International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 9 Sep 2021, pp: 1679-1683 www.ijaem.net ISSN: 2395-5252

Web Spoofing Prevention:A User-focused Approach

Okerezi Goodnews E., Ahamba Ugochukwu Blessing, Uburu Elisha, Odion Victoria, Musa Tauheed Mohammed

Submitted: 15-09-2021 Revised: 25-09-2021 Accepted: 28-09-2021

ABSTRACT
The internet which encompasses all its services as well as its dependencies has a significant impact on our lives today, affecting education, business, finance and so forth. It is no wonder why it has become an active target of malicious individuals seeking to defraud and abuse the users of the Internet. This has resulted in anti spoofing research and development of applications to defend users of the internet. This paper will provide a review of research that has been done into spoofing and anti-spoofing, with a focus on the World Wide Web. After briefly introducing and describing various spoofing methods, as well as anti-spoofing techniques, an investigation which includes test scenarios and feedback analysis is carried out to identify what user-focused approach can be adopted in the direction of mitigating attacks particularly targeted at users of the Internet.

Keywords: Internet, web, spoofing, alert, sensitize

I. INTRODUCTION

It is hardly possible today to have a complete conversation without speaking of the internet. Undoubtedly, it has become an integral part of our lives. It has even become more so resulting from the expedient advent of smartphones and the Internet of things (IoT). As these devices continue to be churned out exponentially, the internet becomes even more rampant. This has no doubt brought about increased opportunities as individuals are daily capitalizing on the numerous positive benefits of the internet. A huge demand is as a result created for software designers and network engineers with skills in creating new internet-enabled applications or porting existing/legacy applications to the internet platform. We are constantly seeking for the best applications, so we can perform with different, fast, reliable, attractive and most important secure tasks (Halili, 2015).

Unfortunately however there exist individuals who decidedly use the internet for unbecoming activities. These individuals capitalize on the inherent lapses and vulnerabilities in the internet to launch attacks on unsuspecting members of the general public tricking or luring them into actions that have a potential to negatively affect their reputation as well as cause significant financial losses. The process of launching these attacks is referred to as spoofing. Many online service providers believe that their reputation is at stake and fear that users will lose confidence in electronic commerce (Kirda & Kruegel, 2005). The gravity of these attacks can be very severe. They can cost us millions in dollars and should not be overlooked or taken for granted by the internet security community (Babu et al., 2010). Despite the deployment of sophisticated cryptographic protocols (SSL/TLS), the web and its users are suffering from a growing number and different forms of malicious, criminal abuses, (Herzberg, 2006).

Over the years, much advancement has been made on configuring devices and applications to try to detect and block spoofing attacks. Yet failure scenarios continue to drive a wedge against these advancements. A critical look at a number of these advancements reveals an unamplified yet undeniable truth which is that every approach to this problem seems to rely on the vigilance of Web users. (Felten et al., n.d.) Can we realistically expect everyone to remain vigilant all of the time? This brings to the fore the need to give conscious attention to alerting and sensitizing users of the internet on these pitfalls.

In this article, investigation into alert mechanisms that can help us evoke and maintain the vigilance of users of the internet is done. The article is structured as follows: Section 2 reviews

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 9 Sep 2021, pp: 1679-1683 www.ijaem.net ISSN: 2395-5252

relevant related literature thus establishing a logical basis for this research, Section 3 discusses how the investigations are carried out and in subsequent the section we discuss our findings. We conclude by giving our recommendations in the final section.

II. AIMS AND SPECIFIC OBJECTIVES

This paper aims at developing and proposing an aggressive strategy towards alerting the internet users, especially the users of the World Wide Web about spoofing attacks in a way that calls them to action.

Our specific objectives are-:

1. Research into existing methods that have been used to alert, sensitize users of the World Wide Web in the process of their using this internet dependency.
2. Outline steps/approaches that have been used over time and identify their shortcomings
3. Propose a suitable strategy based on findings pertaining to behavioral tendencies for alerting and sensitizing users so as to protect them against spoofing during use of these web environments

SCOPE OF THE WORK

The internet covers a broad spectrum. As a result, spoofing can take on many forms in the computer world, all of which involve some type false representation of information (Babu et al., 2010). For the purpose of this research work, we will be focusing on web spoofing.

III. RELATED WORK

Understanding spoofing

Initial work in the field of securing networks has focused on describing the malicious attacks users of constantly faced using the internet. One such attack is spoofing. Spoofing can take on many forms in the computer world, all of which involve some type false representation of information. (Babu et al., 2010) These attacks arise when an attacker creates a misleading context in order to trick the victim into making an inappropriate security-relevant decision. (Felten et al., n.d.)

In the paper "Analyzing Spoofing Attacks in Wireless Networks", Jindal et al(2014) posits that as regards information security, and especially network security, a spoofing attack is a situation in which a person or program disguises successfully as another by presenting false data, to gain an illegitimate advantage. (Jindal et al., 2014) This attack becomes more achievable when an unsuspecting user trusts a system that the spoofer hijacks. Spoofing impersonates another person or computer, in most cases by providing the false information (e-mail, name, URL or IP address). (Babu et al., 2010)

Further research identified the a number of spoofing attacks and described several spoofing attacks, which include but are not limited to Internet protocol (IP) spoofing, Web and/or URL spoofing Email spoofing, DNS spoofing and so forth. (Jindal et al., 2014) A few are described below.

IP spoofing occurs when a system **impersonates** another system and sends packets of data to a third system creating the impression that the packet is coming from the **trusted** system. After creating this impression, it attempts to connect to an address authenticated service or port. If successful, it plants a backdoor access for future reference. (Babu et al., 2010) This type of attack is the case where there is an implementation of **trust** relationships between machines. (Jindal et al., 2014) This trust is leveraged and harm is done

Email spoofing is achieved by capitalizing on the lack of authentication mechanism by SMTP a protocol that oversees the sending of electronic mails. (Jindal et al., 2014) A spoofer alters the sender address along with other parts of an email such as the header to appear as if the email originated from a **trusted** source. An **impersonation** occurs and a misleading context is created thereby endangering an unsuspecting person.

DNS spoofing is successful insertion of resolution information that is not correct and that ultimately leads to the diversion of information from a legitimate target to an address under the attacker's control.(Babu et al., 2010) This diversion reroutes traffic to the intruder/attacker's computer(Halili, 2015), thus exposing sensitive data.

Web spoofing

Overtime research into spoofing has narrowed down into describing how the web users are affected. In discussing website spoofing, Babu et al. (2010) describes spoofing as an attack that allows someone to view and modify all web pages sent to a victim's machine. A website is created, as a hoax, with the intention of misleading those who engage the website that the website has been created by a different person or organization. (McCarthy, 2017) Normally, the spoof website will adopt the design of the target website, and it sometimes has a similar URL. (Spoof Website Will Stay Online, 2004) Usually, the person being impersonated is usually an entity that has gained

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 9 Sep 2021, pp: 1679-1683 www.ijaem.net ISSN: 2395-5252

the trust of a set of persons the attacker is targeting. This attack results in having all of the victim's traffic go through the attacker's machine, causing the attacker to obtain the victim's sensitive information. (Felten et al., n.d.).

As noted by Felten et al. (n.d.), in a typical web spoofing attack, the attacker can create a "shadow copy" of the entire World Wide Web (Felten et al., n.d.). The attacker's machine then becomes the funnel that collects all access to the falsified web copy, allowing the attacker to see all the activities carried out by the victim's including any passwords or account numbers the victim inputs. The attacker can also engineer a **trusted** web server to send false or misleading data to the victim in the name of any Web server, or receive false or misleading data in the victim's name.

Another web spoofing approach employs a 'disguised' URL (San Francisco Electronic Crimes Task Force, 2005). By utilizing domain forwarding, or fixing into the URL one or more control characters, the link can bear the appearance of a genuine while masquerading the actual address of the malicious webpage. Puny code is yet another technique that can be employed to do this. This technique takes advantage of the similarities in letters of different writing systems. A security researcher managed to register the domain 'xn--80ak6aa92e.com' in 2017, and have it show on several browsers as apple.com. Originally, the characters used were not from the Latin script (McCarthy, 2017). However due to the default font the browsers used, the resultant URL was non-Latin letters and numbers that could not be distinguished from those belonging to the Latin script.

As noted by Babu et al. (2010), spoofing has no constructive or legitimate uses of any type. In most cases, the objective is fraudulent gearing towards theft, maliciousness sport or other unspeakable activities. At other times, it could serve the purpose of criticizing or making fun of the person or body whose website the spoofed site purports to represent.

Defense approaches

Research into the subject matter also went further to provide analyses of on various defense strategies particularly on the web users showing what approaches have been adopted and the short comings of some of them. The focus is on those approaches that have alerted the users to some extent.

TrustBar (Herzberg, 2006) is a secure site identification widget which translates the contents of the SSL certificate into user readable feedback by abstraction of information such as the organization that verified the site as authentic. It also possesses a feature that allows a user to select an image on the site they are currently on to have it examined and identified and its authentication displayed at the top of the browser for the users to see. For the reason that it occurs at the top of the screen, it is usually the not the first thing a hasty user will notice. As a result of user falls prey.

Another development is SpoofGuard (Boneh, 2005) is a plug-in solution specifically developed to mitigate phishing attacks in a symptom-based manner. That is, the plug-in looks for "phishing symptoms" such as similar sounding domain names and masked links in the web sites that are visited (Kirda & Kruegel, 2005). On detection of symptoms, alerts are generated. This alert occurs as a single dialog box in the middle of the screen.

A third example is AntiPhish (Kirda & Kruegel, 2005). Users determine information that is sensitive to them they would like to keep from falling into the hands of predators. Once such information faces a significant risk, an alert message in form of a dialog box is displayed telling the user that s/he is a potential victim and that there has occurred a termination of the process.

As much as these alerts especially those in the SpoofGuard and AntiPhish software will go a long way to register that a danger is lurking, many persons have become used to certain dialog boxes that they close a single dialog box instance without reading it. This is often referred to as the click-through syndrome (Herzberg, 2006). Hence more aggressive steps need be taken.

Herzberg (2006) recommended a highly personalized greeting from the server after user has logged into their account that occurs in a highly visible manner perhaps also incorporating audio. This strategy is more aggressive. But it does not take into account that there are sign up pages that require sensitive information that could be harvested by malicious persons and that the visitation of any spoofed web page is the first port of risk to the user. Hence we examine how we can keep the user alert on visiting a webpage, sign up and login.

International Journal of Advances in Engineering and Management (IJAEM)
Volume 3, Issue 9 Sep 2021, pp: 1679-1683 www.ijaem.net ISSN: 2395-5252

IV. METHODOLOGY

The main focus is to determine the most effective method of keeping users of the Internet always alert when surfing the Internet so that they don't fall prey to the activity of spoofers. Despite the fact that builders of Internet compliant applications have made conscious effort to implement the application side of the defense approach, it still continues to stare us in the face that the alertness of users cannot be substituted in all its ramifications. True, inexperienced and technically sophisticated users cannot determine the trustworthiness of a website. However, when an application that does this cannot supply proper, visible and aggressive feedback to the users then there is no point in the first place.

When using an application that provides some form of connection to the Internet, a user needs to exercise caution so as to escape being served malicious content or even having his/her valuable security relevant information from being stolen. It is crucial to the emotional and psychological well being that users of the Internet as well as the propagation of Internet based applications that these user be helped to remain unharmed and keep themselves safe.

To achieve an aggressive strategy for this, a search using different search engines which included Google search was done to determine how web browsers alert users of the validity of a site. The following listing shows a number of them.

1. Notification bar below the menu bar(Herzberg, 2006)
2. Pop-ups in the middle of the screen (Kirda & Kruegel, 2005)
3. Padlock icon at the left side of the address bar(Herzberg, 2006)
4. Sequel to the recommendation by Herzberg (2006), we also employed audio feedback as an alert mechanism, using different sounds.

Test environment

A test environment was put in place for determining the reactions of persons to these various alert mechanisms. The test environment was a simulated website with three divisions and 5 web pages for each division, each having a one of the alert mechanisms obtained from our search embedded into it. All the kinds of feedback were programmed to simulate flagging a malicious webpage.

Test procedure

The test procedure consisted of three stages: scenarios, interview, and analysis. They are described below: -

Three scenarios were used to test these alert mechanisms and the interaction of the participants with the simulation was observed.

Scenario 1: In this scenario, the participant visited a URL. The participant pressed one of the "visit URL" buttons on the simulated webpage to set this scenario in motion. For each page that was to be visited, one alert mechanism was used.

Scenario 2: In this scenario, a participant fills a sign up form requiring sensitive personal information.

Scenario 3: Here a participant fills a sign in form requiring sensitive information.

Following the scenarios, oral interviews were done to ascertain the effect of various methods of alert on the participants. The following questions were asked: -

1. Which alert mechanisms were easiest to dismiss?
2. Which alert mechanisms were not visible enough to be seen?
3. Which alert mechanisms had the strongest impact on you?
4. Which alert mechanism was the easiest to see?
5. On a scale of 1-10, how much impact did the audio alerts have on you?

Finally, the feedback was examined and analyzed. This stage involved studying and discussing the replies of the participants of the tests. The order of visibility and the alertness created of the above listed mechanisms from most visible to least visible was deduced during this stage from the feedback gotten.

V. RESULTS

Our findings show that being alerted by the system as quickly as possible i.e. on visiting a site helps the user focus on how they would navigate the site. Secondly, one step pop-ups were quickly dismissed. On the other hand, we observed that the majority of the participants were more inclined to stop and review after they had been presented with a three step confirmation process occurring in form of pop ups. Further to that, pop-ups that blocked the entire page were remarked as being very evident although a number of the participants felt disturbed by it. Bright red colored notifications were quickly noticed as they took precedence over the other contents on the page. Conclusively, sound alerts had a very high perception rate. All the participants reported becoming more alarmed and hence focused at sharp audio feedback indicating of its

effectiveness.

RECOMMENDATIONS AND CONCLUSION

These recommendations are primarily directed to those who build browsers and its add-ons to incorporate into their designs and implementation for the security of those using their products.

1. Despite the fact that pop-ups blocking the entire page reduce user experience they are quite effective. Hence these should be employed as often as possible to ensure alertness. Alternatively, smaller pop-ups that do not get dismissed after one step will help persons review their decisions before continuing. For the sake of the user, those pop-ups should not be designed in a mechanical way.
2. The padlock icon needs to be conspicuous enough. This can be done by including a visible call out that keeps people on their toes. These pop-ups need to use bright colors to make their feedback have hierarchical priority over other elements on the web page.
3. Sounds should be used. Sharp sounds that can evoke consciousness should be employed to engage the users.

Having said that, it is important to mention that there is a serious need to sensitize the general public using campaigns, school curriculum at the secondary school level, workshops and all publicity mediums to ensure that persons have the necessary minimum technological know-how to keep themselves safe when they surf the web. We may not completely end spoofing but we can significantly prevent it. We hope this paper inspires the implementation of a user-focused approach to significantly reduce number of persons who fall prey to web predators.

REFERENCES

[1]. Spoof website will stay online. (2004, July 29). Bbc News. http://news.bbc.co.uk/2/hi/uk_news/3936497.stm

[2]. Felten, E. W., Balfanz, D., Dean, D., & Wallach, D. S. (n.d.). Web Spoofing: An Internet Con Game (Revised ed.).

[3]. San Francisco Electronic Crimes Task Force. (2005, January). Anti-Phishing Technology.

[4]. McCarthy, K. (2017, April 18). That apple.com link you clicked on? Yeah, it's actually Russian.Theregister.Com.https://www.theregister.com/AMP/2017/04/18/homograph_attack_again/

[5]. Jindal, K.; Dalal, S.; Sharma, K. K. (February 2014). "Analyzing Spoofing Attacks in Wireless Networks". 2014 Fourth International Conference on Advanced Computing Communication Technologies: 398–402. doi:10.1109/ACCT.2014.46. ISBN 978-1-4799-4910-6. S2CID 15611849.

[6]. Babu, P. R., Bhaskari, D. L., & Satyanarayana, C. H. (2010). A Comprehensive Analysis of Spoofing. International Journal of Advanced Computer Science and Applications, 1(6).

[7]. Halili, R. (2015). NETWORK SECURITY AND SPOOFING ATTACKS [E-book].

[8]. Herzberg, A. (2006). Preventing Phishing, Spoofing, Malware and Other Attacks on Web Users [E-book].

[9]. Ross, B., Jackson, C., Miyake, N., Boneh, D., Mitchell, J. (2005) A Browser Plug-In Solution to the Unique Password Problem, http://crypto.stanford.edu/PwdHash/

[10]. Boneh, D. (2005) SpoofGuard Home Page, http://- crypto.stanford.edu/SpoofGuard/