Web Spoofing a Growing Internet Concern...

By Chet Hosmer, President & CEO
WetStone Technologies, Inc.

As on-line shopping, banking, day trading, and virtual auctions become part of our daily Internet life, the question is regularly raised as to whether these types of electronic transactions are safe. Analyzing the global web experience on face value, most people believe that online transactions are relatively safe. Many of us are still concerned about using our credit card widely on the web, but even the most skeptical among us has probably purchased a book or two from Amazon.com.

So What's The Problem?

If we always work with reputable merchants, are careful about what we download, religiously run the most recent version of our virus software, and update our browsers with the latest patches we should be fine!…. right? Maybe not! In searching for the answer to that question, one has to consider the daily exploits perpetrated against corporate, government and law enforcement web pages. Some of the most prominent locations on the web have been easy targets of web graffiti assassins, and have been either taken over or hijacked. These assassins have gained notoriety for breaking the web security of the New York Times, the FBI, the Supreme Court, the Central Intelligence Agency and even Jack Daniels. What has become a greater concern is that these same techniques used by the graffiti artists can and are being used to perpetrate crimes against web users.

How Does It Work?

The attack is called Web Spoofing and is very similar in nature to the “man-in-the-middle” attack used on dial-up networks. It is not within the scope of this article to describe how the web pages are changed, but since these types of attacks are launched hundreds of times a day without much difficulty, it’s clear that web servers are vulnerable to malicious content changes.

Currently, in most of the highly publicized graffiti attacks perpetrated against web servers, the changes are made in an obvious way to attract attention and ridicule the organization, whereas Web Spoofing is almost unnoticeable to the web page visitor. The changes made are so small and buried in thousands of lines of HTML so that even a thorough inspection of the source could still miss the fact that link addresses within have been slightly modified.

I’ve chosen to use eBay.com in the following example. Clicking on the Antiques link (http://pages.ebay.com/antiques-index.html) indicated on the actual eBay main page takes you to auctions involving antiques, as one would expect. However, if the link is modified in a subtle way, for even a very short time interval (only minutes), a great number of unsuspecting users will be spoofed.

The following is a simple change a criminal could make to the HTML code shown above for the Antiques link by hacking into a web provider’s site. Notice that in the following address, only a 1-character change would be needed to pull off the spoof:

http://pages.ebay.com/antiques-index.html

It is important to note that this change in the HTML would have little visual effect on the page. Although most browsers will display the link in the bottom window when the cursor is placed over a clickable region, a minor change in a long string of characters would probably go unnoticed by the majority of users. And unfortunately we can also spoof that visual cue by adding some additional JavaScript code. This innocuous change sends the user click (web page request) to the Internet server ebay.com instead of ebay.com.

What happens next is actually quite straightforward. The spoofed user request is routed to eBay.com...
(instead of ebay.com), which is being controlled by the criminals. The criminal server corrects the spoofed request (changes eby to ebay) and forwards it to the actual ebay server. The ebay server responds with the corresponding page to the criminally controlled server. The perpetrator could simply reply back to the unsuspecting user with the correct page supplied from ebay. However this is the point that the hacker intercept provides the opportunity to perform some additional actions.

In order to keep the spoof going as long as possible and collect as much information as possible from the unsuspecting user, the hacker intercept server modifies the page received from ebay. All references to ebay.com are changed to eby.com throughout the page and it is then sent off to the user. Nothing looks visibly different to the unsuspecting user and depending on the hacker intercept capabilities, the user shouldn’t even notice the slight delay introduced by the intercept. The user, unaware of the intercept, continues on with his business at ebay…. but with the folks at eby.com watching his every move!

Another artifact of this kind of attack is that the pages returned by the hacker intercept are stored in the user’s browser cache, and based on the additional actions taken by the user, the spoofed pages may live on long after the session is terminated.

Threats Imposed By Web Spoofing

Assuming that the hacker intercept is successful, all requests, forms and scripts transmitted back and forth will be intercepted by the hacker. This means that sites visited, web based logins, user ID’s and password are easily captured. Also, credit card numbers (even those using secure transactions) can be captured once the user has been spoofed. And, if you are using web based e-mail services such as hot-mail, yahoo etc. all of your e-mail conversations can be captured by the intercept.

Web Spoofing is a serious problem that is becoming more prevalent, and must be addressed by the web community if we are to conduct our lives and our business through the Internet.

What Can be Done?

Web site providers must maintain better control of site content and immediately react and correct modified web content. They need to continually monitor the integrity of what they are presenting to the world, and to detect and react to both graffiti attacks and the more subtle but threatening Web Spoofing attacks immediately. Actually, the web server provider may potentially have some liability if a user is spoofed when being provided services through their site.

As web surfers and users we must always be wary of the content of the web pages we surf, look for clues to spoofing, and report immediately to the providers. NEVER click on a link provided to you in an e-mail from someone you don’t know or trust. This is a very easy way to get you to that Hacker Intercept site! As an example, let’s say you get the following e-mail from someone claiming to know you.

Hi Johnny,

I found this new book on gardening on Amazon and I thought you would enjoy it. Check it out...

Square Foot Gardening – Mel Bartholome

Love,
Mom

Close inspection of the link above provides the following:


The link points to amazone.com instead of amazon.com. Everything else in the link is genuine. So before buying this great new book recommended by Mom, you’ll be stopping by and visiting the folks at amazone.com and giving them your credit card number, expiration date, name, address and phone.

Copyright © 2000, WetStone Technologies, Inc.