ORIGINAL RESEARCH PAPER

Computer Science

SECURITY THROUGH PUBLIC WEB-BROWSER WITH PRIVACY PRESERVING

KEY WORDS: security, web browser, extensions

Umma Khatuna Jannat Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, 641021, India.

Dr.M.Mohan Kumar Associate professor, Department of Computer Science, Karpagam Academy of Higher Education Coimbatore, 64102, India.

Syed Arif Islam Research Scholar, Department of Computer Science, Karpagam Academy of Higher Education, Coimbatore, 641021, India.

ABSTRACT

Modern web browsers must provide expanded capability and customizability as consumers satisfy an increasing number of computing wants through the web. Recent web browsers have the capacity to be altered on the consumer side via browser extensions, which is an essential capability. Users can customise the behaviour of their browsers with extensions to meet their own needs. Extensions are used to improve user productivity (for example, by restrictive access to time-wasting websites), syncing with cloud-based password managers, blocking intrusive advertisements and trackers, and providing fresh ways to organise bookmarks and tabs, among other things. In this article, we conduct the browser extensions and we provide a two-stage approach first detect and then block malicious. This is the most comprehensive analysis of browser extensions to date.

INTRODUCTION

The internet has become an integral aspect of social life. Public web browsers have become more complex than they have ever been and currently maintenances everything from a plain web page to a full-fledged operating system that runs on another computer. Browser extensions are software modules that can be added to the browser to make changes. Malicious attacks in the browser are extremely extensive, and it is very likely to succeed against systems that haven't been hardened, especially those that haven't been hardened. Browser extensions have been used in a variety of attacks in the past [1]. Malicious extensions of various kinds have affected millions of people through the browser [2]. More or less widely used public web browsers: Vivaldi, Microsoft Edge, Opera Browser, Mozilla Firefox ,Google Chrome and so many. Browser security add-ons can also assist in thwarting such assaults. Unfortunately, Google Chrome, which is the most popular operating system, doesn't have a very good system for protecting users' abilities [3]. This article aims to safeguard these public web browsers from malicious attack using browser extensions.

METHODOLOGY

This research takes place in a browser on a Chrome extension intended to detect and block malicious content, where the user can easily learn how to programme computational models of extension phenomena. We observed and recorded the work numbers of users while using safe phenomena. In order to analyse the use of chrome extension processes the users went through, three theoretical perspectives were used: knowledge integration, comprehension plug-in [4], and problem-solving strategies to detect and prevent malicious attract.

FINDINGS

The following are our major contributions: Detect & Block Malicious Google Chrome Extensions.

The extension is known as Salesforce Security, which detects and blocks dangerous chrome extensions. Here's what we need to do.

Step 1: First of all, download & install the Salesforce Security extension on our web browser Google Chrome.

Step 2: Now, double click on the same icon next to the address bar, and it will show a window with a list and all the extensions installed in Chrome.

Step 3: We need to activate or deactivate those that we want, even if we prefer it all at once from the switch that we can find in the upper right part.

Step 4: Each extension have circle that can be of several colours. When the extension is trusted, only it is green.

Step 5: Salesforce Security classifies with the colour red become high risk and orange can be dangerous.

Step 6: From the list, in addition to being able to deactivate, by clicking on each of them we can see the permissions that we have approved and which may be endangering data.

Now extensions will detect and block malicious in Google Chrome web browser data.

CONCLUSIONS

In the Google Chrome browsing environment, Salesforce security privileged browser extensions are more secure. To protect sensitive user data from malicious attacks, we provide a revolutionary, full-featured security system in a public online browser. This article assures that it will become a more user-friendly solution because it does not rely on hard work or a customised browser extension. Users only need to install the Salesforce security extension, after which it is simple to deploy secure.

REFERENCES:

[1] Picazo-Sanchez, P., Tapiador, J., & Schneider, G. (2020). After you, please: browser extensions order attacks and countermeasures. International Journal of Information Security, 19(6), 623-638.

[2] Joseph, J., & Bhadauria, S. (2019, October). Cookie Based Protocol to Defend Malicious Browser Extensions. In 2019 International Carnahan Conference on Security Technology (ICCST) (pp. 1-6). IEEE.

[3] Pantelaios, N., Nikiforakis, N., & Kapravelos, A. (2020, October). You've changed: Detecting malicious browser extensions through their update deltas. In Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (pp. 477-491).

[4] Sjösten, A. (2020). Information Flow for Web Security and Privacy (Doctoral dissertation, Chalmers Tekniska Hogskola (Sweden)).