WEB BROWSER: DESIGN AND SECURITY ISSUES

Sarbjeet Singh
Assistant Professor, Computer Science and Applications, Guru Nanak College, Panjab University, Punjab, India
Email –rakeshuppal44@gmail.com

Abstract: *In the environment of internet, servers and clients communicate with each other with the help of protocols and internet by using some browser. The information that is exchanged with the client and server via browser and such information is very sensitive. This kind of sensitive information can be steal by attackers. There are lot of concerns related to the security of the browser because number of web attacks and frauds are increasing day by day. Due to the availability of the internet, attacker can access the addresses of the web users from anywhere. It is easy for them to upload malicious files on the internet. Attackers uses the automated tools that update the malicious files constantly. They use the internet for entering into personal systems of the web users by security loopholes. Sometimes user clicks on the link that he thinks that it is safe or not, sometimes user installs any free software and any browser extension but he is unaware from the security threats that may infect the user's system and steal the vital information from their systems. From the network security point of view the browser designers should design the browser in more secure way than existing browser design. Various constraints should add by the designers of the web browser for making the browsing experience more secure.*

Key Words: *Automated, Malicious, Extension , loopholes.*

1. INTRODUCTION:

Web browser starts communication with a website, then the information is collected related to the browser. There may be much vulnerability related to any particular browser that can permit any kind of malicious code to initiate the processes in unintended ways within the web browser. Once the malicious code run on the user's web browser then the attacker can easily get the privileged access to the user's system. In this way a attacker can easily enter into the client's system. There are so many security issues related to the browser and browsing experience. So, the design of the web browser should be such that it can handle various security attacks and provide the secure browsing experience.

2. BROWSER DESIGN ISSUES:

There are various issues related to the design of the web browser. Some of them are-:

- **Absence of security:** Most of the web browsers provide the unrestricted access to common implementation and context of the users that are running the web browsers .So, the level to security downs directly due to this .So it becomes easy for attackers to enter into the client's machine via web browser.
- **Inconsistent Practices for Storage:** For data storage, web browsers uses the storage in randomly and with random methods of keeping the various files like browsing history, downloads, temporary files, cookies, configuration data, entries of cache and records which are sensitive like passwords. Such kind of data may be stored in program installation folders, temporary directories, user home directories.
- **Programming languages:** Mostly the code of famous browsers like Chrome, Firefox, Opera, and Internet Explorer, is written using the programming languages like C++. For manipulations of image libraries the C language is used for programming to provide the high performance. All is depends upon designer to choice of C or C++ or both during the design of the web browser.
- **Inconsistent UI :** There is always some kinds of constant notifications and pop ups in the browser UI, Which makes the experience of browsing worst. So, these things should be reduced to provide the better experience to web browser user. Because, these UI related things makes the browsing experience inconsistent.
- **Web technologies:** Many popular browsers like chrome are developed using the web languages like HTML, XML and JavaScript for implementation of the web browsers. But such kind of web languages are also used by the attacker and hackers like HTML injection .So the choice of web technologies for browser implementation also increases the level of risks for browsing experience because same technologies are used by the attackers.

How Attackers work? : The basic things about phishers are:-

- They request clients to get their personal information via email by showing themselves as companies.

- They tries to convince the clients for any visiting any website by using emotional drama.
- Giving offers like free service or products by clicking on any particular link.
- Shows themselves as genuine banking site for requesting the information which is confidential

Phishers use these methods.

- Manipulation of Links is most common method that is used by the phishers for putting the clients in their trap by sending some email and showing them they are genuine or sometime uses trick of using domain name that looks similar to popular domains.
- Phishers use the commands in scripting languages to alter the address bar of browser and opens a different website instead of opening original website.

3. Desirable Design For Browser:

Sandboxes can be designed for the browsers where the browser run the code like as any flash content or JavaScript. In this way, the malicious code can be checked before it can harm the system of the computer user. Many browsers have own sandboxes. Such kind of sandboxes should be implemented for making the browsing experience more secure. Zone based security can also be implemented in the web browsers for enabling the security features depending upon the zone of website on which user visit. Protection mode can also be added in the browser where the user can on or off the protection mode depending upon his own requirement and content he is surfing.

4. Conclusion:

Browsers provide the path of browsing for clients. By using the browsers both client and server can communicate with each other. So, browser is like a heart of internet and browsing experience. So, browser designers should design the browser design in more secure ways to provide the best and secure browsing experience to the clients.

5. Acknowledgement:

During this research paper, I have put my best efforts for completing this research paper. I hope that this research paper will be helpful for the future authors who want to do further research related to browser security.

REFERENCES:

1. Maone, Giorgio. "NoScript :: Add-ons for Firefox". Mozilla Add-ons. Mozilla Foundation.
2. Skinner, Carrie-Ann. Opera Plugs "Severe" Browser Hole Archived 20 May 2009 at the Wayback Machine.
3. Smith, Dave. "The Yontoo Trojan: New Mac OS X Malware Infects Google Chrome, Firefox And Safari Browsers Via Adware". IBT Media Inc.
4. Goodin, Dan. "MySQL.com breach leaves visitors exposed to malware".
5. "Facebook privacy probed over 'like,' invitations". CBC News. 23 September 2010.