International Journal of
Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-5, Issue-6)

Research Article | **June 2016**

Study on Clickjacking Attack

Neeru Yadav
CSE, Ambedkar Institute of Advanced Communication Technologies & Research, New Delhi, India

Bharti Nagpal
Assistant Profeesor, Ambedkar Institute of Advanced Communication Technology & Research, New Delhi, India

Abstract—

With the features of the internet, the whole world are becoming closure to each other. Hence internet has provided a medium to communicate over long distances. So, social sites platform users have become an easy targets or victims of the attackers and hackers who exploit the vulnerabilities of websites. Clickjacking and drive-by downloads have become a popular tools through which the attackers try to exploit the users[2]. In This paper, we will study about the clickjacking,its examples,existing clickjacking attacks and defences.

Keywords— Include at least 5 keywords or phrases

I. INTRODUCTION

Clickjacking attack is an emerging threat on a social web. It is also known as User interface readdress attack or UI Readdressing .It is a malevolent technique which deceives user into clicking on one thing that is entirely different from what user or victim perceives. By clicking on, the victims reveal their confidential information or taking control of their computer while clicking on seemingly innocuous web pages.

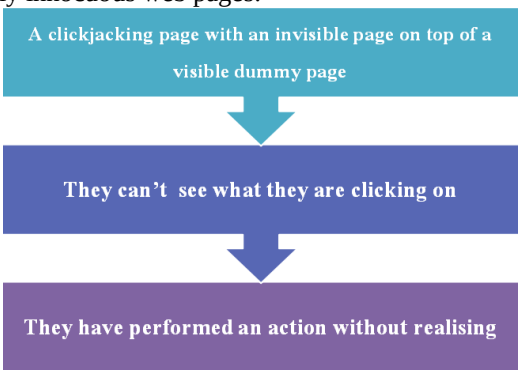

Fig. 1

These attacks lures users to click on objects transparently placed in malicious web pages. This fig (1) shows how an attacker attracts the user to click on the hyperlink to a certain webpage. User doesn't know about the action which the attacker is performing. The result of click function causes unwanted actions within the authentic websites without the knowledge of users or victims. Users end up performing actions on the hidden page. Example for such sites is online-banking auction sites, web mail services, File sharing sites, Net Banking and Social networking sites. Clickjacking can cause severe damages, including compromising a user's private webcam, email or other private data and get access to user's system. User end up performing unintended clicks that are advantageous for the attacker. Its propagate worms, steal confidential information passwords, cookies, send spam, delete personal mails, etc. Most websites still have not implemented effective protection against clickjacking.

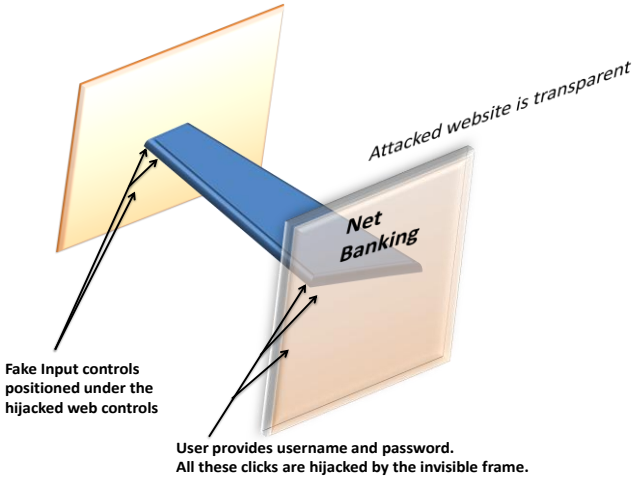

Fig. 2

By using JavaScript technology attacker creates a transparent frame that hovers above the website the user actually sees. A clickjacked page tricks a user into performing unwanted actions by clicking on a hidden link. On this clickjacked page, the attackers load another page over it in a transparent layer. The users think that they are clicking visible buttons, while they are actually performing actions on the hidden/invisible page. The hidden page may be an authentic page; therefore, the attackers can trick users into performing actions which the users never intended.

Analysis of clickjacking attack can be done by the following ways[9]:

1. First Gathering of data from websites which are malicious like advertised on Facebook pages.
2. Secondly,analyze it efficiently to detect clickjacking instances.

Examples of click jacking:

1. A user might receive an email with a link to a video about a news item, but another web page says a product page on SNAPDEAL.com, can be "hidden" on top or underneath the "PLAY" button of the news video. The user tries to "play" the video but actually "buys" the product from snapdeal. The hacker can only send a single click, so they rely on the fact that the visitor is both logged into Snapdeal.com and has 1-click ordering enabled.
2. Sharing or liking links on Twitter.
3. Playing you tube videos to gain views.
4. Clicking Google Adsense ads to generate pay per click.

Another example of click jacking is facebook. In this, attacker creates a website similar to the original one that authorized user thinks that it is original and thus put his credential information.

Fig. 3 : Original website

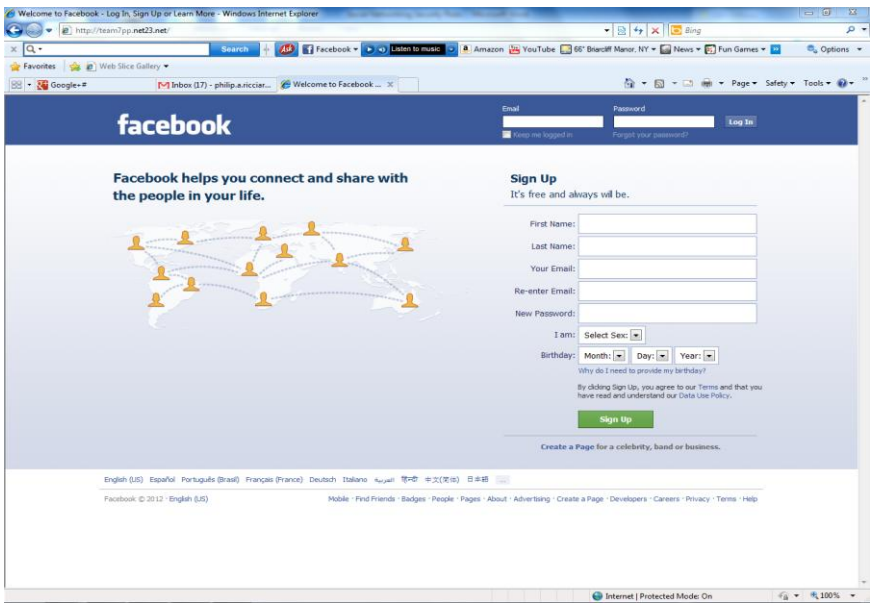

Fig. 3 : Attacker Website

In fig.3. facebook login page is authenticated page but to perform click jacking, attacker creates a facebook login page that looks similar to the original login page like in fig.4.When any authorized user opens the login page, he or she thinks that it is actual page and puts confidential information. This is one type of click jacking. So to prevent from click jacking, always check the address bar of the website you are on.

CURSORJACKING:

Cursorjacking is the concept introduced by Eddy Bordi. In this, users are deceived by use of a custom cursor image. So the displayed cursor gets shifted to the right from the actual mouse position. With clever positioning of page elements attacker directs user clicks to desired elements.

Attack compromising pointer integrity – It guarantees users to rely on cursor feedback to select locations for their input events. One of the advantages of such attack is that target link could be visible and hence located at its original place. Because of this, it is difficult to identify an attack by robot and block compromised page. It even works if java script is disabled in user's browser. The user's cursor is replaced with a fake one by an attacker. Fake cursor should be shifted relatively to its normal position, so it will provide false feedback of pointer location to the user.

LIKEJACKING: It is a variation of clickjacking in which malicious coding is associated with a Facebook Like button.

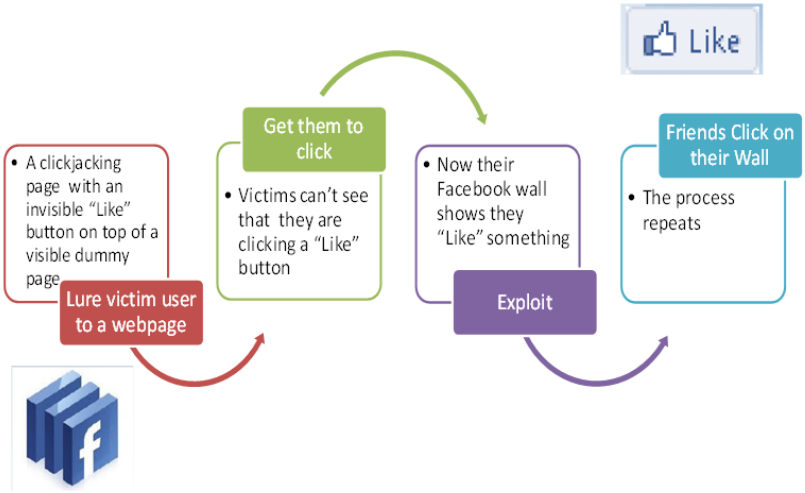

Fig. 4

A "Like" is an approval of a post, product, business or some other page content, registered by clicking the button associated with that item[7]. There are two basic types of likejacking which involve a post that is likely to attract the user, such as an offer for a free gift card or a compelling video, and both spread through ill-advised or automatically generated shares and likes[1]. The initial post may be enabled through a hacked account or the acceptance of a request to add a friend, who turns out to be a scammer.

Clicking on the post itself brings up a splash page that is coded so that if the user clicks anywhere on the page, it registers as a "Like" and shares the original post to the user's Facebook wall. The purpose of this type of exploit may be spreading a hoax or fraudulent promotion of a business or product.

- In the other version, the developers responsible for the post add coding to the Like button that leads users through a series of pages designed to gather their personal information, such as surveys and membership applications. The scammer may receive payment for each completed survey. Applications for membership may require credit card information for "fee payment".

Fig.5 Likejacking example

In above likejacking example, imagine an attacker who builds a web site that has a button on it that says "click here for a new free ipod" and on top of that site page, attacker has loaded an ifmail account and lined up exactly any other messages like "delete all messages" button directly on the top of that free ipod button.User tries to click on that free ipod button but in actually he or she clicked on the "delete all messages" button. By this attacker got access of that user's information.The user can be tricked into clicking like button, on an attacker's website. In this,Like button hidden behind another button.

Here are a few another common examples of likejacking:

- An image of a sick or injured child with text claiming that Facebook will donate $1 toward the child's care for every like.
- A bogus offer for a free iPad, iPhone or other popular electronic device.

Real-life examples

Since social media sites works as hubs for the latest updates, clickjackers mostly target the social media sites like facebook and Twitter and many other e-commerce sites. The following points explain how an attacker attacks the social media sites.

1. Redirects to malicious content:

An attacker attacks a legitimate webpage or website that seems to be providing additional meaningful content to an end user. However, that page will be redirected to another page with malicious content[3]. When posting such a link on a social media site, user is tricked into believing that he or she will be taken to real site and thus the user end up clicking on the malicious page. Clickjacking attacks have been used against both Facebook and Twitter both in the past and present.
One of the recent example is disappearance of Malaysian flight MH370 provides examples of social engineering in combination with clickjacking[3]. Attackers took advantage of people's fascination with this curious event and soon created scam news stating that MH370 was found, which spread through the Twitter account @OfficialCNN. The tweet contained a link to a fake news page containing the article.

This attack's purpose was not to harm end user but only to show how the government or the people could be manipulated by clickjacking if it is done on a very large scale.

Another example of this attack is the creation of a Facebook Valentine's theme. It was spread through Facebook posts which when clicked redirected to a site asking the user to install an extension to their browser. The extension in turn contained a Trojan that injected ads and monitored the user's browser.

2. Taking unwanted actions:

Another variant of clickjacking lures users into clicking links that directly shares, likes or retweets content that was not intended to be. An example is the 'Don't click' link that attacked Twitter in 2009[3]. It worked by tweeting a message that told others not to click a following link. Curiosity then made large amounts of users to click the link, which if the user were logged in to Twitter directly tweeted the same message by the account of the clicking user. No direct purpose other than the spread of the message were found for that particular attack.

Similar attacks can be seen on Facebook still[3]. One example is to Facebook external pages which mimics the look and feel of the original Facebook site to trick users into confirm age, press join to see more content or similar social engineering techniques that makes users click hidden like or share buttons, thus called likejacking by many . This type of attack have for example been used by affiliates to the controversial advertising firm Adscend in 2011. Adscend put into system a way of spreading the word of their customers by placing code that automatically liked and shared their customers' promotional Facebook pages without the end user's permission.

II. EXISTING CLICK JACKING ATTACK

Existing attacks [8] can be classified according to three ways of forcing the user into issuing input commands out of context.

1. Compromising Target Display Integrity:

- **Hiding the target element:** Supported HTML/CSS styling features modern browsers allow attackers to visually hide the target element but still route mouse events to it[8]. The attacker can draw a decoy under the target element by using CSS opacity property and z-index property. Attacker may completely cover the target element with an opaque decoy, but make the decoy Unclickable by setting the CSS property pointer- events: none. A victim's click would then fall through the decoy and land on the invisible target element.
- **Partial overlays:** Sometimes, it is possible to visually confuse a victim by obscuring only a part of the target element. For example, attackers could overlay their own information on top of a PayPal checkout iframe to cover the recipient and amount fields while leaving the "Pay" button intact; the victim will thus have incorrect context when clicking on "Pay". 3) Cropping: Wrapping target element in a new iframe and choose CSS position offset properties.

2. Compromising Pointer Integrity:

The attacker may violate pointer integrity by displaying a fake cursor icon away from the pointer, known as cursorjacking. This leads victims to misinterpret a click's target, since they will have the wrong perception about the current cursor location. Using the CSS cursor property, an attacker can easily hide the default cursor and programmatically draw a fake cursor elsewhere or alternatively set a custom mouse cursor icon to a deceptive image that has a cursor icon shifted several pixels off the original position. Another variant of cursor manipulation involves the blinking cursor which indicates keyboard focus. For example, an attacker can embed the target element in a hidden frame, while asking users to type some text into a fake attacker controlled input field. The blinking cursor confuses victims into thinking that they are typing text into the attacker's input field, whereas they are actually interacting with the target element.

3. Compromising Temporal Integrity:

Earlier attacks manipulated visual context to trick the user or victim into sending input to the wrong UI element. An independent way of achieving the same goal is before actual click occurs. Humans typically require a few hundred milliseconds to react to visual changes and attackers can take advantage of our slow reaction to launch timing attacks. The double-click attack is based on compromising temporal integrity. The browser do not protect against Framebusting. The double-click attack do Bait and switch that the user do a double click right after the first click. The attacker diverts the focus of user to Google pop up window under the right before the second click. To predict clicks more effectively, the attacker could trick the victim to repetitively click objects in a malicious game or to double-click on a decoy button.

4. Whack-a-Mole Attack:

The whack-a-mole attack is the hybrid of pointer and temporal integrity. The attacker tricks the user to click and suddenly switch Face book like button and gets the profile of the user. The attacker ask the user to play a whack-a-mole game and encourage her to score high and earn rewards by clicking on buttons shown at screen location. Throughout the game, attacker uses a fake cursor to control where the user attention should be. At later point in the game, switch in a Facebook like button at the real cursor's location, tricking user to click on it.

5. Likejacking Attack:

Likejacking which is a type of Clickjacking attack to hijack the very popular Facebook's like button can be used to cause degradation of social sites in the form of posting unwanted videos,images and links to a Facebook user's wall without his knowledge. The main idea behind this attack is to conceal the like button under the veil of genuine or real information. Third party widgets such as like button on Face book, tweet button on Twitter, + 1 button on Google Plus, share button and other such type of buttons are all susceptible to c1ickjacking.

III. CONCLUSION

Clickjacking is a new web attack about which most of the users don't know. In a clickjacking attack, a malicious page is constructed in which it tricks users or victims into clicking to a different page that is hidden visible. By stealing the victim's clicks, an attacker could force the user to perform an unintended action that is not visible to the attacker like online money transaction.. Clickjacking makes it hard to protect sites and their users.This attack uses social engineering concept. Thus, it could be a way into user's systems that is easily overlooked even by a security conscious computer user. In this survey paper, we discussed Clickjacking attack and clickjacking examples which will help to understand Clickjacking attack and causes behind it. Also discussed various Clickjacking existing attacks and clickjacking real life example. As per study, it is found that there are many techniques to defend both the attack but still cannot provide full protection.

REFERENCES

[1] Vrindamol P1, Neena V V2, "DETECTION AND PREVENTION OF CLICKJACKING AND CROSS SITE REQUEST FORGERY 2",University of Delhi,Delhi centre.

[2] Tatwadarshi P. Nagarhalli, J.W. Bakal, Neha Jain (Asst. Prof), "A Brief Survey of Detection and Mitigation Techniques for Clickjacking and Drive-by Download Attacks" , International Journal of Computer Applications (0975 – 8887), Vol. 138 – No.2, March 2016.

[3] Martin Kaldma Martin Nordén, "Clickjacking", Project Report for Information Security Course Linköpings universitetet, Sweden

[4] Gustav Rydstedt, Elie Bursztein, Dan Boneh Collin Jackson, "Busting Frame Busting: a Study of Clickjacking Vulnerabilities on Popular Sites", July 20, 2010.

[5] Marco Balduzzi,Manuel Egele,Engin Kirda,Davide Balzarotti,Christopher Kruegel, "A Solution for the Automated Detection of Clickjacking Attacks", ASIACCS'10 April 13–16, 2010, Beijing, China.

[6] A.Sankara Narayanan, "Clickjacking Vulnerability and Countermeasures", 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.

[7] "Security assessment.com ,Clickjacking For Shells", OWASP Wellington, New Zealand Chapter Meeting September 2011.

[8] Lin-Shung Huang, Alex Moshchuk, Helen J. Wang, Stuart Schechter, Collin Jackson, "Clickjacking: Attacks and Defenses".

[9] Giulia Deiana, "Analysis and Detection of Clickjacking on Facebook", Report of MEng Computer Science.

