Web browser security: An overview

CANADIAN CENTRE FOR CYBER SECURITY

October 2024 | ITSAP.40.017

Just about any computer device you use today has at least one web browser installed on it. Therefore, it is extremely important to make sure they are secure. Securing your browser involves not just configuring security settings, but also understanding the way certain web protocols work. By doing so, you can help keep your data and computer systems safe from threat actors. This publication highlights some key web protocols and how they are used to protect your personal information.

Communications protocols

Protocols are sets of rules that allow for multiple devices to communicate and transmit data with each other. These rules define the type of data that can be sent, the structure of the information, and how each device will receive it. There are many communications protocols in use today. Some common ones include:

- Transport Layer Security (TLS)
- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)

TLS certificate

TLS is a protocol that protects data that is sent over the Internet. TLS ensures that threat actors cannot see what you transmit, like your passwords or credit card numbers. TLS authenticates webservers via a certificate issued by a trusted entity called a certificate authority. The certificate binds a cryptographic key to the webserver's domain address. Using this cryptographic key, TLS employs encryption to ensure that data is transferred securely between the webserver and your browser.

HTTP

HTTP is used for transferring data over a network. HTTP does not provide any security. Therefore, your data is in plaintext and can be monitored at any point on the network transmission path between the webserver and the browser.

HTTPS

HTTPS uses TLS to encrypt the data sent and received on your network. When in use, HTTPS can appear as a lock icon at the beginning of the web browser address bar in some browsers.

HTTPS encrypts the content to ensure privacy and authenticates it so that it can not be modified. Even though HTTPS is more secure than HTTP, it can still be susceptible to adversary-in-the-middle (AitM) attacks.

TLS stripping is an AitM technique used by a malicious actor where secure HTTPS connections are converted to unsecured HTTP connections. Web browsers may warn users if HTTPS is rejected and downgraded to HTTP and give them the option to terminate the connection.

The presence of HTTPS itself isn't a guarantee that a site is legitimate. Sophisticated threat actors can spoof a website by fabricating the appearance of a secure site to trick you into entering personal information. Users are advised to carefully look at the web address to ensure it is the expected domain of the intended website

HSTS

HTTPS Strict Transport Security (HSTS) is a web security policy tool that forces the browser to load the secure version of a website, and ignores any attempted redirection to an unsecured HTTP website. HSTS is a server-side configuration. It can prevent TLS stripping.

Content Security Policy

Content Security Policy (CSP) is a widely supported web browser security standard that detects and lessens certain kinds of attacks, like cross-site scripting and code injection. These attacks can lead to data theft, website defacement or malware distribution.

To implement CSP, website developers make lists of approved origins for all of the content that a browser is allowed to load for a specific website. In other words, what content the browser can load and where the content can be loaded from. Content can include:

- JavaScript
- Cascading Style Sheets (CSS)
- HTML files
- Fonts
- Image, audio and video files

Tracking pixels

Tracking pixels are tiny images, 1x1 pixel in size that are embedded in the HTML of webpages, advertisements and emails. This tiny image is hosted on a server and collects information about the user when browsing the webpage. They are generally used by companies to enhance advertising efforts by gathering information about people's interests and habits to create targeted ads. Browser tracking pixels can do the following:

- Collect location information, like IP address
- Determine whether you have taken a certain action on a webpage, such as signing up for a mailing list
- Track pageviews, clicks, and redirects
- Determine user device type and operating system

One of the main issues with tracking pixels is privacy. They often collect data without the knowledge or consent of users and sending it back to their home server. Tracking pixels are also vulnerable to data leaks if the information is not correctly stripped of identifiable and personal information before it is transmitted back to the server. Webpages should disclose that they are using tracking pixels and provide the user the option to opt out. Please see the section below on extension and plug-ins for mitigation advice.

Communications Security Establishment Canada
Centre de la sécurité des télécommunications Canada

Cat no. D97-1/40-017-2024E-PDF

ISBN 978-0-660-73888-8

Canada

Cookies

Like tracking pixels, cookies also gather and store information about users and their habits online. This information is stored in the web browser file. Cookies can help improve user experience, such as remaining logged into a retailer to update items in your cart. They can also be used to enhance advertising efforts as they keep track of who visits a webpage, and how they are engaging with specific online content. Some cookies are necessary for website functionality as they help authenticate and manage the user's session. Other cookies can be deactivated by users such as advertising cookies. However, cookies can be vulnerable to poisoning or hacking. Threat actors can use cookies to impersonate users and steal sensitive information.

Best practices for tracking pixels and internet cookies

- Only allow necessary and functional cookies
- Perform regular malware scans

Web browser plug-ins and extensions

Many browser extensions and plug-ins claim to enhance privacy and cyber security. They can do things from blocking ads and managing passwords, to generating coupons when shopping online. They can allow the user to customize their browser experience in pretty much any way. New plug-ins and extensions are being created all the time. Some you can pay for, and some are free. Some are created by legitimate companies, and others are not. Extensions and plug-ins are given certain authorizations within the browser which can be exploited by threat actors. They can request permission to gather all information that the browser sees, including passwords and keystrokes. Some extensions can have malware secretly included in their code which could affect your device as soon as you download it. The fewer extensions you have on your device, the better.

Best practices for plug-ins and extensions

- Only download from trusted and official sites
- Review permissions before accepting
- Read reviews from other users before installing

Security settings for your web browser

Often the browser installed on your device operates using only the default security settings. To secure your browser, you should:

- block third-party cookies so as not to be traced
- block pop-ups
- perform automatic updates
- avoid saving any passwords within the browser itself
- allow java only when necessary

If you are setting up a website, we recommend that you:

- publish services using only HTTPS
- redirect users from the HTTP version of your services to the HTTPS option
- use the latest TLS software and patch it regularly
- activate HSTS to secure connections to your service

Security actions for your computer

Securing your computer goes hand in hand with securing your browser. Some simple actions you can take to secure your computer include:

- using strong and unique passwords for logins
- installing and running anti-virus and anti-malware software
- allowing automatic software updates when available
- adopting the principle of least privilege for your user accounts
- avoiding risky online behaviour
- backing-up your data regularly
- filtering URLs at your firewall

Web browser security recommendations for your organization

- Determine trusted and restricted sites
- Validate the reliability of ad blockers or third party plug-ins
- Check the permissions to determine the level of privilege
- Use a standard web browser across your organization
- Allow only functional cookies
- Educate staff about pop-ups, cookies, web browser vulnerabilities
- Update anti-malware software regularly and install a firewall
- Review peripheral devices for obsolete products regularly