# Chapter 9
# Hijacking of Clicks:
## Attacks and Mitigation Techniques

**Hossain Shahriar**
*Kennesaw State University, USA*

**VamsheeKrishna Devendran**
*Kennesaw State University, USA*

## ABSTRACT

*Clickjacking attacks are an emerging threat on the Web. The attacks allure users to click on objects transparently placed in malicious Web pages. The resultant actions of the click operations may cause unwanted operations in the legitimate websites without the knowledge of users. Recent reports suggest that victims can be tricked to click on a wide range of websites such as social network (Facebook, Twitter), shopping (Amazon), and online banking. One reported incident on clickjacking attack enabled the webcam and microphone of a victim without his/her knowledge. To combat against clickjacking attacks, application developers need to understand how clickjacking attacks occur along with existing solutions available to defend the attacks. This chapter shows a number of basic and advanced clickjacking attacks. The authors then show a number of detection techniques available at the client, server, and proxy levels.*

## INTRODUCTION

Hijacking of Click (also known as Clickjacking) attacks steal clickable actions from victims and direct clicks towards legitimate websites without the knowledge of the victims (Clickjacking-OWASP 2014). When multiple applications or websites (or OS principals in general) share a common graphical display, they are subject to clickjacking (Aharonovsky 2008) attacks. To perform a clickjacking attack, an attacker first designs a malicious web page containing an iframe which may load a legitimate web page. The iframe opacity level is set very low to make it barely visible by a victim. The malicious web page allures the victim to click on visible GUI element (overlapping the invisible legitimate webpages loaded in an iframe). If a victim clicks on the visible GUI element supplied by an attacker, it results in an action on the legitimate web page and may cause unwanted actions.

Some common incidents due to the hijacking of clicks include posting unwanted messages in Twitter without the knowledge of victims, sharing

DOI: 10.4018/978-1-4666-6324-4.ch009

dubious links as well as liking other users on the Facebook, and making individual profile public (Balduzzi, M., Egele, M., Kirda, E., Balzarotti, D., & Kruegel 2010). Clickjacking attacks are being used to generate revenues for large scale botnet operators (Hachman 2014). To address and mitigate the loss due to hijacking of clicks, one key step is to understand the basic and advanced attack types as well as the capability of the state-of-the art mitigation techniques.

In this chapter, we provide a detailed overview of techniques to hijacking the clicks while users visit malicious webpages. We discuss advanced attack techniques that are built on top of existing defense mechanisms applicable at the server and client-sides. We also explore well-known anti-clickjacking solutions applicable at the client, server, and proxy sides. The chapter will enable practitioners to understand the working principle of existing defense techniques and select appropriate techniques based on their needs.

The chapter is organized as follows. Section 2 discusses three common variants of clickjacking attacks. Section 3 discusses the framebusting technique, a common defense against clickjacking attacks followed by a number of advanced attack techniques. Section 4 describes some client-side defense techniques, whereas Section 5 highlights some server-side defense techniques. Section 6 shows an example of proxy-level approach for detecting clickjacking attacks. Finally Section 7 concludes the chapter.

## BASIC CLICKJACKING ATTACK TECHNIQUE

A clickjacking attacker has all the capabilities of a web attacker. He/she owns a domain name and controls the contents served from web servers, and can make a victim visit a malicious website, thereby rendering attacker's supplied content in the victim's browser. When a victim visits the attacker's page, the page hides a sensitive UI element visually or temporally, and lures a user to perform actions (*e.g.*, clicking on element) which may be out of context and without the knowledge of a user where it is actually being clicked.

To date, there are two kinds of widespread clickjacking attacks in the wild: *Tweetbomb* and *Likejacking* (Kharif 2012). In both attacks, an attacker tricks victims to click on Twitter's Tweet or Facebook's Like button using hiding techniques, causing a link to the attacker's site to be reposted to the victim's friends and thus propagating the link virally. These attacks increase traffic to the attacker's site and harvest a large number of friends or followers.

We classify clickjacking attacks into three types based on how users are forced or allured to click on objects out of context (Huang, Moshchuk, Wang, Schechter & Jackson, 2012): (i) target display manipulation, (ii) modification of pointer location, and (iii) modification of timer event. We discuss the three techniques with examples below:

### Target Display Manipulation

Here, a user believes that he fully sees and recognizes the target element before clicking an object. An HTML element is rendered in an invisible frame where the element if clicked may perform a legitimate action. However, an attacker places another webpage on top of the invisible iframe so that a victim does not understand that the click is effective for the invisible GUI element. We show an example of target display manipulation attacks by loading Facebook "Like" GUI element and hiding it in an iframe of a web page controlled by an attacker. The hiding of the GUI element is being done by making the iframe invisible based on Cascading Style Sheet (CSS) styling features. Figure 1(a) shows the HTML code while Figure 1(b) shows the display result.

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 a clickable object "Like" from Facebook for an