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

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

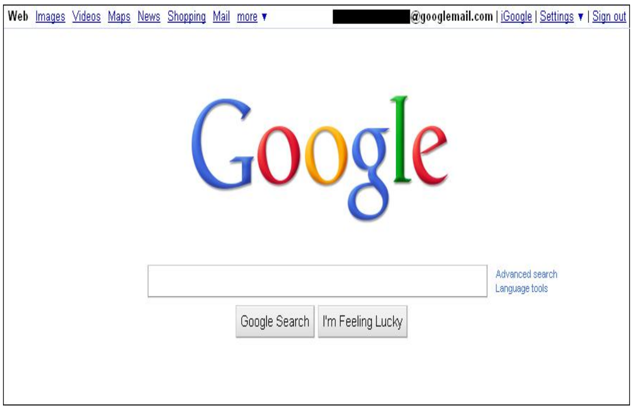

Web Images Videos Maps News Shopping Mail more ▾
[redacted]@googlemail.com | iGoogle | Settings ▾ | Sign out
Google
Advanced search
Language tools
Google Search
I'm Feeling Lucky

Fig 1: Inner.html

Clickjacking.html

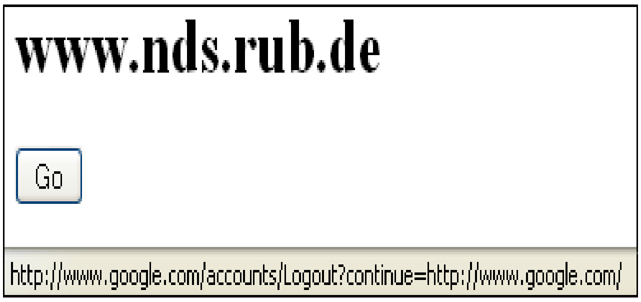
```
<iframe id =" inner " src =" inner.html " width ="2005" height ="290" scrolling =" no" frameborder =" none "></ iframe >
```

2. <style type =" text /css "><!--
3. # inner { position : absolute ; left : -1955 px; top : -14 px ;}
4. //--></ style >

Trustedpage.html

1. <h1 >www .nds .rub .de </h1 >
2. <form action =" http :// www.nds.rub.de">
3. <input type =" submit " value =" Go">
4. </form >
5. <iframe id =" clickjacking " src =" clickjacking .html " width ="50" height ="300" scrolling ="

   no" frameborder =" none ">
6. </iframe >
7. <style type =" text /css "><!--
8. # clickjacking { position : absolute ; left :7 px; top :81 px; opacity :0.0}
9. //--></ style >



www.nds.rub.de

http://www.google.com/accounts/Logout?continue=http://www.google.com/

Fig 2: Trustedpage.html

1. “inner.html”: Frame “google.com” (2000x2000px)
2. “clickjacking.html”: Shift the iframe with “src=inner.html” to the left
3. “trustedPage.html”: Place a transparent iframe with “src=clickjacking.html” over the “Go” button

The order of search results on Google’s search results pages is based, in part, on a comparison between three attacks.

Table 1. Clickjacking vs. Browser Based Attack

	Google Results	***Years***
Cross-Site Scripting(XSS)	15,700,000	15
Cross-Site Request Forgery(CSRF)	2,870,000	11
Clickjacking	1,200,000	3

The following chart (figure 3) shows the clickjacking google results.

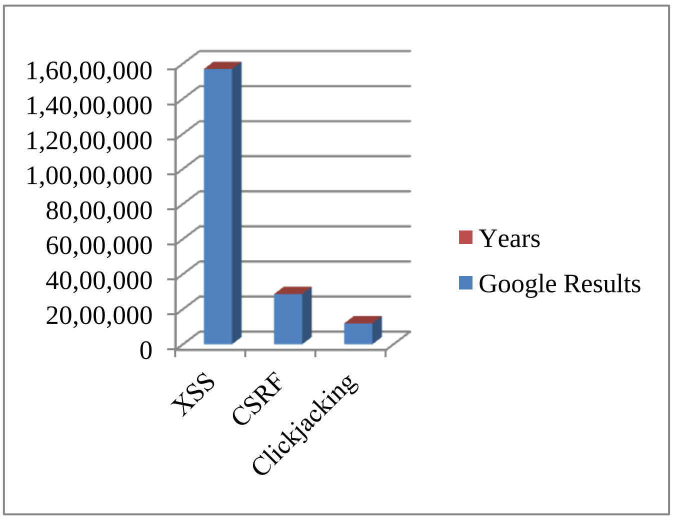
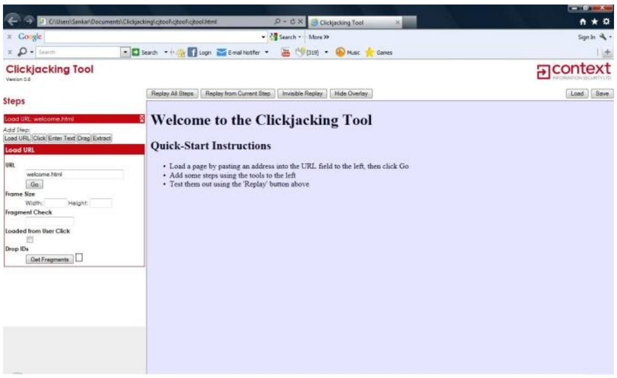


Fig 3: Clickjacking growth chart

3. CLICKJACKING TOOLS

Introduced by Stone at the Black Hat Europe in 2010, it is visualize clickjacking techniques in practice. This tool can be used to craft and replay various clickjacking techniques against web sites that have not yet implemented clickjacking protection. This tool has been tested in Firefox 3.6 and Internet Explorer 8.

Download the Clickjacking tool link: http://www.contextis.com/research/tools/clickjacking-tool/



Welcome to the Clickjacking Tool

Quick-Start Instructions

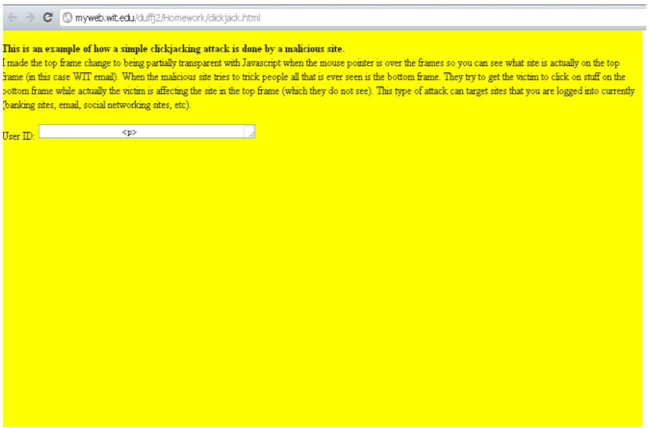
- Load a page by pasting an address into the URL field to the left, then click Go
- Add some steps using the tools to the left
- Test them out using the 'Replay' button above

Fig 4: Clickjacking Practice Tool

3.1 Online Clickjacking Sample Pages

1) http://myweb.wit.edu/duffj2/Homework/clickjack.html

Click the above URL it’s a real time sample page. This is simple example of clickjacking; it will show the top of a visible dummy page and bottom of the transparent or target page.



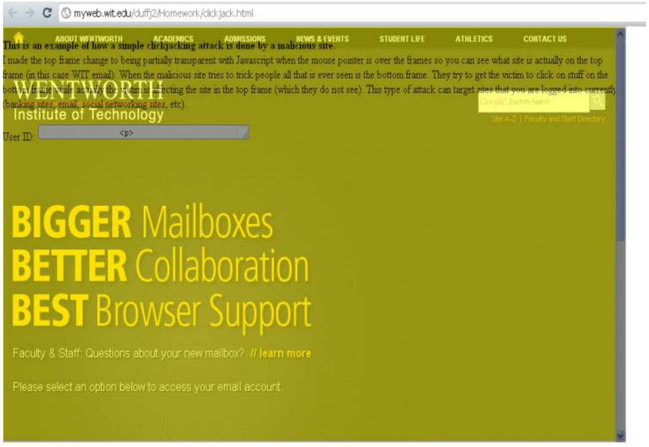
myweb.wit.edu/duffj2/Homework/clickjack.html

This is an example of how a simple clickjacking attack is done by a malicious site.
I made the top frame change to being partially transparent with Javascript when the mouse pointer is over the frames so you can see what site is actually on the top frame (in this case WIT email). When the malicious site tries to trick people all that is ever seen is the bottom frame. They try to get the victim to click on stuff on the bottom frame while actually the victim is affecting the site in the top frame (which they do not see). This type of attack can target sites that you are logged into currently (banking sites, email, social networking sites, etc).

User ID: <p>

Fig 5: Clickjacking dummy page

User sees the top of a visible dummy page



myweb.wit.edu/duffj2/Homework/clickjack.html

This is an example of how a simple clickjacking attack is done by a malicious site.
I made the top frame change to being partially transparent with Javascript when the mouse pointer is over the frames so you can see what site is actually on the top frame (in this case WIT email). When the malicious site tries to trick people all that is ever seen is the bottom frame. They try to get the victim to click on stuff on the bottom frame while actually the victim is affecting the site in the top frame (which they do not see). This type of attack can target sites that you are logged into currently (banking sites, email, social networking sites, etc).

User ID: <p>

BIGGER Mailboxes
BETTER Collaboration
BEST Browser Support

Faculty & Staff: Questions about your new mailbox? // learn more

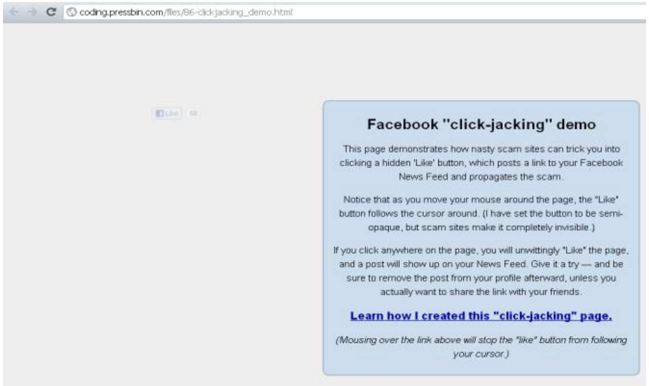
Please select an option below to access your email account.

Fig 6: Clickjacking Invisible page

Inside Clickjacking the invisible page

2) http://coding.pressbin.com/files/86-clickjacking_demo.html

Click the above URL it's a real time online demo page. If you move your mouse around the page "Like" button follows the cursor around.



coding.pressbin.com/files/86-clickjacking_demo.html

Facebook "click-jacking" demo

This page demonstrates how nasty scam sites can trick you into clicking a hidden 'Like' button, which posts a link to your Facebook News Feed and propagates the scam.

Notice that as you move your mouse around the page, the "Like" button follows the cursor around. (I have set the button to be semi-opaque, but scam sites make it completely invisible.)

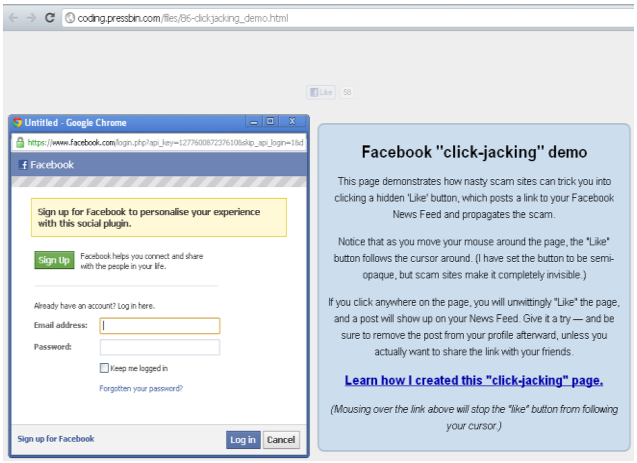
If you click anywhere on the page, you will unwittingly "Like" the page, and a post will show up on your News Feed. Give it a try — and be sure to remove the post from your profile afterward, unless you actually want to share the link with your friends.

Learn how I created this "click-jacking" page.

(Mousing over the link above will stop the "like" button from following your cursor.)

Fig 7: Clickjacking demo page

What the user clicks on



coding.pressbin.com/files/86-clickjacking_demo.html

https://www.facebook.com/login.php?api_key=127760087237610&skip_api_login=1&d

Sign up for Facebook to personalise your experience with this social plugin.

Facebook helps you connect and share with the people in your life.

Already have an account? Log in here.

Email address:

Password:

□ Keep me logged in

Forgotten your password?

Facebook "click-jacking" demo

This page demonstrates how nasty scam sites can trick you into clicking a hidden 'Like' button, which posts a link to your Facebook News Feed and propagates the scam.

Notice that as you move your mouse around the page, the "Like" button follows the cursor around. (I have set the button to be semi-opaque, but scam sites make it completely invisible.)

If you click anywhere on the page, you will unwittingly "Like" the page, and a post will show up on your News Feed. Give it a try — and be sure to remove the post from your profile afterward, unless you actually want to share the link with your friends.

Learn how I created this "click-jacking" page.

(Mousing over the link above will stop the "like" button from following your cursor.)

Fig 8: Clickjacking Redirected Page

What the user sees (user clicks anywhere in the page it will redirect to facebook)

4. CLICKJACKING PROTECTION

https://addons.mozilla.org/en-US/firefox/addon/noscript/

The link of the tool that is used in Firefox against ClickJacking, you need to install No Script. This free, open source add-on will only allow JavaScript, Java, Flash and other plugins to be executed by sites you trust; all scripting is blocked by default. When you visit any website you will find the option on the down side.

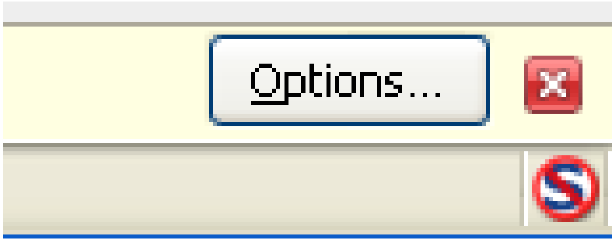
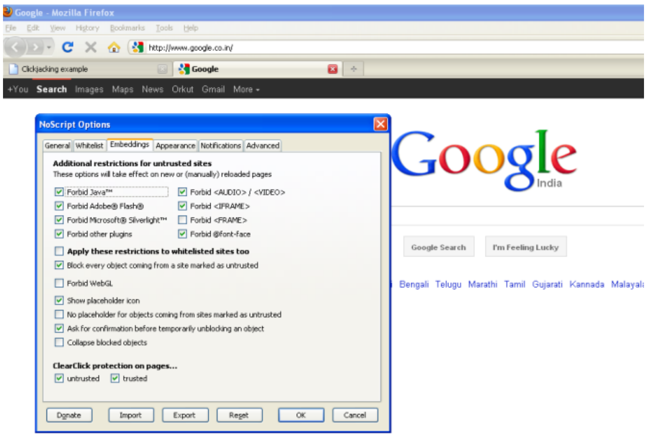


Fig 9: Options add-on

You have multiple option to choose from either stop some script to run and allow some script to run, beside it you can allow the entire website to run as well as you can stop to complete website or simply block it. What you do for trusted website click it on option and allow you trusted website, but when you are visiting about an tentative website so be careful and allow NoScript to do the job.


Google - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://www.google.co.in/
Clickjacking example
Google
+You Search Images Maps News Orkut Gmail More
NoScript Options
General Whitelist Embeddings Appearance Notifications Advanced
Google
India
Google Search
I'm Feeling Lucky
Bengali Telugu Marathi Tamil Gujarati Kannada Malayal
Donate Import Export Reset OK Cancel

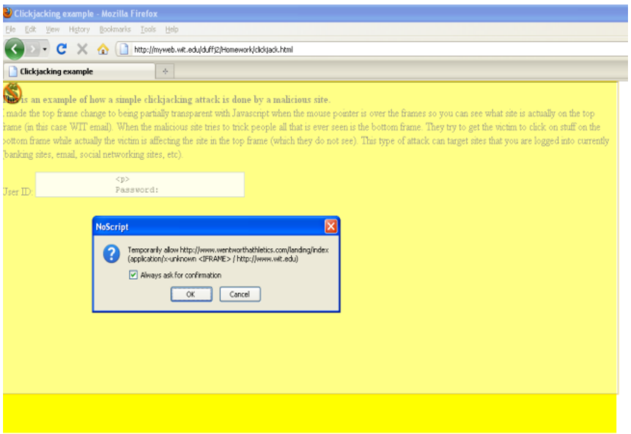
Additional restrictions for untrusted sites
These options will take effect on new or (manually) reloaded pages

- ☑ Forbid Java™
- ☑ Forbid Adobe® Flash®
- ☑ Forbid Microsoft® Silverlight™
- ☑ Forbid other plugins
- ☑ Forbid <AUDIO> / <VIDEO>
- ☑ Forbid <IFRAME>
- □ Forbid <FRAME>
- ☑ Forbid @font-face
- □ **Apply these restrictions to whitelisted sites too**
- ☑ Block every object coming from a site marked as untrusted
- □ Forbid WebGL
- ☑ Show placeholder icon
- □ No placeholder for objects coming from sites marked as untrusted
- ☑ Ask for confirmation before temporarily unblocking an object
- □ Collapse blocked objects

ClearClick protection on pages...
☑ untrusted ☑ trusted

Fig 10: Enable iframe

There are so many options beside it like tracking site and ad host etc. Clickjacking you needed to enable the Forbid <IFRAME> and possibly apply these restrictions to trust sites as well NoScript options.


Clickjacking example - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://myweb.wit.edu/duffj2/Homework/clickjack.html
Clickjacking example
NoScript
OK
Cancel

This is an example of how a simple clickjacking attack is done by a malicious site.
I made the top frame change to being partially transparent with Javascript when the mouse pointer is over the frames so you can see what site is actually on the top frame (in this case WIT email). When the malicious site tries to trick people all that is ever seen is the bottom frame. They try to get the victim to click on stuff on the bottom frame while actually the victim is affecting the site in the top frame (which they do not see). This type of attack can target sites that you are logged into currently (banking sites, email, social networking sites, etc).

User ID: <p> Password:

Temporarily allow http://www.wentworthathletics.com/landing/index (application/x-unknown <IFRAME> / http://www.wit.edu)

☑ Always ask for confirmation

Fig 11: Clickjacking blocking alert

When you are enabling the Forbid <IFRAME> it will block the clickjacking IFRAME.

5. CONCLUSION

There have been many news items, discussions, and blog postings on the topic. However, 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. This paper will help realize end users understand the risks related to using Clickjacking vulnerabilities. Although it has been three years since the concept was first introduced, most websites still have not implemented effective protection against clickjacking. So beware of any websites, it may be Clickjacked.

6. REFERENCES

[1] Paul Stone, 2010. Next Generation Clickjacking, White Paper . Context Information Security Ltd.

[2] Marco Balduzzi, Manuel Egele, Engin Kirda, Davide Balzarotti, Christoper Kruegel, 2010. A Solution for the Automated Detection of Clickjacking Attacks. ASIACCS.

[3] Gustav Rydstedt, Elie Bursztein, Dan Boneh, Collin Jackson, 2010. Busting Frame Busting: A Study of Clickjacking Vulnerabilities on Popular Sites. Web 2.0 Security and Privacy.

[4] Clickjacking for Shells, 2011. OWASP Wellington, New Zealand Chapter Meeting.

[5] Robert Hansen, Jeremiah Grossman, 2008. Clickjacking. Sec Theory, Internet Security.

[6] Agam Shah, Joab Jackson, 2011. Doj Charges Seven in Massive Clickjacking Scheme. Network World IDG News Service.

[7] Lucian Constantin, 2011. Clickjacking Attacks Possible Despite Frame Busting Protection. Infoworld News Service.

[8] Gustav Rydstedt, Baptiste Gourdin, Elie Bursztein, Dan Boneh, 2011. Framing Attacks on Smart Phones and Dumb Routers Tap-jacking and Geo-localization Attacks. Security Lab Stanford.

[9] Face Book Clickjacking Demo. [Available: http://coding.pressbin.com/files/86-clickjacking_demo.html]

[10] Online Clickjacking Sample Page. [Available: http://myweb.wit.edu/duffj2/Homework/clickjack.html]

[11] Egele, Kirda, Balzarotti, Kruegel, 2010. New Insights into Clickjacking. OWASP Foundation AppSec Research.

[12] Bikash Dash, 2011. Introduction and Prevention to Clickjacking Attack. Eg Hacking.

[13] Clickjacking. [Available: http://www.wisegeek.com/what-is-clickjacking.htm]

[14] Clickjacking Tool, Context Information Security Ltd. [Available: http://www.contextis.com/research/tools/clickjacking-tool/]

[15] Clickjacking, 2012. The Open Web Application Security Project. [Available: https://www.owasp.org/index.php/Clickjacking]

[16] Clickjacking-Black Hat 2010. Context Information Security Ltd. [Available: http://www.contextis.com/research/white-papers/clickjacking-black-hat-2010/]