UNIVERSITY OF RWANDA

NATIONAL POLICE COLLAGE

WEB SECURITY

TPOIC: How Web Browser works in terms of Security?

Presenter:

NDAYISHIMIYE LEON Pierre

220000862

Done 15 oct 2022

INTRODUCTION

Web browser security consists of all measures, procedures, and policies necessary to protect users accessing the Internet from a web browser application.

Almost everyone who is online has a web browser available on their computer or mobile device. Since it is so common, hackers and other cybercriminals prefer to launch compromising attacks on this client-side application.

A web browser can store information for your convenience, but others may eventually access the information. Therefore, it provides a large surface area for exposure to email accounts, usernames, all sorts of passwords, and personal or corporate information. Attackers often target the web browser to hijack or sniff on the web traffic from it. They may also use it as a means to access the device itself or any files available on it.

1. **How Attackers Target the Browser**

The web browser can display text documents, play multimedia files, and allow users to play games or interact with forms and all other content on the Internet.

The versatility of the web browser is good, but this also makes it more challenging to secure since there are more "weak points" an attacker could exploit. The most vulnerable parts of a web browser are as follows:

1. **Connections to DNS servers, websites, and other online resources**

A DNS server is the bridge between the browser and the content from any site. It points the browser to the correct website, and the site makes the appropriate content available to the browser.

Many attacks compromise and intercept this communication, and it can occur at one of several points. The goal is often to redirect the browser to a malicious website, where the browser (and by implication, the user) encounters driveby downloads, exploit kits, and unwanted content.

2. Browser plugins

Browsers are frameworks on which users can install third-party tools to be more comprehensive. However, such plugins may contain vulnerabilities that cyberattacks can exploit to snoop on the browser's web traffic, hijack it, and install malware or carry out harmful actions on the device. Finance-related data is lucrative for such browser attacks.

3. Browser-specific vulnerabilities

Flaws in a browser can enable attackers to sniff sensitive data passing through the web browser, such as when the user fills web forms. These flaws may also give criminal elements unwarranted access to devices.

2. How to Improve Web Browser Security

In computing circles, this is also called "hardening the browser" by taking measures to improve security and prevent attacks. Note that it's nearly impossible to achieve 100% impenetrability, but attackers will have a much harder time succeeding.

1. Use the latest web browser version

Users should get the latest updates of their web browser software. Vendors often release updates of their browsers, adding new functionality or improving existing features. The most critical security features include:

Anti-phishing: Assess and filter suspicious links in search results or on a webpage.
Anti-malware: Scan and block downloading of suspicious files.
Plugin security: Analyse and block insecure plugins.
Sandbox: Build a fence around web browser processes to prevent access to the operating system. A few browsers include an auto-update function, notifying the user of updates.

2. Restrict user access

It is advisable to use the web browser from a limited user account without administrator privileges. It limits the ability of any malware that succeeds in infecting the machine to have little to no room to operate within the machine.

3. Use custom security settings

Even though the controls differ, modern browsers often allow some customisation of security-related settings. The recommendation is to set the following settings as high as possible:

Block fake sites: Always enable this feature to prevent unplanned visits to malicious websites.

Camera & Microphone: These should never run automatically. The browser should confirm if the user wants to use the camera or microphone at any time.

Cookies: Completely disable cookies. Users should only enable cookies if a trusted site needs them.

JavaScript: Same rule as for cookies.

Plugins/Add-ons: Same rule as for cookies and JavaScript

Pop-up windows: Same rule as for cookies, JavaScript, and Plugins/Add-ons.

4. Only include plugins that improve security or those you will use

The best thing users can do with plugins is to remove them if they are not using them regularly. With a few clicks, it is easy to re-enable or re-install them when needed. The advantage of removing them is that they can minimise potential points for compromise.

Some plugins improve web browser security. Security professionals recommend the following for all browsers:

Flashblock: This add-on will prevent Flash ads from playing until the user opts to allow them.

HTTPS Everywhere: This plugin encrypts a user's web browsing traffic. It is the result of a joint effort by the Electronic Frontier Foundation and The Tor Project.

NoScript or ScriptSafe: These programs are popular and block scripts on websites unless the user explicitly accepts to run them. The US-CERT specifically recommends NoScript.

5. Other steps users can take to harden the browser

All of these actions focus on manipulating the browser to be more secure. It is also advisable to add another layer of security such as implementing firewalls, installing antivirus software, and avoiding unsafe behaviour, the Home Network Security Incident document outlines.

3. Using Multiple Browsers

A user may install multiple web browsers as a way to improve security. Document viewers and email clients may use another browser or offer various functionalities depending on the browser in use. Specific browsers may be necessary to open certain file types. The point is that one web browser will not necessarily fit all of a user's applications and purposes.

It is therefore essential to securely configure each web browser available on a computer. There is a distinctive advantage in dedicating one web browser for sensitive activities such as online banking while dedicating another for general-purpose web browsing.

The use of multiple browsers greatly minimises the probability of compromising sensitive information in a specific browser, website, or software.

Improving internet security for web browsers will protect networked data and computer devices from malware or privacy breaches.