Web Spoofing For User Security Awareness

Pooja Kalola
M.Tech I.T.
Patel College of Science & Technology, Indore

Sachin Patel
HOD of IT Dept.
Patel College of Science & Technology, Indore

Chirag Jagani
Assistant Professor
M. & N. Virani Science College,Saurashtra Uni.

ABSTRACT

Web spoofing is the process of creating a shadow of an original web site that a user requests to access. The fraudulent web site looks similar, if not identical, to an actual site, such as a bank web site. An attacker who intercepts the request to a web site and replaces it with another modified one creates the shadow. When a victim is at the spoofed site, not only can the attacker see the information that the victim types, such as internet banking username, password, credit card information, and social security number, but the attacker can make changes to the data that the victim receives. In this paper, we present details of web spoofing, including research, history, how attacks occur, what damages it can do to victims, and how users can protect themselves from web spoofing.

Keywords

Web Spoofing, Security, Client, Server, credit card information

1. INTRODUCTION

Web spoofing occurs when a user requests access to a web page and an attacker intercepts the request and creates a shadow copy of the requested web page [4]. After this, all of the communications takes place between the victim's machine and the attacker's server.

In effect, web users are redirected through the attacker's machine, allowing the attacker to monitor and control the victim's activity on the web. An example of this activity could be typing internet-banking information such as login name, password, account number, etc. The attacker can change the data before transmitting back to the victim. Web spoofing is also referred to as an "internet con game."

Internet users generally face three types of spoofing attacks: web spoofing, IP spoofing, and email spoofing. Although the goal of all three types is to attack a network and get users' personal information, they work differently. In web spoofing, as described above, a middleman intercepts theclient's request to a web page, replaces it with another page, and then transmits it to the victim.

In IP spoofing the attacker gains unauthorized access to a victim's computer by pretending it comes from a trusted server [12]. The attacker must first find the IP address of a trusted host and then modify the headers of the packet (data traveling on internet broken into small pieces called packets) in a manner to make it appear that the packets are coming from a trusted host. The attacker fools the victim into believing that he communicates with a trusted source. As a result, the attacker sees the victim's communication. Some examples of recent IP spoofing attacks include man-in-the-middle, routing redirect, source routing, blind spoofing, and flooding SYN (SYN is a flag that is set in each packet that requests the opening of a new connection to the server from the spoofed IP address.)

Similar to IP spoofing, email spoofing occurs when users receive an email that appears to have initiated from a known and trusted source when it actually came from a different source. The purpose of email spoofing is to make the victim believe that the email came from well- known financial or commercial organizations so the receivers reveal their personal information [1]. Fraud of this type is very common and CERT (Computer Emergency Response Team), a Carnegie Mellon University organization that publishes security vulnerabilities and attacks by hackers on public internet users, data shows that about five percent of users are being fooled this way and do reveal their personal information. Suggestions on how to react to email spoofing are available on CERT web site.

The spoofing techniques described here are called internet phishing. Our focus in this paper is on web spoofing. The organization of the paper is as follows. Section 2 presents the web spoofing research. Section 3 discusses how web spoofing works. Section 4 introduces web spoofing history. Section 5 summarizes different ways to protect against web spoofing. Conclusion remarks explained in section 6.

2. WEB SPOOFING RESEARCH

Researchers at Princeton University first introduced web spoofing in 1996 [4]. In their experiment, theyused JavaScript to rewrite the URL for the web page that users request. For example, if a user tries to access the http://www.good.org, the attacker will replace this URL with the http://www.bad.org/ http://www. good. org. This causes the victim's request to go through the attacker's server, which can then view victim's data and change some information before it is transmitted to the victim. This kind of attack is possible by intercepting the communication between a web user and the destination server the user is intending to access. This is called the man-in-the middle attack.

Web spoofing has also been reported in a related but independent work [11]. They simulated the attack by inserting some Java applets into a victim's machine using the destination page the victim intended to access. Upon execution of the applet by the victim, a Trojan horse will be saved on the victim's machine. In addition, it will pop up a small window asking for login id and password. If the user enters the requested information, the Trojan horse captures it and then transfers the information to the attacker's machine.

In another report [3] researchers used Java and JavaScript to launch two kinds of attacks in browsers. The first one, a Java applet, embedded in a HTML document, and then saved it on a client machine. After this, every time the client tries to launch a web page with the embedded Java applet, new Java threads are created and started, which in turn create and collect information such as login id and password and

transmit them to the attacker's machine. In their second attack, they used a different java applet to detect clients' activities on the internet. Once a client is on a sensitive website, such as online banking, the applet then displays a fake website that can be used to steal sensitive information including credit card numbers, etc.

Researchers at Dartmouth College [13] reported their work as an extension of the previous works on web spoofing. They demonstrated that although modern browsers have fixed some of the previously known vulnerabilities, the attackers have also become more sophisticated and many browsers are still vulnerable to this kind of attack. They also demonstrated that malicious servers could forge all of the SSL (Secure Socket Layer), a protocoldeveloped by Netscape for transmission of data over the internet. SSL uses a private key for data encryption. Both Netscape Navigator and Microsoft Internet Explorer support SSL. SSL is popular among web sites for secure data transmission, such as credit card numbers. By convention, URLs that require an SSL connection start with https. The researchers have forged an SSL session by creating an SSL icon, which leads the client to believe that the session with their desired page is secure even though there was no SSL connection and therefore not secure. This is accomplished by faking a website and opening a new window for the client when he is requesting access to a webpage. The new windows address location, appearance, name, and content information looks exactly as the clients expect it. For example, if the user is trying to access the Chase Bank web page, the browser opens a new window that looks exactly like the Chase bank web site with secure SLL being on. Consequently, all users' activities can be captured and modified by the attacker's server.

3. HOW WEB SPOOFING WORKS

3.1 Browsers-Server Interactions

Generally, people request access to a web site Through their web browser such as Netscape, Firefox, Microsoft Internet Explorer, etc., by typing the URL (Universal Resource Locator) of the their desired web site, e.g. www.google.com. The first part of the URL consists of host name and the second part is DNS (Domain Name Server). In the case of "http://www.google.com", the host name is "www" and the DNS is "google.com".

When users enter this in a web browser address field, the browser typically uses the DNS resolver on the system to determine the IP address of host "www" in domain "google.com". The above process is a normal user web page interaction and is based on the assumption that everything works smoothly. However, sometimes when a client types a URL in their browser to request a web site, instead of the browser going directly to the requested site's server it may go through a "middleman". The middleman can change the URL and send it back to the client.

For example. If the actual URL is http: // www. good. com, the middleman changes it to http: // middleman /http: //www.good.com. As a result, the browser thinks http://middleman is the web server location and http://www.good.com is the content the client is trying to get. The middleman web server sees the requested URL, knows that http://www.good.com is where the client wants to go, and calls that server for the client. After it makes a copy of all the pages the client requested, the middleman changes the entire special HTML commands that may reference a URL and changes them before giving it back to the client. Table 1 shows some examples of the HTML commands that have URLs [6].

TABLE 1

Some examples of html commands that have urls

URL	Description
<A HREF="URL">	A link to something
<APPLET CODEBASE="URL">	To define a java applet location
<AREA HREF="URL">	To define the area of a section
<BODY BACKGROUND="URL">	To define the background image
<EMBED SRC="URL">	To insert an object into a page
<FORM SRC="URL">	To define a form
<FRAME SRC="URL">	To define the source for a frame
<IMG SRC="URL">	To display an image
<INPUT "URL">	To define the source for input
<META URL="URL">	To perform a client side pull

3.2 Involving a Middleman

The client-server communication is set so that all requests to a web site go through a proxy server. The proxy server is a server that allows users to connect to their desired server through the proxy. The requests first go through the proxy and then the proxy connects to the desired server. The proxy has the authorityto change the requested URL. One advantage of a proxy server is the reduction of network traffic and user wait times to distribute and manage information. A proxy server can help relieve bandwidth congestionat network bottlenecks and ensure that users are securely and productively access network resources.

Use of a proxy server is a good security precaution but it does not prevent web spoofing attacks. It is possible to insecurely configure Web proxy servers, which then can be exploited by a remote attacker to make arbitrary connections to unauthorized hosts. Problems with engine such as Google, Alta Vista, Yahoo, etc., they are taken to the attacker's server. For example, a search result for SunTrust bank's web site may return http://www.SunTrustBank.com. Unfortunately, users may be unaware that the SunTrust bank's actual website is http://www.SunTrus.com and may accept the first site as legitimate and start interacting with the site. Consequently, they are vulnerable to a web spoofing attack.

The above techniques, makes it possible for the middleman to reside between a client's web browser and a requested server. From this point onward, the middleman can intercept all of the client's activities including any URL requests. The middleman then requests the desired website on behalf of the client, makes a copy of it, possibly changes it, and then transfers them to the client. As a result, the middleman controls all of the client's activities and can view everything the client types including bank account id, passwords, and social security number.

4. HISTORY OF WEB SPOOFING

In this section we report some incidents of web spoofing in the past few years. An incident of web spoofing happened in 1997 when Eugene Kashpureff, founder of AlterNIC.com, detected a flaw in the InterNIC Company's Domain Name Service (DNS). InterNIC is a company that controls the registration of most domain names on the Internet. People can

contact the company and make sure that the domain name is registered under the same company with whom they plan to do business. Kashpureff exploited the flaw by redirecting the users of the InterNIC to his web site. As a result, many users who were trying to reach www. Inter NIC .net found themselves unknowingly at Kashpureff's site.

Sullivan at his interview with MSNBC [9] explained how attackers established a hostname called PayPai to fool people into thinking that it is the PayPal host. The attackers used email spoofing and provided the PayPi.com in the email. The email asked the user to login to the site and update their PayPal account information. Once the user has entered their personal information such as login id and passwords, the attackers can use them for illegal activities. This attack was possible because many users could not distinguish between a lower 'I' and 'l'.

In January 2003 the Citibank web site was spoofed. A hacker sent an email to Citibank customers asking them to login to their account and update their banking information. The customers were advised to use the URL that was provided in the email. When they clicked on the link provided by the hacker, they were taken to a page that looked exactly like the Citibank page. This attack was possible by exploiting an unpatched Internet Explorer vulnerability. By exploiting this vulnerability, the hacker was able to modify the HTML file such that the URL displayed in the address bar was exactly the Citibank address and the user had no idea that they were not at the Citibank's site. Since then Microsoft has fixed this vulnerability by providing appropriate patches.

As we mentioned before web spoofing, IP spoofing, and email spoofing collectively are called phishing. There is a non-profit organization, Anti-Phishing Working Group (APWG) [2], which collects and informs the public of any phishing activities. They have a monthly bulletin that reports any phishing activities on the internet. The APWG also may share the report of any phishing activity to law enforcement agencies. In the December 2005 issue of the APWG bulletin there were 15244 phishing reports. Most of these phishing reports target financial institutions. Other common victims of phished sites include eBay, PayPal, and Amazon.com [2].

On the Netscape and the Internet Explorer browsers, if Internet users work with JavaScript option enabled, then they leave the door open for possible spoofing.

5. AVOIDING WEB SPOOFING

Up to this point we are aware that a middleman can change the URL that a user is trying to access. The least that (s) he can do is to view critical personal information about the user as (s)he types this information. Even worse, a middleman can change the information before transmitting to the destination or to the user. An example of a change would be the modification of the recipient's address and the dollar amount of the user's bill payment. The question is what we can do to avoid this situation. Generally, there are two types of web access, as a manager to maintain the web or as a user.

A web manager can perform the following steps to avoid web spoofing [13]:

Using URL-link checker such as QuickCheck freeware software to ensure that the requested links point to expected locations. It provides a listing of all of the URL links that are referenced in a surfer's web pages. The list can be scanned for accuracy by the user. QuickCheck can check up to 10 URL's per hour and up to 50 per day. It generates a list of the URL's that have been visited and a system review list.

Using host security policies and procedures to ensure that critical files cannot be accessed and modified by unauthorized users. For example, the manager can impose some type of access control method to either deny access or log a message in that respect.
Organizations, especially financial organizations, should follow the recommendations of Comptroller of the Currency Administrator of National Banks.

A user who wishes to access a critical web site such as a bank or medical record can take the following steps to avoid possible attack:

Users should cut and paste the URL they are trying to go to into their web browser address location instead of clicking on the URL provided by adversaries [10]

Any browser has an option of showing the URL of the web page that users trying to access. Enabling this feature would allow the surfer to actually see the URL that is being accessed. It is recommended that users be especially cautious when they are trying to access critical web pages such as financial and banking web sites. In e-commerce this is especially important.

Online users should specifically be careful about giving out personal information such as credit card number, social security number, etc. Users are advised to double check the URL and make sure it is the intended web site. Users could also use the InterNIC WhoIs service to see if the domain is registered to the company with whom they believe they are dealing. Individuals can also call the InterNIC WhoIs to make sure that they dealing with appropriate company.

6. CONCLUSIONS

In this paper we have examined details of web spoofing including past research activities, history, and steps that users can take to avoid web spoofing. We should point out that there are two sides in any e-commerce activity, the customer, and the company. In our work we explained customers' responsibilities and actions that must be taken by them. However, companies, especially financial organizations, must also take appropriate steps in order to make sure that their company's website is secure and that appropriate procedures are in place to check for any suspicious activities. For example, the banking industries, in addition to using SSL, must monitor returned emails and web server logs and control their internet traffic for possible spoofing attacks.

7. REFERENCES

[1]Adida, Ben, David Chau, Susan Hohenberger & Ronald L. Rivest, "Lightweight Signatures and Encryption for Email", MIT Computer Science and Artificial Intelligence Laboratory Research Abstract, 2005. http://publications. csail.mit.edu/ abstracts/abstracts05/srh ohen3/srhohen3.html

[2] Anti-Phishing Working Group http://www.antiphishing.org

[3] De Paoli, F., A. L. DosSantos and R. A. Kemmerer "Vulnerability of 'Secure' Web Browsers." Proceedings of the National Information Systems Security Conference. 1997.

[4] Felten, E., D. Balfanz, D. Dean, and D. Wallach. "Web Spoofing: An Internet Con Game." 20th National Information Systems Security Conference. 1996

[5] http://www.cs.dartmouth.edu/~pkilab/demos/Spoofing.

[6] Web spoofing http://www.cs.princeton. edu/sip /WebSpoofing/http://bau2.uibk.ac.at/matic/spoofing.htm.

[7] Internet Assigned Number Authority Web Site, http://www.internic.net/

[8] Johnson, Brad C., "How Web Spoofing Works," A Prospective on Electronic Commerce," System Express, August1998. http://www.systemexperts.com/tutors/webspoof.pdf.

[9] Labor, Eric , "Dnssec: Security for Essential Network Services," LinuxSecurity.com, 2003 http://www.linuxsecurity.com/content/view/113965/151/

[10] Quick Check is a Free Online Link Checking and HTML ValidationService, http://www.elsop.com/linkscan/quickcheck.htm

[11] Sullivan. Bob, "Scam artist copies PayPalWeb site." MSNBC. http://www.msnbc.com/news/435937.asp?cp1=1#BODY , July 21, 2000

[12] Threats from Fraudulent Bank Web Sites, OCC Bulletin, 2005-24 http://www.occ.treas.gov/ftp/bulletin/2005-24.doc

[13] Tygar J. D., and Alma Whitten. "WWW Electronic Commerce and Java Trojan Horses." The Second USENIX Workshop on Electronic Commerce Proceedings.1996.http://www.cs.cmu.edu/People/decaf/usenix96/main.html

[14] Velasco, Victor, "Introduction to IP Spoofing" an Internet publication, 2000. http://www.wbglinks .net/pages/reads/wbgreads/ipspoof/ipspoof07.html http://www.cert.org/tech_tips/email_spoofing.html

[15] Zishuang Ye, Eileen , Yougu Yuan, and Sean Smith, "Web Spoofing Revisited: SSL and Beyond", Technical Report TR2002-417, Dartmouth College.