Client-Side Detection of Clickjacking Attacks

Hossain Shahriar, Kennesaw State University, Kennesaw, GA, USA
Hisham M. Haddad, Kennesaw State University, Kennesaw, GA, USA

ABSTRACT

Clickjacking attacks are emerging threat for web application users where click operations performed by victims lead to security breaches such as compromising webcams and posting unintended messages. Effective client-side defense technique could prevent the possible victims. This paper presents a client side approach to detect clickjacking attacks. The authors’ approach examines web page requests and responses; the proposed approach is designed to detect advanced attack types such as cursorjacking, double click, and history object-based attacks. They evaluate the proposed approach with a set of legitimate and malicious websites. The results indicate that our approach has low false positive and false negative rates. The overhead imposed by the proposed approach is negligible.

Keywords

Clickjacking, Framebusting, iFrame, X-Frame-Options, Double Clickjacking, History Object-based Attacks

1. INTRODUCTION

Clickjacking attacks are common web security threats where user clicks may cause unwanted activities on legitimate websites (Hansen and Grossman, 2008; Clickjacking, 2015; Aun, 2015). A number of reported attacks attempted users tricking to click on websites (e.g., Amazon), and online banking (Balduzzi et al., 2010) that led to activities not intended by victim’s such as purchasing a book from online. Few incidents related to clickjacking attacks include liking an attacker made profile in social website that a victim may not be familiar with, posting messages on Twitter website (NoScript, 2015; Balduzzi et al., 2010; Huang et al., 2012). Several techniques are currently available to prevent clickjacking attacks (Balduzzi et al. 2010; Huang et al., 2012; Clickjacking, 2015, Rydstedt et al., 2010). Unfortunately, these plain approaches rely on the successful execution of JavaScript code. There are challenges to ensure that all browsers to comply with server side defense technique (e.g., X-Frame-Options, 2015) to disallow rendering of pages in iframes at the browsers. Since attackers take advantage of client side presentation of web pages to lure victims, we think that effective clickjacking attacks could be better prevented by employing client-side approach, overcoming limitations of existing approaches.

In this paper, we propose a client-side attack detection approach where we examine request headers and response page contents. Our approach can identify known signatures of script code
or payload part of requests related to clickjacking attacks. It can also identify advanced attack types such as double clickjacking. We implement a prototype and evaluate our approach with a set of legitimate and malicious websites. The results indicate that our approach detects well known clickjacking attacks and have lower performance overhead.

This paper is organized as follows: Section 2 presents some examples of clickjacking attack; Section 3 provides the brief overview of existing side defense techniques; Section 4 provides some examples of clickjacking attacks; Section 5 presents the client-side approach to detect clickjacking attacks; Section 6 discusses some results; and finally Section 7 concludes the paper.

2. ILLUSTRATIVE EXAMPLE

We illustrate an example code snippet mimicking a clickjacking attack based on Facebook “Like” action. Here, the GUI element for “Like” is being hidden in an iframe of a web page controlled by an attacker. The attacker hides the GUI element by making the iframe invisible based on Cascading Style Sheet (CSS) features.

In Figure 1(a), a div tag named icontainer has a lower CSS z-index with an opacity level of zero. The div includes iframe fbframe that loads the clickable object “Like” from Facebook for an individual’s profile (xyz). The URL represents a clickable “Like” action element which can be embedded in any web page and if the element is clicked then the profile of xyz is being liked by the person who clicked it. Since the visibility of the div is zero, the loaded iframe will not be visible to the victim. To lure the victim to click on the element, the attacker places a lucrative message (CLICK HERE TO WIN AN IPAD) in the iframe (Figure 2). Thus, making the victim think that clicking on the message will take him/her to another web page. However, clicking the link will initiate a “Like” action on Facebook for profile xyz without the victim’s knowledge.

In Figure 1, note that the width and height of the div element (10, 12), iframe (50, 23), and the Facebook URL (450, 80) do not match with each other.

If a website designer intends to place a “Like” object in his website in a legitimate way, then the width and height of the URL and the displayed container should match. This is an indication of malicious code.

3. DEFENSE TECHNIQUES

We divide existing clickjacking defense techniques into two categories: server-side and client-side. They are described below in Sections 3.1 and 3.2.

3.1. Server-Side Defense Techniques

3.1.1. Frame busting

Website owners can protect their users against iframe-based clickjacking by including JavaScript code snippets in pages that need protection against clickjacking (Rydstedt et al., 2010). The code snippet in Figure 3 checks if a loaded web page is at the top window or not. If the current page is not in the top window, then it is loaded on the top window, thereby stopping the page loading in the iframe. A number of recent studies have found that most websites do not deploy frame busting code (Rydstedt et al., 2010; Lekies et al., 2012). Thus, our work (applicable at the proxy-level) can be a complementary approach for those websites without including any frame busting code.
Related Content

Designing a Secure Cloud Architecture: The SeCA Model
[www.igi-global.com/article/designing-secure-cloud-architecture/64344?camid=4v1a](www.igi-global.com/article/designing-secure-cloud-architecture/64344?camid=4v1a)

Denial-of-Service (DoS) Attack and Botnet: Network Analysis, Research Tactics, and Mitigation
[www.igi-global.com/chapter/denial-of-service-dos-attack-and-botnet/201608?camid=4v1a](www.igi-global.com/chapter/denial-of-service-dos-attack-and-botnet/201608?camid=4v1a)
Information Systems Security Assurance Management at Municipal Software Solutions, Inc.
[www.igi-global.com/article/information-systems-security-assurance-management/34055?camid=4v1a](www.igi-global.com/article/information-systems-security-assurance-management/34055?camid=4v1a)

Security and Privacy Approaches for Wireless Local and Metropolitan Area Networks (LANs & MANs)
[www.igi-global.com/chapter/security-privacy-approaches-wireless-local/22081?camid=4v1a](www.igi-global.com/chapter/security-privacy-approaches-wireless-local/22081?camid=4v1a)