Session 8

Securing Your Web Browser

This article will help you configure your web browser for safer Internet surfing. It is written for home computer users, students, small business workers, and any other person who works with limited information technology (IT) support and broadband. Although the information in this document may be applicable to users with formal IT support as well, organizational IT policies should supersede these recommendations. If you are responsible for IT policies for your organization, please consider implementing these recommendations as part of your policy.

Why Secure Your Browser

Today, web browsers such as Microsoft Internet Explorer, Mozilla Firefox, and Apple Safari are installed on almost all computers. Because web browsers are used so frequently, it is vital to configure them securely. Often, the web browser that comes with an operating system is not set up in a secure default configuration. Not securing your web browser can lead quickly to a variety of computer problems caused by anything from spyware being installed without your knowledge to intruders taking control of your computer.

Ideally, computer users should evaluate the risks from the software they use. Many computers are sold with software already loaded. Whether installed by a computer manufacturer, operating system maker, Internet service provider, or by a retail store, the first step in assessing the vulnerability of your computer is to find out what software is installed and how programs will interact with each other. Unfortunately, it is not practical for most people to perform this level of analysis.

There is an increasing threat from software attacks that take advantage of vulnerable web browsers. We have observed new software vulnerabilities being exploited and directed at web browsers through use of compromised or malicious websites. This problem is made worse by a number of factors, including the following:

- Many users have a tendency to click on links without considering the risks of their actions.
- Web page addresses can be disguised or take you to an unexpected site.
- Many web browsers are configured to provide increased functionality at the cost of decreased security.
- New security vulnerabilities are often discovered after the software is configured and packaged by the manufacturer.
- Computer systems and software packages may be bundled with additional software, which increases the number of vulnerabilities that may be attacked.
- Third-party software may not have a mechanism for receiving security updates.
- Many websites require that users enable certain features or install more software, putting the computer at additional risk.
- Many users do not know how to configure their web browsers securely.
- Many users are unwilling to enable or disable functionality as required to secure their web browser.

As a result, exploiting vulnerabilities in web browsers has become a popular way for attackers to compromise computer systems.

In addition to following this paper's recommendations, refer to the documentation in the References section for other steps you can take to secure your system.

Web Browser Features and Risks

It is important to understand the functionality and features of the web browser you use. Enabling some web browser features may lower security. Vendors often enable features by default to improve the computing experience, but these features may end up increasing the risk to the computer.

Attackers focus on exploiting client-side systems (your computer) through various vulnerabilities. They use these vulnerabilities to take control of your computer, steal your information, destroy your files, and use your computer to attack other computers. A low-cost method attackers use is to exploit vulnerabilities in web browsers. An attacker can create a malicious web page that will install Trojan software or spyware that will steal your information.

Additional information about spyware is available in the following document:
http://www.cert.org/archive/pdf/spyware2005.pdf.

Rather than actively targeting and attacking vulnerable systems, a malicious website can passively compromise systems as the site is visited. A malicious HTML document can also be emailed to victims. In these cases, the act of opening the email or attachment can compromise the system.

Some specific web browser features and associated risks are briefly described below. Understanding what different features do will help you understand how they affect your web browser's functionality and the security of your computer.

ActiveX is a technology used by Microsoft Internet Explorer on Microsoft Windows systems. ActiveX allows applications or parts of applications to be utilized by the web browser. A web page can use ActiveX components that may already reside on a Windows system, or a site may provide the component as a downloadable object. This gives extra functionality to traditional web browsing, but may also introduce more severe vulnerabilities if not properly implemented.

ActiveX has been plagued with various vulnerabilities and implementation issues. One problem with using ActiveX in a web browser is that it greatly increases the attack surface, or "attackability," of a system. Installing any Windows application introduces the possibility of new ActiveX controls being installed. Vulnerabilities in ActiveX objects may be exploited via Internet Explorer, even if the object was never designed to be used in a web browser (VU#680526). In 2000, the CERT/CC held a workshop to analyze security in ActiveX. The results from that workshop may be viewed at http://www.cert.org/reports/activeX_report.pdf. Many vulnerabilities with respect to ActiveX controls lead to severe impacts. Often an attacker can take control of the computer. You can search the Vulnerability Notes Database for ActiveX vulnerabilities at http://www.kb.cert.org/vuls/byid?searchview&query=activex.

Java is an object-oriented programming language that can be used to develop active content for websites. A Java Virtual Machine, or JVM, is used to execute the Java code, or "applet

," provided by the website. Some operating systems come with a JVM, while others require a JVM to be installed before Java can be used. Java applets are operating system independent.

Java applets usually execute within a "sandbox" where the interaction with the rest of the system is limited. However, various implementations of the JVM contain vulnerabilities that allow an applet to bypass these restrictions. Signed Java applets can also bypass sandbox restrictions, but they generally prompt the user before they can execute. You can search the Vulnerability Notes Database for Java vulnerabilities at http://www.kb.cert.org/vuls/byid?searchview&query=java.

Plug-ins are applications intended for use in the web browser. Netscape has developed the NPAPI standard for developing plug-ins, but this standard is used by multiple web browsers, including Mozilla Firefox and Safari. Plug-ins are similar to ActiveX controls but cannot be executed outside of a web browser. Adobe Flash is an example of an application that is available as a plug-in.

Plug-ins can contain programming flaws such as buffer overflows, or they may contain design flaws such as cross-domain violations, which arises when the same origin policy is not followed.

Cookies are files placed on your system to store data for specific websites. A cookie can contain any information that a website is designed to place in it. Cookies may contain information about the sites you visited, or may even contain credentials for accessing the site. Cookies are designed to be readable only by the website that created the cookie. Session cookies are cleared when the browser is closed, and persistent cookies will remain on the computer until the specified expiration date is reached.

Cookies can be used to uniquely identify visitors of a website, which some people consider a violation of privacy. If a website uses cookies for authentication, then an attacker may be able to acquire unauthorized access to that site by obtaining the cookie. Persistent cookies pose a higher risk than session cookies because they remain on the computer longer.

JavaScript, also known as ECMAScript, is a scripting language that is used to make websites more interactive. There are specifications in the JavaScript standard that restrict certain features such as accessing local files.

VBScript is another scripting language that is unique to Microsoft Windows Internet Explorer. VBScript is similar to JavaScript, but it is not as widely used in websites because of limited compatibility with other browsers.

The ability to run a scripting language such as JavaScript or VBScript allows web page authors to add a significant number of features and interactivity to a web page. However, this same capability can be abused by attackers. The default configuration for most web browsers enables scripting support, which can introduce multiple vulnerabilities, such as the following:

- **Cross-Site Scripting**

Cross-Site Scripting, often referred to as XSS, is a vulnerability in a website that permits an attacker to leverage the trust relationship that you have with that site. For a high-level description of XSS attacks, please see the whitepaper published at http://www.cert.org/archive/pdf/cross_site_scripting.pdf. Note that Cross-Site Scripting is not usually caused by a failure in the web browser. You can search the Vulnerability Notes Database for Cross-Site Scripting vulnerabilities at http://www.kb.cert.org/vuls/byid?searchview&query=cross-site+scripting.

- **Cross-Zone and Cross-Domain Vulnerabilities**

  Most web browsers employ security models to prevent script in a website from accessing data in a different domain. These security models are primarily based on the Netscape Same Origin Policy: http://www.mozilla.org/projects/security/components/same-origin.html. Internet Explorer also has a policy to enforce security zone separation.

  Vulnerabilities that violate these security models can be used to perform actions that a site could not normally perform. The impact can be similar to a cross-site scripting vulnerability. However, if a vulnerability allows for an attacker to cross into the local machine zone or other protected areas, the attacker may be able to execute arbitrary commands on the vulnerable system. You can search the Vulnerability Notes Database for cross-zone and cross-domain vulnerabilities at http://www.kb.cert.org/vuls/byid?searchview&query=cross-domain.

- **Detection Evasion**

  Anti-virus, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) generally work by looking for specific patterns in content. If a “known bad” pattern is detected, then the appropriate actions can take place to protect the user. However, because of the dynamic nature of programming languages, scripting in web pages can be used to evade such protective systems.

How to Secure Your Web Browser

Some software features that provide functionality to a web browser, such as ActiveX, Java, Scripting (JavaScript, VBScript, etc.), may also introduce vulnerabilities to the computer system. These vulnerabilities may stem from poor implementation, poor design, or an insecure configuration. For these reasons, you should understand which browsers support which features and the risks they could introduce. Some web browsers permit you to fully disable the use of these technologies, while others may permit you to enable features on a per-site basis.

This section provides links that show you how to securely configure a few of the most popular web browsers and how to disable features that can cause vulnerabilities. We encourage you to visit the vendor's website for each browser you use to learn more. If a vendor does not provide documentation on how to secure the browser, we encourage you to contact the vendor and request more information.

Multiple web browsers may be installed on your computer. Other software applications on your computer, such as email clients or document viewers, may use a different browser than the one you normally use to access the web. Also, certain file types may be configured to open with a different web browser. Using one web browser to manually interact with websites does not mean other applications will automatically use the same browser. For this reason, it is important to securely configure each web browser that may be installed on your computer. One advantage to having multiple web browsers is that one browser can be used for only sensitive activities such as online banking, and the other can be used for general purpose web browsing. Using multiple browsers can minimize the chances that a vulnerability in a particular web browser, website, or related software can be used to compromise sensitive information.

Web browsers are frequently updated. Depending on the version of your software, the features and options may move or change.

Microsoft Internet Explorer

Microsoft Internet Explorer (IE) is a web browser integrated into the Microsoft Windows operating system. For up-to-date information on security and privacy settings for Internet Explorer, visit http://windows.microsoft.com/en-us/internet-explorer/ie-security-privacy-settings

Mozilla Firefox

Mozilla Firefox is a popular third-party browser for Windows, Mac, and Linux. To learn how to keep your information safe and secure with Firefox's private browsing, password features and other security settings, visit https://support.mozilla.org/en-US/products/firefox/privacy-and-security.

Apple Safari

Apple Safari is installed on its line of computers, tables, and phones. For information on the Safari's security settings on Apple devices, visit https://support.apple.com/en-us/HT201265. For information on Safari installed on computers, visit http://help.apple.com/safari/mac/8.0/ and select "Privacy and security" on the menu.

Google Chrome

In 2012, Google Chrome became the most widely used browser worldwide, according to Stat Counter and other sources. For more information on Chrome's security, safety and reporting features, visit https://support.google.com/chrome#topic=3421433 and select the options displayed under the topic.

Other Browsers

Other web browsers may have similar options to those described above. Please refer to each browser's documentation to determine which options are available and how to make the necessary changes. For example, the links below show where to find security information for two other web browsers:

- Opera
    - Security badges: http://help.opera.com/opera/Windows/1857/en/private.html#badges
    - Web preferences: http://help.opera.com/opera/Windows/1857/en/controlPages.html#content

- Chromium
    - Security information: https://www.chromium.org/Home/chromium-security

Keeping Your Computer Secure

In addition to selecting and securing your web browser, you can take measures to increase protection to your computer in general. The following are steps and links to information resources that will help you secure your computer.

A. Read the Home Network Security document

B. Enable automatic software updates if available

Vendors will usually release patches for their software when a vulnerability has been discovered. Most product documentation offers a method to get updates and patches. You should be able to obtain updates from the vendor's website. Read the manuals or browse the vendor's website for more information.

Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's website for information about automatic notification. If no mailing list or other automated notification mechanism is offered, you may need to check the vendor's website periodically for updates.

C. Install and use antivirus software

While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks. Many antivirus packages support automatic updates of virus definitions. We recommend using these automatic updates when available. A list of virus basics is available on the CERT/CC website.

D. Avoid unsafe behavior

Additional information on this topic can be found in the Home Network Security document.

- Use caution when opening email attachments or when using peer-to-peerfile sharing, instant messaging, or chat rooms.
- Don't enable file sharing on network interfaces exposed directly to the Internet.

E. Follow the principle of least privilege — don't enable it if you don't need it

Consider creating and using an account with limited privileges instead of an 'administrator' or 'root' level account for everyday tasks. Depending on the operating system, you only need to use administrator level access when installing new software, changing system configurations, etc. Many vulnerability exploits (e.g., viruses, Trojan horses) are executed with the privileges of the user that runs them — making it far riskier to be logged in as an administrator all the time.