RESEARCH ARTICLE OPEN ACCESS

# ClickCheck: A Novel Framework for the Detection of ClickJacking Attacks on Html5 Webpages

Anoop MV [1], Arun P Kuttappan [2]
Student [1], Professor [2]
Department of Computer Science d Engineering, GISAT
Mahathma Gandhi University
Kottayam - India

## ABSTRACT

Clickjacking means hijacking the user clicks to perform malious actions.It will redirect the users towards an external links. Clickscheck is a browser-based tool to increase reliability and security to prevent clickjacking attacks. MyClickSafe Tool is the main core engine of the clicksafe. It consists four modules. Each modules have its own functionalities depending upon their duties. The main section started from html processor. First the html processor fetches the html code and html parser analyse the elements to check wheather any clickjacking condition is possible. After the analysis of the webpage elements, the parser will return the result of the analysis to the Clickjacking engine. The database module is used to store the details about the analysis. It is a backup repository. The result of the parser checking is returned to the Clickjacking engine. The core engine will send this result to the database module. It store the results. It also records the user's activities. So that these result can be used for future expansion. This database consist of details of several type clickjacking codes. The subframe engine recursively analyze the frames contained in the webpages.The html processor send the elements to the Subframe engine. This module will analyze wheather the page contains any frames like iframes. Mainly clickjacking attacks are coming with iframes.The attacker uses malicious javascripts with iframe for attacks.So this module will recursively check for any presence of iframes and block it if they occur. Controller module perform the overall control of the core engine. It enables the mutal communication between the different modules. Clickcheck is strongest from other clickjacking tools because the detection and mitigation process is based on a wide ranging framework.It uses detection of malicious webpage components and necessary user feedback. Clickcheck detects clickjacking attacks that describes its performance, and highlights. This will assure safety against click jackingttacks to a large number of users inorder to protect their personal information's.

***Keywords :***— clickcheck, MyClickSafe Tool, html processor database, Controller, Subframe engine.

## I. INTRODUCTION

Clickjacking is a dangerous attack through frames. In this type of attack, the user unknowingly clicks on a malicious page that sits on top of a valid page. This is usually done by loading a malicious page over a valid page. It will requires a user click or some other input credentials such as a login. The malicious page is appeared as transparent page. When the user enter the input, an event is sent to the malicious page that is generated by attacker that causes some undesirable action to be taken. Basically this is happen in form of click event.

In clickjacking attack, the attacker will overlaying an invisible frame over a valid page. Clickjacking Tweet bomb was a famous clickjacking attack. In this attack, the attacker place a malicious page embedded Twitter.com with a transparent IFRAME. The victim webpage attract the user by placing a 'Don't click' button above the invisible 'Tweet' button. When the user clicked on the button, a status message will appear. Which contains a link to the malicious website.

Clickjacking can be also implemented by hiding single UI elements. Clickjacking is also referred to as UI redressing. In this type of attack, the browser is the main source of attack. Likejacking and Tapjacking attacks are the common examples of such attacks.

For this reason we must focus on the context of web browsers. Many defenses methods have been available in market for clickjacking for web browsers but they have all been cheated by malicious users. The defense system consists of frame busting, which simply limits browser functionality by disallowing the IFRAME , but it does work as the webpage cannot get framed over another webpage.

There are several defenses are available. But these defence mechanism are very old and inefficient to detect new type clickjacking attacks. So we need a new mechanism that is capable of overcome the drawbacks of the existing tools.

## II. RELATED WORKS

An application vulnerability is the system flaw in an application that can be exploited to compromise the security of such application. Once an attacker has found a flaw in an application, and determined how to access that, then the attacker exploits the application vulnerability. These attacks mainly target the confidentiality, integrity, or availability of an application, its creators, and its users. Attackers will rely on some tools to perform application vulnerability discovery and compromise.

**Application Vulnerability Management**

It is common to both software and application developers to use scanning software to detect and report the application vulnerabilities in code, but can be costly and difficult to use. Scanning the application quickly becomes outdated and inaccurate.

Table 1.Available Tools

| Name | Type | Click Jacking Detection |
|---|---|---|
| Sandcat | Foreign Commercial | No |
| W3AF | Open Source | Under development |
| WebRavor | Domestic commercial | No |
| IBM AppsScan | Foreign Commercial | No |
| Acunetix | Foreign Commercial | No |
| Burp Suite | Foreign Commercial | Yes |
| SkipFish | Open source | No |

**Sandcat Browser**

It is a fast web browser. It consists of scripting language packed with features for pen-testers. Sandcat Browser is a freeware web browser. The Sandcat Browser is built on top of Chromium, and make use of Lua programming language and scripting support.

**WebRavor**

WebRavor can test almost all WEB application vulnerabilities, like SQL injection, cross-site scripting, xxs forgery, Trojan. It can show the relevant evidence to show the existence of vulnerabilities in loading webpages.

**Acunetix**

It is a website vulnerability scanning tool. This tool discover security vulnerabilities in your web applications that an attacker would use to gain access to your systems and data. It also checks multiple vulnerabilities like cross site scripting, and SQL injection, weak passwords.

**Burp Suite**

It is an integrated platform for performing security testing of different web applications. Its different tools work together to support the overall testing process. It works by finding and exploiting security vulnerabilities.

## Existing Mitigation Methods

**1) Website script:**

This mitigation techniques are implemented on the website where the website is responsible for mitigation.

**2) Browser Add-on code.**

This mitigation techniques are mainly based on the add-on in the loaded webpages. In this case, the web browser is responsible for the mitigation of clickjacking.

**3) Browser with Website code.**

This is the coordination of both browser and the website. In this the browser is responsible for utilizing the method and the website must also adopt relevant code.

## Existing Detection Methods

**ClearClick:**

It is an extension of No script add-on that especially catered to clickjacking. When the user interacts with an embedded element which is transparent, then clearclick will intercept the action and reveal the hidden elements. It provide supports of desktop and mobile versions via the NoScript add-on. It also works like click safe that is focused to educate the naive user.

**CSS check:**

The page will parse and check for any overlapping and invisible elements based on the CSS characteristics. To block mouse clicks a browser may detect the clicked cross-origin frame is not fully visible.

**Browser Add-on:**

Disable onBeforeUnload event to make sure frame busting: Using this technique, a web user can manually cancel the navigation request submitted by another framed page. When a framing page is to be unloaded due to navigation, an onBeforeUnload handler will called.

**Freezing DOM check on elements:**

Using, this works by freezing objects with the help of new features on ECMA Script 5th Edition. It blocks malicious code from changing object properties in a manner providing clickjacking.

**Opaque Overlay Policy:**

Gazelle is a web browser .This browser adopted a method that forced all cross-origin frames to be appeared as opaquely. But this ype approach causes many benign sites to be break down.

**Disable windows switching:**

JavaScript allows the frames and windows to be loaded along with another webpage. The scripts of these webpages are disabled in order to provide security regarding clickjacking.

**Disable all JavaScript Code:**

It blocks all JavaScript code from page and limits the functionality of the webpage and user experience than address clickjacking as a whole. It works like flash block.

## III. PROPOSED SYSTEM

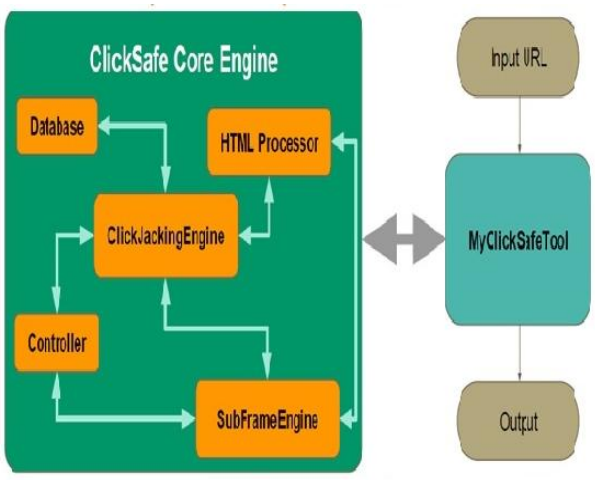


Fig1.Clickcheck Architecture

**MyClickSafeTool**

This is the main core engine of the clicksafe.It consists of the following modules.Each modules have its own functionalities depending upon their duties.They are,

**HTML Processor**

The main section started from html processor.A wepages contains several contents .It includes javascripts,css,frames etc.First the html processor fetches the html code and html parser analyse the elements to check wheather any clickjacking condition is possible.After the analysis of the webpage elements, the parser will return the result of the analysis to the Clickjacking engine.It is the core engine.

**Database**

The database module is used to store the details about the analysis.It is a backup repository.The result of the parser checking is send to the Clickjacking engine.Then the core engine will send this result to the database module in order to store in the database. So that these result can be used for future expansion or future reference. This database consist of details of several type clickjacking codes. So that anyone who want the clickjacking codes for patches checking, can access these code.

**Subframe Engine**

The subframe engine recursively analyse the frames contained in the webpages.The html processor send the elements to the Subframe engine.This module will analyse wheather the page contaisn eny frame.The iframes are the main reason of the clickjacking attacks.The attacker will combines malicious javascripts with iframe and used it for clickjacking attacks.So this module will recursively check for the presence of iframes and block it if they occur.

**Controller**

This module perform the overall control of the core engine.It enables the mutal communication between the different modules.

In the proposed system,we mainly focused on detecting attacks on html5 webpages. HTML5 code writing is easy to learn in comparison with other technologies. Companies can save money if they develop platform independ applications. HTML5 allows to develop applications that adapt to different resolutions, screen sizes, aspect ratios and guidelines. Features such as GPS, camera and accelerometer can be use of with HTML5 and provide a user experience context in a variety of devices, like smartphones, tablet computers etc.

## IV.CONCLUSION

Websites are very vulnerble in nature.Every day the attckers develops new attacking methods to steal user's personal information.So this paper present a new idea detect the clickjacking attacks on html5 webpages.Due to the advantages of html5 code, most of the web developers uses html5 method for designing.The information obtained from this method,that is the database information, can used to create a black and white lists about different attacks and it can be used for the future reference.It can be also used to overcome the limitationsof the previous solutions. This method can not analyse the javascripts coming with the webpages. Ignoring some limitations, this defence method is efficient to providing security against clickjacking attacks on html5 wepages. We plan to extend this mecahnism by dynamic analysis of JavaScript code parallel with encryption/authentication system which doest not allow a system to compromised.

## ACKNOWLEDGMENT

I am very happy because i can share my thoughts about website vulnerbilities through my paper.So i express my pleasure to the the people who have supported me . Firstly I express my sincere thanks to our respected principal and our Department head of GISAT who provides necessary facilities and support. I also thanks to my respected tutor, Mr. Arun Pkuttappan for his valuable guidance throughtout my paper preparation.Also I thanks to my parents and finally, to my friends.

## REFERENCES

[1] G. Rydstedt, E. Bursztein, D. Boneh, and C. Jackson. "Busting frame busting: a study of clickjacking vulnerabilities" at popular sites. In Proceedings of the Web 2.0 Security and Privacy, 2010.

[2] M. Mahemoff. Explaining the "Don't Click" Clickjacking Tweetbomb. http://softwareas.com/explaining-the-dont-click-clickjacking- tweetbomb,2 2009.

[3] M. Zalewski. X-Frame-Options, or solving the wrong problem.http://lcamtuf.blogspot.com/2011/12/x-frameoptions-or-solving- wrong.html, 2011.

[4] Maone,G.Noscrip,clearclick.http://noscript.net/faq#clearclick, January 2012

[5] R. Lundeen, O. Jesse, R. Travis. "New Ways I'm Going to Hack Your Web App. Blackhat AD, 2011.

[6] E. Lawrence. IE8 Security Part VII: ClickJacking Defenses. http://blogs.msdn.com/b/ie/archive/2009/01/27/ie8-security-part-vii- clickjacking-defenses.aspx, 2009.

[7] R.Hansen.Clickjacking.a.ckers.org/blog/20080915/clickjacking. Last accessed July 31st, 2013

[8] M.Niemietz."UI Redressing: Attacks and Countermeasures Revisited". In CONFidence, 2011.