Web Spoofing: An Internet Con Game

Edward W. Felten, Dirk Balfanz, Drew Dean and Dan S. Wallach

November 24,1999

Presented by Nadeem Ilkal

1 Introduction

This paper describes an Internet security attack that could endanger the privacy of World Wide Web users and the integrity of their data. The attack can be carried out on today's systems, endangering users of the most common Web browsers, including Netscape Navigator and Microsoft Internet Explorer. Web spoofing allows an attacker to create a "shadow copy" of the entire World Wide Web. Accesses to the shadow Web are funneled through the attacker's machine, allowing the attacker to monitor all of the victim's activities including any passwords or account numbers the victim enters. The attacker can also cause false or misleading data to be sent to Web servers in the victim's name, or to the victim in the name of any Web server.In short, the attacker observes and controls everything the victim does on the Web.

2 Web Spoofing

Web spoofing is a kind of electronic con game in which the attacker creates a convincing but false copy of the entire World Wide Web. The false Web looks like the real one: it has all the same pages and links. However the attacker controls the false Web, so that all network traffic between the victim's browser and the Web goes through the attacker.

- **Surveillance** : The attacker can passively watch the traffic, recording which pages the victim visits and the contents of those pages.
- **Tampering** : The attacker is also free to modify any of the data travelling in either directon between the victim and the Web. The attacker can modify form data submitted by the victim.

3 Spoofing the Whole Web

You may think it is difficult for the attacker to spoof the entire World Wide Web, but it is not. The attacker need not store the entire contents of the Web.

the whole Web is available on-line; the attackers server can just fetch a page from the real Web when it needs to provide a copy of the page on the false Web.

4 How the Attack works (URL Rewriting)

The key to this attack is for the attacker's Web server to sit between the victim and the rest of the Web. The attacker's first trick is to rewrite all the URLs on some Web pages that they point to the attacker's server than some real server. Assuming the attacker's server is on the machine `www.attacker.org` the attacker rewrites the URL by adding `http://www.attacker.org` to the front of the URL. For example, `http://home.netscape.com` becomes `http://www.attacker.org/http://home.netscape.com` Once the attacker's server has fetched the real documet needed to satisfy the request, the attacker rewrites all the URLs in the document into the same special form by splicing `http://www.attacker.org` onto the front. Then the attacker's server provides the rewritten page to the browser. Since all the URLs in the rewritten page now point to www.attacker.org, if the victim follows a link on the new page, the page will again be fetched through the attacker's server. Thevictim remains trapped in the attacker's false Web and can follow links forever without leaving it.

5 "Secure" Connections don't help

One distressing property of this attack is that it works even when the victim requests a page via a secure connection. If the victim does a "secure" web access (a Web access using the Secure Sockets Layer) in a false Web, everthing will appear normal: the page will be delivered, and the secure connection indicator (usually an image of a lock or key) will be turned on. The victim's browser says it has a secure connection because it does have one. Unfortunately the secure connection is to www.attacker.org and not to the place the victim thinks it is. The victim's browser thinks everything is fine: it was told to access a URL at www.attacker.org so it made a secure connection to www.attacker.org. The secure-connection indicator only gives the victim a false sense of security.

6 Starting the Attack

To start an attack, the attacker must somehow lure the victim into the attacker's false Web. There are several ways to do this. An attacker could put a link to a false Web onto a popular web page. If the victim is using web-enabled email, the attacker could email the victim a pointer to a false Web, or even the contents of a page in a false Web. Finally the attacker could trick a Web search engine into indexing part of a false Web.

7 Completing the Illusion

The attack described so far is fairly effective but not perfect. However it is possible for the attacker to eliminate virtually all of the remaining clues of the attack's existence.

- **The Status Line** : When the mouse is held over a Web link the status line displays the URL the link points to. second when a page is being fetched, the status line briefly displays the name of the server being contacted. The attacker can cover up both these cues adding a Javascript program to every rewritten page. Since JavaScript programs can write to the status line and since it is possible to bind avaScript actions to the relevant events, the attacker can arrange things so that the status line participates in the con game, always showing the victim what would hvae been on the status line on the real Web. This makes spoofing even more convincing.

- **The Location Line** : The attack as described so far causes a rewritten URL to appear in the location line, giving the victim a possible indication that an attack is in progress. again a JavaScript program can hide the real location line and replace it by a fake location line that looks right and is in the expected place. The fake location line can show the URL the victim expects to see. The fake location line can also accept keyboard input, allowing the victim to type in URLs smoothly. The JavaScript program can rewrite typed-in URLs before they are accessed.

- **Viewing the Document Source** : A user could possibly look for rewritten URLs in the HTML source and could therefore spot the attack. The attack prevents this by using JavaScript to hide the browser's menu bar, replacing it with a menu bar that looks like the original. If the user chose “view document source” from the spoofed menu bar, the attacker would open a new window to display the original(non-rewritten) HTML source.

8 Short-term Solution

The best defense is to follow a three-part strategy :

1. Disable JavaScript in your browser so that the attacker will be unable to hide the evidence of the attack.

2. Make sure your browser's location line is always visible.

3. Pay attention to the URLs displayed on your browser's location line, making sure they always point to the server you think you're connected to.

This strategy will significantly lower the risk of attack, though you could still be victimized if you are not conscientious about watching the location line.

9 Long-term Solution

Changing browsers so they always display the location line would help although users would still have to be vigilant and know how to recognize re-written URLs. This is an example of a "trusted path" technique in the sense that the browser is able to display information for the user without possible interference by untrusted parties. For pages fetched via a secure connection an improved secure-connection indicator could help. Rather than indicating a secure connection, browsers should clearly say who is at the other end of the connection.

10 Conclusion

The paper describes an important Internet security attack which is not difficult but rather effective. Using this attack the attacker can observe and control everything the victim does on the Web. This makes Web spoofing a dangerous and nearly undetectable security attack. Some short-term and long term solutions have be proposed but unfortunately no long-term solution to this problem is known.