International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868
Foundation of Computer Science FCS, New York, USA
Volume 4– No.7, December 2012 – www.ijais.org

Clickjacking Vulnerability and Countermeasures

A.Sankara Narayanan
Department of Information Technology
Salalah College of Technology
Sultanate of Oman

ABSTRACT

Clickjacking is a web framing attack that has recently received wide media coverage. Web framing attacks such as clickjacking use iframes to hijack a user's web session. In a clickjacking attack, a malicious page is constructed such that it tricks victims into clicking on an element of a different page that is only just or not at all visible. This paper will discuss the basic clickjacking vulnerabilities and countermeasures. This will also show that Clickjacking tool and online Clickjacking sample webpage's. Although clickjacking has been the subject of many discussions and reports, it is currently unclear to what extent clickjacking is being used by attackers in the wild, and how significant the attack is for the security of Internet users. Security experts describe a technique whereby an attacker tricks a user into performing certain actions on a website by hiding clickable elements inside an invisible iframe.

Keywords

Clickjacking, ClickIDS, Web Security, Browser Plug-in

1. INTRODUCTION

The Clickjacking attack was introduced by Robert Hansen and Jeremy Grossman in September 2008. This attack constructs a malicious web page to trick the user into performing unintended clicks that are advantageous for the attacker. Its propagate worms, steal confidential information passwords, cookies, send spam, delete personal mails, etc [4]. This is very much attracted a broad attention by the security industry and the web community. Most websites still have not implemented effective protection against Clickjacking [16]. This vulnerability across a variety of browsers and platforms, a Clickjacking takes the form of embedded code or script that can execute without the user's knowledge, such as clicking on a button that appears to perform another function. Clickjacking also known as user interface redressing is one of Malicious Technique tricking users to click the button or image that will run hidden malicious script from another site. An attacker uses multiple transparent or opaque layers to trick a user into clicking on a button or link on another page when they were intending to click on the innocuous page [15]. Thus an attacker hijacks the click to another website. That's why it is known as Clickjacking (Click+Hijacking). The possibilities for how clickjacking software could be abused are endless. There are a number of things that have major Web sites and companies especially alarmed. In some cases, the user may be able to recognize this immediately; in other cases, the user may be totally unaware of what took place. First is the fact the program can run on virtually any Web site without the Web site owner's knowledge or ability to stop it. Second, clickjacking can take the user to a mirror site while still making them believe they are on the Web site of the company and mine personal information, often which is freely given. Third, no browser, except the very few that are not based on graphics, is immune from clickjacking software [13]. In addition to stealing personal data, such as bank account information, credit card information and Social Security numbers, clickjacking can also install a number of software applications on a computer without the user's knowledge. This software could be harmful viruses, spyware or adware. The latter may not be extremely harmful in nature but it often presents a big problem for computers. Browsers and Internet security software companies are working on a security patch that would help correct the situation. However, that may take some time.

2. BASIC CLICKJACKING

A typical clickjacking attack uses two nested iframes to crop and position an element from a target website. The inner iframe contains the target page and must be large enough to display it in its entirety, such that the element on which the user will click is visible without scrolling. The outer iframe is much smaller and acts as a window onto the page loaded in the inner iframe. For a user interface redressing attack, the outer iframe should only be large enough to display the targeted element [1]. You think you are clicking on the website you see but no, you are really clicking on an invisible website you cannot see that's right under your mouse. Clickjacking affects many browsers and platforms.

Inner.html

1. <iframe id =" inner " src =" http :// www.google.com " width ="2000" height ="2000" scrolling =" no" frameborder =" none ">
2. </iframe >

Fig 1: Inner.html

Clickjacking.html

1. <iframe id =" inner " src =" inner.html " width ="2005" height ="290" scrolling =" no" frameborder =" none "></ iframe >