JOURNAL OF SCIENCE OF HNUE DOI: 10.18173/2354-1059.2017-0009
Natural Sci. 2017, Vol. 62, No. 3, pp. 69-75
This paper is available online at http://stdb.hnue.edu.vn

ĐỀ XUẤT MỘT SỐ BIỆN PHÁP PHÒNG CHỐNG PHƯƠNG THỨC TẤN CÔNG CLICKJACKING

Nguyễn Đăng Tiến
Trường Đại học Kĩ thuật Hậu cần Công an Nhân dân, Bộ Công an

Tóm tắt. Trong bài báo này, chúng tôi đề xuất một số biện pháp phòng chống phương thức lừa đảo trực tuyến (phishing) rất phổ biến, đó là phương thức tấn công Clickjacking. Đây là dạng tấn công mà khi sử dụng trình duyệt để truy cập các ứng dụng, nạn nhân bị lừa truy cập và thao tác trên các trang web giả mạo do hacker tạo ra. Những trang web này thường được núp dưới vỏ bọc của một trang web an toàn. Tấn công Clickjacking không yêu cầu kĩ thuật cao nhưng hiệu quả thu được có thể rất lớn. Hậu quả gây ra nhẹ là sự phiền toái đối với người dùng, nặng hơn là bị mất cắp thông tin các loại tài khoản hay các dữ liệu nhạy cảm. Chúng tôi cũng đưa ra một số phương pháp phòng ngừa từ phía máy chủ Web và từ phía người dùng để ngăn chặn dạng tấn công này một cách hiệu quả.

Từ khóa: Tấn công Clickjacking, thẻ iframe, thiết lập z-index, hacker, dịch vụ mạng.

1. Mở đầu

Clickjacking được Robert Hansen (người sáng lập và điều hành hãng SecTheory) và Jeremiah Grossman (Haker mũ trắng) phát hiện và công bố vào năm 2008. Năm 2010, tại hội thảo Black Hat Europe diễn ra tại Barcelona, chuyên gia bảo mật người Anh - Paul Stone cũng đã trình diễn thêm các kĩ thuật khai thác mới của dạng tấn công này [1].

Clickjacking (hay UI Redress Attack) là một dạng tấn công lừa đảo trên ứng dụng web. Thuật ngữ Clickjacking mô tả việc hacker dụ người dùng click vào các liên kết độc hại, nguy hiểm, được ẩn mình dưới vẻ ngoài là một trang web an toàn. Việc click vào các liên kết đó có thể đơn giản là bị điều hướng sang các trang web khác, tăng view cho một quảng cáo giúp kiếm tiền cho hacker, hay nặng hơn là bị đánh cắp các thông tin bí mật, nhạy cảm và chiếm quyền điều khiển máy tính. Điều đáng ngại là hình thức lừa đảo này xuất hiện nhiều trên web đến mức người ta xem đó là một phần hiển nhiên khi truy cập Internet. Các thiệt hại thường xảy ra đối với các cá nhân sử dụng internet hơn là nhà cung cấp dịch vụ hoặc doanh nghiệp nên phương thức tấn công này ít được truyền thông chú ý so với các dạng tấn công khác như SQL injection, DoS hay DDoS….

Một số giải pháp phòng chống Clickjacking đã được nghiên cứu trước đây. Trong [2], tác giả đề xuất một phương pháp trong đó tại thời điểm ban đầu, hành động truy cập vào từng đường dẫn của trang web được mô phỏng. Sau đó hệ thống sẽ phân tích mô phỏng này và đưa ra lời cảnh báo đối với người dùng rằng có khả năng đây là trang web tấn công Clickjacking hay không. Guvstav và cộng sự [3] đã trình bày phương pháp trong đó sử dụng kĩ thuật frame-busting và áp dụng cho một số trang web.

Ngày nhận bài: 19/2/2017. Ngày nhận đăng: 20/3/2017.
Tác giả liên hệ: Nguyễn Đăng Tiến, email: ndtient36@gmail.com

Trong [4-6], các tác giả tập trung vào phân tích các chiến thuật hacker sử dụng trong phương pháp Clickjacking và cách phòng các kĩ thuật phòng chống loại tấn công này. Nhằm nâng cao nhận thức của người sử dụng internet về Clickjacking, trong bài báo này tôi trình bày một số nghiên cứu về các kĩ thuật tấn công, mối nguy hiểm của phương thức này và cuối cùng là một số hướng dẫn cách thức phòng chống.

2. Nội dung nghiên cứu

2.1. Phương pháp tấn công Clickjacking và cách phòng trống

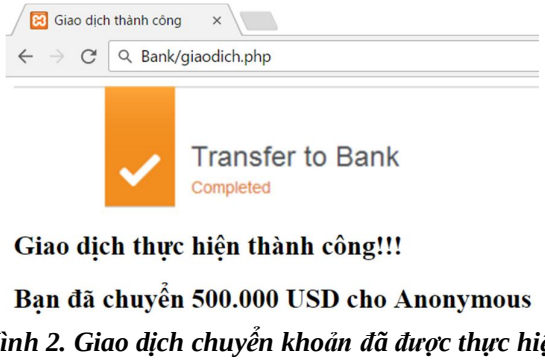
2.1.1. Kịch bản tấn công Clickjacking

Ở phần này, tôi mô tả kịch bản của một cuộc tấn công Clickjacking đơn giản. Quá trình có thể được thực hiện như sau:

Hacker dụ người dùng truy cập vào một trang web đã được tạo sẵn, trang web này có thể là một tin thông báo nhận thưởng với các tài sản hấp dẫn, hay các trang có nội dung nhạy cảm thu hút người xem… Chúng thường có dạng như sau:

Hình 1. Trang trúng thưởng nhằm thu hút người dùng

Truy cập web để trúng thưởng một chiếc iPhone? Phần thưởng này đủ hấp dẫn để khiến người dùng dễ dàng nhấn chuột vào nút "NHẬN THƯỞNG" mà không biết rằng đang bị đưa vào nguy hiểm. Thứ hiện ra sau cú click chuột sẽ là:



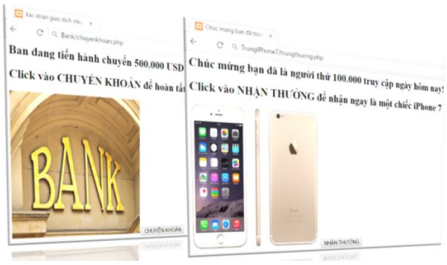
Hình 2. Giao dịch chuyển khoản đã được thực hiện

Chuyện gì đã xảy ra? Người dùng đang tương tác với trang web thông báo trúng thưởng, click vào nút "NHẬN THƯỞNG" chứ không sử dụng gì đến dịch vụ ngân hàng, vậy thông báo chuyển khoản thành công ở đâu? Tại sao số dư trong tài khoản đã biến mất 500 USD?

Xem xét kĩ hơn một chút, ở đây rõ ràng người dùng đang tương tác với dịch vụ Internet Banking của ngân hàng, với một nút "CHUYỂN KHOẢN" nằm ở trên đó. Nhưng thứ hiển thị lên trên màn hình máy tính của nạn nhân lại là một trang web không liên quan gì đến nội dung. Khi người dùng click vào nút "NHẬN THƯỞNG" được hiển thị trên màn hình thì thực sự hacker đã điều hướng click vào nút "CHUYỂN KHOẢN", do đó giao dịch chuyển tiền được thực hiện, tiền trong tài khoản bị mất.

Kĩ thuật này có thể thực hiện được là do một số tính chất của ngôn ngữ HyperText Markup Language (HTML) đã bị lợi dụng. Ngôn ngữ HTML cung cấp thẻ iframe có chức năng hiển thị nội dung của các trang web khác trên trang web hiện tại. Mỗi phần tử của một trang web (HTML Element) có ba chế độ đó là hiển thị, làm mờ và bị ẩn. Nếu các HTML Element chồng lên nhau thì thứ tự của nó được quyết định bởi một tham số gọi là z-index.

Như vậy ở trong trường hợp này, trang giao dịch ngân hàng đã được dùng thẻ iframe để tải về và chạy trên trang web của hacker, đồng thời được thiết lập z-index để đặt trước tất cả các thành phần khác nhưng lại tồn tại ở trạng thái ẩn. Một trang web thông báo trúng thưởng được cho hiển thị trên màn hình nhưng hoàn toàn không có ý nghĩa, vị trí của nút "NHẬN THƯỞNG" chính là vị trí của nút "CHUYỂN KHOẢN" đã được ẩn đi. Chúng ta có thể hình dung trang web như sau:



Hình 3. Mô tả cách mà trang web được hiển thị và trang bị ẩn đi

Đối với người dùng, khi họ nhấn nút "NHẬN THƯỞNG" cũng là lúc tiền được chuyển đi. Như vậy, các giao dịch nhạy cảm liên quan đến dịch vụ ngân hàng được ẩn ngay trước mắt người dùng nhưng họ không hề hay biết, và hậu quả gây ra có thể là rất lớn.

2.1.2. Một số kĩ thuật tấn công Clickjacking

Clickjacking là một dạng tấn công kiểu lừa đảo, do đó nó không yêu cầu quá cao về mặt kĩ thuật, mà chủ yếu khai thác ở yếu tố con người. Thực tế chỉ ra rằng đối với mọi cơ chế bảo mật, yếu tố con người là quan trọng nhất và cũng dễ bị khai thác nhất. Việc tấn công dò tìm tài khoản, đoán mật khẩu đối với hacker khó hơn nhiều so với việc lợi dụng sự sơ ý của người dùng để chiếm đoạt thông tin. Clickjacking có thể được sử dụng với nhiều kĩ thuật đa dạng, từ đơn giản đến nâng cao. Trong phần tiếp theo, tôi sẽ đề cập đến một số kĩ thuật đặc trưng nhất của Clickjacking.

**** Tương tác với frame ẩn***

Kĩ thuật này được trình bày ở ví dụ trên, lợi dụng các tính năng được cung cấp của ngôn ngữ HTML và Cascading Style Sheets (CSS) đó là thẻ iframe và chỉ số z-index. Trong HTML, thẻ iframe được dùng để tải và chạy các trang web khác trên trang hiện tại. Một thẻ iframe có thể được khai báo như sau:

```
<body>
<iframe src="../transfer.html" width="555" height="200">
</iframe>
</body>
```

Trong đó, src="../transfer.html"là địa chỉ trang web muốn tải về. Hacker sẽ tạo một iframe tải nội dung của các trang nhạy cảm như giao dịch ngân hàng, khai báo thông tin tài khoản… về trang của mình, việc tải qua iframe này vẫn cung cấp đầy đủ chức năng bình thường như khi ta truy cập vào chính trang web đó.

Hình 4. Website của ngân hàng BIDV được tải về và chạy bình thường sử dụng thẻ iframe tại thời điểm bài báo

Đoạn code giúp tải nội dung về có thể được viết đơn giản như sau:

```
    <head>
          <title>Chúc mừng bạn đã trúng iPhone</title>
    </head>
    <body>
          <iframe src="http://www.bidv.com.vn/" width="100%"
height="100%" id="bank" frameborder="0" scrolling="yes">
          </iframe>
    </body>
```

Ở ví dụ trên, trang giao dịch của ngân hàng BIDV được tải về trên trang web của hacker bằng thẻ iframe, kết hợp cấu hình thêm một vài tham số như width="100%"height="100%"frameborder="0", trang giao dịch này đã có thể hiển thị và hoạt động bình thường như khi truy cập vào địa chỉ chính chủ.

Tuy nhiên, điều nguy hiểm là hacker không để người dùng thấy được trang này, mà ẩn giấu nó bằng thiết lập z-index. Trong CSS, z-index là tham số thiết lập thứ tự xếp chồng lên nhau của các thành phần HTML, mặc định là 0 và thành phần nào có z-index lớn hơn sẽ ưu tiên xếp cao hơn, nghĩa là được ưu tiên hiển thị hơn. Ở đây, hacker thiết lập z-index=-1, do đó thành phần nguy hiểm này sẽ được ẩn mình sau các HTML Element khác, ngay trước mắt nhưng người dùng không nhận ra. Khi đó, họ vô tình thao tác trên một trang web nguy hiểm mà không hề hay biết.

**** Sửa đổi vị trí con trỏ chuột***

Đây là kĩ thuật sử dụng các tính năng của Javascript, hacker không cần thiết phải dụ người dùng click vào một điểm nào đó trên màn hình nữa, mà chúng có thể kiểm soát được vị trí của con trỏ chuột. Đồng thời, kết hợp với việc thay đổi vị trí của các đối tượng trên trang web, khi người dùng click chuột vào bất kỳ điểm nào thì vị trí đó đều đang chứa những liên kết độc hại.

**** Một số kĩ thuật tấn công Clickjacking nâng cao***

Dựa vào ý tưởng chủ đạo trên, hacker có thể phát triển thêm những kĩ thuật phức tạp hơn, giúp ẩn mình tốt hơn, tăng khả năng thành công và lượng thông tin thu thập được. Các kĩ thuật tấn công nâng cao có thể sử dụng đến gồm có:

- Sử dụng các đoạn mã Java và Javascript, hacker không những kiểm soát được thao tác click chuột, mà còn có thể thực hiện kéo-thả các đối tượng như dịch chuyển một đoạn text vào form dữ liệu hay chuyển ra khỏi iframe. Qua đó, hacker có thể thu được các thông tin nhạy cảm như tài khoản ngân hàng, mật khẩu đăng nhập.

- Hacker có thể lợi dụng lỗ hổng cross site scripting của các web site bằng cách chèn vào URL của các web site này một script điều hướng

http://myidol.com.vn/home/search.php?q=%3Cscript+type%3Dtext%2Fjavascript+src%3D%22http%3A%2F%2F192.168.0.207%3A3000%2Fhook.js%22%3E%3C%2Fscript%3E.

Khi người dùng click vào link chứa URL trên, người dùng sẽ bị điều hướng tới web site chứa một đoạn mã độc java script (như URL trên thì đoạn mã độc là Hook.js). Sau đó, đoạn mã độc này sẽ được tiêm nhiễm vào trình duyệt của người dùng và Hacker hoàn toàn có thể kiểm soát hay điều khiển trình duyệt. Khi đó, Hacker tạo ra những thông báo giả mạo như update flash và chèn tiếp mã độc reverse shell giả mạo phần mềm flash, khi người dùng cài đặt phần mềm này thì Hacker sẽ chiếm toàn quyền sở hữu máy của người dùng. Hay Hacker có thể tùy ý tạo ra những Plugin giả mạo khác để dụ người dùng click vào và lấy cắp thông tin người dùng như các tài khoản quan trọng.

- Thiết kế một iframe ẩn theo dõi sự di chuyển hay điều khiển vị trí của con trỏ chuột, đồng thời kiểm soát thời điểm click chuột. Điều này có thể thực hiện được bởi các tính năng trong Javascript. Từ đó, hacker có thể "chiếm đoạt" các sự kiện click chuột mà không cần quan tâm nó đang ở vị trí nào, hoặc tạo ra một cuộc tấn công multi-click liên tục, được hoàn thành sau một số lần click chuột. Kết thúc cuộc tấn công, hacker sẽ trả lại quyền kiểm soát con trỏ. Ở đây, người dùng chỉ thấy một số thao tác lạ so với bình thường nhưng khó có thể nhận ra mình đang bị tấn công như thế nào.

- Sử dụng các lỗ hổng trong các phần mềm tiềm ẩn nhiều rủi ro như Adobe Flash, ActiveX hay Microsoft SilverLight. Google cũng đã ghi nhận sự xuất hiện của dạng tấn công Clickjacking trên hệ điều hành Android của họ.

**** Một số biện pháp phòng chống tấn công Clickjacking***

Tấn công Clickjacking là một dạng tấn công lừa đảo, hậu quả gây ra cho người dùng cá nhân là khá đa dạng. Ban đầu, kĩ thuật này được sử dụng để nhằm lôi kéo người dùng đến các trang quảng cáo hay các bài viết nhạy cảm. Các hệ thống quảng cáo của Google, Microsoft … tính số lần click chuột vào banner để tính ra số tiền phải trả. Sử dụng Clickjacking, hacker có thể điều hướng người dùng đến các trang quảng cáo, "chiếm đoạt" những cú click chuột của họ và tiền sẽ được đưa về tài khoản của chúng. Facebook cũng từng là nạn nhân của Clickjacing khi người dùng vô tình nhấn vào các đường link làm lây lan các mã độc hại hay đơn giản là "like" một Page nào đó. Tấn công dạng này khá phổ biến trên Internet, đến nỗi nhiều người xem đó là điều hiển nhiên khi truy cập web, dẫn tới tâm lý chủ quan, xem nhẹ tính bảo mật.

Đối với các kĩ thuật tấn công Clickjacing nâng cao, hacker không những chiếm đoạt cú click chuột mà còn cả các đoạn text. Chúng có thể chứa thông tin tài khoản ngân hàng, mật khẩu hay các thông tin nhạy cảm. Thiệt hại có thể xảy đến với người dùng là rất lớn.

Để phòng chống tấn công Clickjacking, hai yếu tố cần được quan tâm đó là con người và kĩ thuật. Trong đó, yếu tố con người có vai trò quan trọng, đặc biệt là với các dạng tấn công lừa đảo. Người dùng cần có hiểu biết cơ bản về bảo mật thông tin, có ý thức cảnh giác khi truy cập vào các trang web lạ và các hành động lạ, đặc biệt cảnh giác trước các lời dụ dỗ, món hời trên Internet.

Có khá nhiều phương pháp khác nhau để phòng chống Clickjacking, trong phạm vi bài báo, tôi đề cập đến một số phương pháp hiệu quả nhất, được thực hiện ở cả hai phía: máy chủ cung cấp dịch vụ và người dung internet.

**** Ở phía Máy chủ web***

- *Kĩ thuật Framebuster*: Kĩ thuật đầu tiên có thể kể đến là sử dụng các kịch bản Javascript đặc biệt nhằm ngăn chặn việc tải nội dung trang web vào trong một frame. Những đoạn mã như thế được gọi là framebuster, chúng tôi đề xuất viết như sau:

```
<script>
    if(top!=window)
    {top.location=window.location}
</script>
```

Ở kịch bản framebuster trên, một điều kiện được kiểm tra đó là trang web được tải có phải nằm trong một frame hay không. Nếu trang làm việc hiện tại không phải là trang cao nhất (được hiển thị) thì trang cao nhất sẽ được gán lại để hiển thị ra cho người dùng. Tuy nhiên, trong thực tế kĩ thuật này chưa hoàn toàn đảm bảo để chống lại Clickjacking.

- *Kĩ thuật X-Frame-Options:* X-Frame-Options Header là một tùy chọn ở máy chủ, thông báo cho trình duyệt rằng website này có cho phép được nhúng vào trong các thẻ frame, iframe hay không. Header này xuất hiện vào năm 2009 và hiện tại đã được hầu hết các trình duyệt hỗ trợ. Có ba giá trị tùy chọn của X-Frame-Options gồm có:

```
X-Frame-Options: DENY
X-Frame-Options: SAMEORIGIN
X-Frame-Options: ALLOW-FROM https://example.com/
```

Ở đây, chúng tôi đề nghị chọn DENY: cấm hoàn toàn việc tải trang Web vào trong frame. Cụ thể chúng tôi đưa ra một số giải pháp như sau

- Đối với máy chủ Apache:

```
Header always set X-Frame-Options DENY
```

- Đối với máy chủ Lighthttpd:

```
server.modules += ("mod_setenv")
$HTTP["scheme"] == "https"
{
setenv.add-response-header
= ("X-Frame-Options" => "DENY")
}
```

Sau khi cuộc tấn công Clickjacking gây ra thiệt hại và được phát hiện, các nhà cung cấp dịch vụ Web lớn đã cảnh giác hơn với nó. Facebook, Twitter hay GitHub đều đã cấu hình X-Frame-Options giúp chặn dạng tấn công này.

- *Kĩ thuật sửa lỗi XSS để tránh bị hacker kết với hợp Clickjacking:* XSS là lỗi ở Server có thể gây nguy hiểm lớn cho người dùng, tuy nhiên lại không quá khó để phòng tránh. Bản chất của XSS cũng là không kiểm soát kĩ dữ liệu nhập vào như SQL Injection. Biện pháp đưa ra là kiểm duyệt kĩ dữ liệu vào, chặn các từ khóa nguy hiểm.

Một phương pháp hiệu quả khác là mã hóa các ký tự đặc biệt của dữ liệu vào, sử dụng hàm htmlentities() của HTML, như sau:

```
echo htmlentities($row["content"]);
```

Phương pháp trên cũng có thể được sử dụng với ASP, JSP.

**** Ở phía người dùng***

Về phía người dùng, trước hết cần nâng cao nhận thức về vấn đề bảo mật khi truy cập Internet, thận trọng với các giao dịch, thao tác nhạy cảm trên mạng.

Về kĩ thuật, có thể sử dụng một số phương pháp sau: Cài đặt Add-on vào trình duyệt để ngăn chặn việc chạy Flash hay Javascript, như NoScript của FireFox hay Clickjacking Reveal của Chrome. Tuy nhiên điều này có thể gây ra một số phiền toái trong quá trình duyệt web; Thường xuyên cập nhật các bản nâng cấp của trình duyệt, hệ điều hành và các bản vá lỗi từ nhà sản xuất; Cẩn thận với các thao tác lạ, các "món quà" bất ngờ từ Internet; Cẩn thận với các URL thiếu tin cậy trên mạng; Cài đặt các phần mềm Anti Virus mạnh và thường xuyên update.

3. Kết luận

Clickjacking là dạng tấn công phổ biến, tuy không yêu cầu kĩ thuật khai thác quá cao nhưng hậu quả gây ra có thể rất nghiêm trọng. Đây là cuộc tấn công mang các đặc trưng của dạng tấn công lừa đảo, do đó ngoài vấn đề kĩ thuật, yếu tố con người là quan trọng trong việc phòng chống, phát hiện và tránh bị rơi vào bẫy mà hacker dựng sẵn. Các dạng tấn công gây thiệt hại hay gián vào các máy chủ cung cấp dịch vụ như tấn công DDOS, SQL-Injection thường được giới truyền thông và chuyên môn chú ý nhiều hơn mà sơ ý bỏ qua các cuộc tấn công có mục tiêu nhằm đến các cá nhân sử dụng internet. Các nhà phát triển website cũng chưa thực sự chú ý đến Clickjacking. Hiện nay, ngoài các trang web lớn đã chặn iframe, vẫn có nhiều trang web nhạy cảm về lĩnh vực tài chính, ngân hàng trong nước cho phép tải trang của mình qua trang web khác. Hơn bao giờ hết, mỗi người dùng Internet phải tự trang bị cho mình những hiểu biết cơ bản về vấn đề an ninh bảo mật thông tin, để có thể "an toàn" trên không gian mạng, đặc biệt là trong thời đại Internet kết nối vạn vật như hiện nay.

TÀI LIỆU THAM KHẢO

[1] S.Paul, 2010. *Next Generation Clickjacking*. White paper.

[2] M. Balduzzi, M. Egele, E. Kirda, D. Balzarotti, C. Kruegel, 2010. *A Solution for the Automated Detection of Clickjacking Attacks*.

[3] G. Rydstedt, E. Bursztein, D. Boneh, C. Jackson, 2010. *B. Busting: A Study of Clickjacking Vulnerabilities on Popular Sites*. Stanford University.

[4] L. Huang, A. Moshchuk, H. Wang, S. Schechter, C. Jackson, 2012. *Clickjacking: Attacks and Defenses.*

[5] A.Narayanan, 2012. *Clickjacking Vulnerability and Countermeasures*, Foundation of Computer Science FCS, New York, USA.

[6] H. Shahriara, V. Devendran, 2014. *Classification of Clickjacking Attacks and Detection Techniques*, Kennesaw State University, Kennesaw, Georgia, USA.

ABSTRACT

Clickjacking attack prevention using various techniques

Nguyen Dang Tien

People's Police University of Technology and Logistics, Bac Ninh, Vietnam

In this paper, we propose some methods of Clickjacking attacks to prevent a very popular online fraud (phishing). This is an attack method that users access the applications via browsers; victims are cheated and manipulated on the fake website created by the hacker. These sites are usually hiding under the guise of a secure site. Clickjacking attack does not require high technical, but the consequences may be serious. The consequences may cause a nuisance for users, more heavily account information or other types of sensitive data may be stolen. We also offer a number of insurance methods to Web servers and users to prevent clickjacking attack effectively.

Keywords: Clickjacking attack, iframe tag, hacker, set the z-index, internet service.