stories/story/0,10738,2677247,00.html. This abuse of trust is just one of many similar schemes that can be found with enough browsing. While the end result isn’t necessarily as “evil” as a malicious trojan, the fact is that an abuse of trust occurs, and the user is duped into running a “spyware” program. In this model, and with this thinking, a similar piece of software could be created with malicious intent, connecting and uploading a user’s sensitive files at will.

What does this all mean, then, to the end user? Current security for home and small office users is minimal at best. Oftentimes, broadband connections are in place without any filtering at all. Even in cases where NAT is being used in combination with packet filtering, the traffic used to carry out these attacks is legitimate browser traffic, and would have to be handled by a stateful packet filtering mechanism (with a MIME type filter, such as MIMESweeper http://www.mimesweeper.com/default.asp) to truly be protected. The home and small office user is left, then, with two realistic choices: get rid of Internet Explorer, and install a personal firewall such as ZoneAlarm. The former is a difficult decision to make, since Internet Explorer works quite well and is free, already installed, and pre-configured. Alternatives exist, however, and it is important to communicate those alternatives to the home user. The latter step, installing a personal firewall, is quick, easy and free in many cases. Most offer easy setup of filters, and can alert the end user if a trojan or other malicious coding attempts to open a network session. Zone Alarm (from ZoneLabs, http://www.zonelabs.com/download/index.html) is free for personal use (though a fully supported, feature rich version is available for a small price as well) and endorsed by many in the security community. At a minimum, until Microsoft isolates the browser from the OS (something that is not likely to occur), the home and small office user should be patching their browser software regularly, at least as often as their anti-virus software (which is now a twice-weekly task). New patches are constantly available, and newer versions of Microsoft’s operating systems include the ability to automatically download and install these updates

as needed. This is the default setting for Windows XP's update engine, which is a good start. In the enterprise, all of the above plus a properly configured stateful firewall in combination with egress routing, packet filtering, and automatic updates (including an automatic "high security" setting for the Internet "zone") should be the rule. Defense in depth, as always, is the best defense.

References:

1) O'Reilly's page for "Malicious Mobile Code" by Roger A. Grimes http://www.oreilly.com/catalog/malmobcode/index.html
2) Microsoft support site with information on Internet Explorer security zone settings http://support.microsoft.com/default.aspx?scid=kb;EN-US;q174360
3) Index of archives at NTBugTraq http://www.ntbugtraq.com/default.asp?pid=36&sid=1&A1=ind0111&L=ntbugtraq
4) WebOPedia MIME definition http://www.webopedia.com/TERM/M/MIME.html
5) NTBugTraq archived message concerning Cuartango hole http://archives.indenial.com/hypermail/ntbugtraq/1998/October1998/0008.html
6) "A Glitch in the Patch," by Michelle Delio, Wired Online, April 2nd, 2001 http://www.wired.com/news/technology/0,1282,42771,00.html
7) "Another Gaping Microsoft Security Hole Goes Unpatched" by user michael, with discussion thread, December 11th, 2001.http://slashdot.org/article.pl?sid=01/12/11/2125224
8) Latest Microsoft security patch and bulletin for Internet Explorer, December13th,2001.http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-058.asp
9) "The mystery of Comet Cursor: How it got on my PC (yours too)" by David Coursey at ZDNet, January 23rd, 2001. http://www.zdnet.com/anchordesk/stories/story/0,10738,2677247,00.html
10) MIMESweeper general information http://www.mimesweeper.com/default.asp
11) ZoneAlarm download site and information http://www.zonelabs.com/download/index.html

General Resources:

1) NTBugTraq and the NTBugTraq mailing list, http://www.ntbugtraq.com
2) Security Focus (for general background), http://www.securityfocus.com
3) ZDNet news archives, http://www.zdnet.com
4) CNet news archives, http://www.cnet.com
5) Wired, http://www.wired.com
6) Microsoft, http://www.microsoft.com
7) EStreet, http://www.estreet.com
8) Slashdot (background and discussion), http://slashdot.org

Alternative Web Browsers:

1) Mozilla, an open source web browser developed on Netscape code is available for free at http://www.mozilla.org
2) Opera, a closed source commercial browser, has a freeware version (with banner ads) and is noted for it's speed and security (many customizations to the MIME handlers, cookie handling, and scripting, among other enhancements). It is available at http://www.opera.com
3) Netscape is freely available at http://www.netscape.com
4) If you don't like graphics, try Lynx. Text based, runs on DOS or Win32 platforms. http://www.fdisk.com/doslynx/lynxport.htm is a good place to start.

Last Updated: September 21st, 2017

Upcoming Training

Community SANS New York SEC401*	New York, NY	Sep 25, 2017 - Sep 30, 2017	Community SANS
Rocky Mountain Fall 2017	Denver, CO	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Copenhagen 2017	Copenhagen, Denmark	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS Baltimore Fall 2017	Baltimore, MD	Sep 25, 2017 - Sep 30, 2017	Live Event
SANS DFIR Prague Summit & Training 2017	Prague, Czech Republic	Oct 02, 2017 - Oct 08, 2017	Live Event
Community SANS Sacramento SEC401	Sacramento, CA	Oct 02, 2017 - Oct 07, 2017	Community SANS
Mentor Session - SEC401	Minneapolis, MN	Oct 03, 2017 - Nov 14, 2017	Mentor
SANS October Singapore 2017	Singapore, Singapore	Oct 09, 2017 - Oct 28, 2017	Live Event
SANS Phoenix-Mesa 2017	Mesa, AZ	Oct 09, 2017 - Oct 14, 2017	Live Event
SANS Tysons Corner Fall 2017	McLean, VA	Oct 14, 2017 - Oct 21, 2017	Live Event
SANS Tokyo Autumn 2017	Tokyo, Japan	Oct 16, 2017 - Oct 28, 2017	Live Event
CCB Private SEC401 Oct 17	Brussels, Belgium	Oct 16, 2017 - Oct 21, 2017	
SANS vLive - SEC401: Security Essentials Bootcamp Style	SEC401 - 201710,	Oct 23, 2017 - Nov 29, 2017	vLive
Community SANS Omaha SEC401	Omaha, NE	Oct 23, 2017 - Oct 28, 2017	Community SANS
SANS Seattle 2017	Seattle, WA	Oct 30, 2017 - Nov 04, 2017	Live Event
San Diego Fall 2017 - SEC401: Security Essentials Bootcamp Style	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	vLive
SANS San Diego 2017	San Diego, CA	Oct 30, 2017 - Nov 04, 2017	Live Event
SANS Gulf Region 2017	Dubai, United Arab Emirates	Nov 04, 2017 - Nov 16, 2017	Live Event
Community SANS Colorado Springs SEC401**	Colorado Springs, CO	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Miami 2017	Miami, FL	Nov 06, 2017 - Nov 11, 2017	Live Event
Community SANS Vancouver SEC401*	Vancouver, BC	Nov 06, 2017 - Nov 11, 2017	Community SANS
SANS Sydney 2017	Sydney, Australia	Nov 13, 2017 - Nov 25, 2017	Live Event
SANS Paris November 2017	Paris, France	Nov 13, 2017 - Nov 18, 2017	Live Event
SANS London November 2017	London, United Kingdom	Nov 27, 2017 - Dec 02, 2017	Live Event
SANS San Francisco Winter 2017	San Francisco, CA	Nov 27, 2017 - Dec 02, 2017	Live Event
Community SANS St. Louis SEC401	St Louis, MO	Nov 27, 2017 - Dec 02, 2017	Community SANS
Community SANS Portland SEC401	Portland, OR	Nov 27, 2017 - Dec 02, 2017	Community SANS
SANS Khobar 2017	Khobar, Saudi Arabia	Dec 02, 2017 - Dec 07, 2017	Live Event
SANS Austin Winter 2017	Austin, TX	Dec 04, 2017 - Dec 09, 2017	Live Event
Community SANS Ottawa SEC401	Ottawa, ON	Dec 04, 2017 - Dec 09, 2017	Community SANS
SANS Munich December 2017	Munich, Germany	Dec 04, 2017 - Dec 09, 2017	Live Event