Privacy and online tracking

Part 1

WebRTC IP Address Leakage

This constitutes different technologies that allow real-time communications between different browsers without installing any software extension. WebRTC is helpful in online activities like gaming, conferencing, and file sharing, and it is a potential security issue since it can reveal the IP addresses of devices.

WebRTC establishes a peer-to-peer communication framework between identities. The process reveals the entity's IP address even when the user has used internet proxies or VPN. This bypasses mechanisms and methods used by VPN and leaks the user's IP address.

The main concern with WebRTC is the undermining of user's privacy. Malicious people can use this technique to acquire the actual geographical location of the user and target them with region-specific content.

Canvas Fingerprinting

This tracking technique develops a unique identity of devices and browsers called fingerprints. It uses the canvas elements of HTML5 to draw animations and graphics within the browser.

When a website utilizes canvas fingering, it can tell the user's browser to draw patterns and images using the HTML5 canvas elements. The information is then used to develop fingerprints of devices and browsers. The data can include the type of browser used, operating system, graphics details, and screen resolutions.

The impact of canvas fingerprinting infringes on the user’s privacy without their knowledge. Hackers can persistently track users’ activities because fingerprints can stay longer than cookies. The site can then analyze the user’s interests, preferences, and behaviors without detection.

HTTP_ACCEPT Headers

HTTP_ACCEPT Headers are components of HTTP used for communication between servers and clients, and they display data accepted by the user’s browser, including UTF-8 characters, HTML, JavaScript, or CSS.

Hackers and malicious people use data on the content that the browser can accept to create a profile of a device and browser. For instance, hackers can identify user plugins, system fonts, languages, data formats, content encryption methods, and screen resolutions to create unique fingerprints for the target user.

Hackers can bypass privacy measures like IP masking or cookie blocking to track users’ content and create a precise browser profile for data analysis, advertisement, and personalized content.

Part 2

I have learned that different tracking techniques affect my online privacy and create personal insecurity issues. It is, therefore, essential to be cognizant of these tools and exploit ways to protect oneself from being persistently monitored and tracked.

A few actions are essential to protect oneself from the implications of the above threat.

- Use secure browsers like Brave with extensive built-in privacy configuration to protect against data collection and tracking. Always use a VPN to hide your IP address.
- Delete the browsing cache and cookies immediately after browsing to reduce the data exposure to tracking methods. Clearing data limits the information that tracking mechanisms collect and makes it difficult to link identifiable details successfully.
- Use browser plugins to stop any tracking and improve browsing privacy. Also, adjust browser settings to limit the data displayed in trackers, such as HTTP_ACCEPT headers.

References

Bernardo, V. M. G. (2015). *Device fingerprinting techniques: threats and protections* (Doctoral dissertation).

Jakobsson, C. (2015). Peer-to-peer communication in web browsers using WebRTC A detailed overview of WebRTC and what security and network concerns exists.