Clickjacking Attack Lab

The development of this document is funded by the National Science Foundation's Course, Curriculum, and Laboratory Improvement (CCLI) program under Award No. 0618680 and 0231122.

1 Lab Overview

Clickjacking, also known as UI-Redress attack, misleads the victim by overlaying multiple frames and making some frames invisible. Thus the victim is displayed with one webpage but his/her action is actually on another webpage that is selected by the attackers. This attack takes advantage of the HTML property called iFrame. The objective of this lab is to understand how iFrame with some Style property can be used as the tool for such an attack. Students will first create HTML webpages to learn the use of iFrame and then they will try Clickjacking attacks on the phpBB Web Application server within the lab environment.

2 Lab Environment

In this lab, we will need the following:

1. Firefox web browser.
2. Apache web server.
3. phpBB message board web application.
4. A malicious website.

The pre-built Ubuntu VM image provided to you has already installed the Firefox web browser with the required extensions. The apache web server is also included in the pre-built Ubuntu image. However, the web server is not started by default. You have to first start the web server using one of the following two commands:

```
  % sudo apache2ctl start
or
  % sudo service apache2 start
```

The phpBB web application is already set up in the pre-built Ubuntu VM image. We have also created several user accounts in the phpBB server. The password information can be obtained from the posts on the front page. You can access the phpBB server (for this lab) using the following URLs (the apache server needs to be started first):

URL	Description	Directory
http://www.originalphpbb.com	Original phpBB	/var/www/OriginalPhpbb/

The attacker has to host a new website to make the Clickjacking attack possible. The following steps show how to host a new wesite using the same Apache web server running on the local machine.

1. Choose a name for your new website. Let us call it `www.clickjackinglab.com`.
2. Add the following line to the `/etc/hosts` file:

```
127.0.0.1   www.clickjackinglab.com
```

3. Create a directory called `ClickjackingLab` in `/var/www/`. All your html files should be kept in this newly created directory.
4. Create a new entry for your new website in the apache server by appending the following information to the file `/etc/apache2/sites-available/default`:

```
<VirtualHost *:80>
        ServerName www.clickjackingLab.com
        DocumentRoot /var/www/ClickjackingLab
</VirtualHost>
```

5. Restart the Apache server using the following command:

```
% sudo service apache2 restart
```

6. Check your website by accessing it through Firefox browser.

Note for Instructors

This lab may be conducted in a supervised lab environment. The instructor may provide the following background information to students at the beginning of the lab session:

1. Information on how to use the preconfigured virtual machine.
2. How to use the Firefox web browser.
3. The creation and use of HTML Webpages.
4. How to access the source code for the web applications.

3 Lab Tasks

3.1 Task 1: Understanding `iFrame`

`iFrame` is a tag defined as `inline Frame` by the HTML standard. `iFrame` facilitates to embedd an HTML document in a frame inside a normal HTML document. HTML has an attribute called `Style`, which provides the user with the option of layouting the HTML element. `Style` attribute introduces Cascading Style Sheet (CSS) to the HTML.

```
<html >
<head>
    <title>title</title>
</head>
<body>
```

```
<center>
<h2>Welcome to my new website</h2>
<iframe id="new" src="http://www.cnn.com" style="opacity:0.0;
position:absolute;top:195px;left:10px;width:1000px;height:200px;">
</iframe>
</center>
</body>
</html>
```

The sample code above defines a simple HTML Webpage containing a `iFrame` element with its `Style` attribute. The property `position` defines location of the `iFrame` and its dimension where as `opacity` defines the visibility percentage of the `iFrame` (1.0 means "complete visible" and 0.0 means "complete invisible"). These above mentioned properties of the style play a very important role in making the `Clickjacking` attack possible. In this task, the student need to get familiar with `iFrame` and its `Style` attribute:

1. Create a website as described in the previous section.
2. Create a webpage by copying the above mentioned code into an "index.htm" file in your website directory.
3. Describe any 3 interesting observation about `Style` properties.

3.2 Task 2: The `Clickjacking` Attack

In `Clickjacking` attacks, the attacker constructs a malicious web page and misleads the victim into clicking on certain (visible) links/buttons, whereas in reality, they are actually clicking on other links/buttons made invisible by the attacker. In such an attack, what victim is displayed to see and what the victim actually clicks are different. In the `Clickjacking` task, the attacker can do the following to make the attack successful:

1. Host a malicious website, and create a webpage that contains an `iFrame`. The `phpBB` web site is loaded into the `iFrame`.
2. Post a message in the `phpBB` whiteboard and attract victims to check for your malicious website.
3. Once the victim visits the attacker's well crafted webpage and clicks on the links/buttons provided by the attacker, some posts/inbox contents in the `phpBB` should get deleted.

Attack Tips: The `Clickjacking` attack is all about crafting the malicious webpage in order to deceive the victim from the attack. One of the important requirements of the attack is that victim has to be logged into the `phpBB` web application in order to make this an successful attack.

- Since the user has be logged into the `phpBB` web application to make the attack, the attacker will post a message to the victim with the malicious website link in the message content. Thus making an attempt to persuade the victim to visit the malicious website.
- The main objective of the attacks is to get the victim to clicks on the `phpBB` web page and delete some of the posts from the page. Obviously, the victims will not make the clicks if they can see what

they are actually doing (they do not want to delete those posts). Therefore, the malicious web page has to be crafed in a way, such that the victims are not clicking on what they are seeing, although they think they are clicking on what they see.

You can achieve the above goal using the `style` properties like `position` and `opacity`. You need to put the `links/buttons` at appropriate positions to make your attacks successful.

3.3 Task 3: Protection against ClickJack attack

Several solutions have been proposed to counter the Clickjacking attack. The followings are two solutions. Please try these solutions, and report your observation.

- **Frame-Busting:** This technique checks if the webpage is the topmost window or embedded in a frame. If the webpage is embedded, it will bust out of the frame and makes itself as the topmost frame. This is achieved with the help of DOM property call `top`. The `top` property defines the topmost ancestor window.

```
<script type="text/javascript">
function breakout()
{
if (window.top!=window.self)
  {
  window.top.location=window.self.location;
  }
}
</script>
```

The above javascript function defines a sample frame-busting function.

4 Submission

Students need to submit a detailed lab report to describe what they have done and what they have observed. Report should include the evidences to support the observations. Evidences include observations, screen-dumps, etc.

References

[1] You don't know (click)jack: http://www.securityfocus.com/news/11535/2

[2] Browser Security Handbook: http://code.google.com/p/browsersec/wiki/Main

[3] UI-Redressing Attacks: http://www.sophos.com/blogs/sophoslabs/v/post/1850

[4] HTML Elements: http://www.w3schools.com

[5] clickjacking UI-Redressing: http://www.imperva.com/resources/glossary/clickjackingui-redressing.html