Quest Journals
Journal of Software Engineering and Simulation
Volume 9 ~ Issue 3 (2023) pp: 57-60
ISSN(Online) :2321-3795 ISSN (Print):2321-3809
www.questjournals.org

Research Paper

Authenticated and Dynamic Websites: A Sure Control against Website Spoofing Attacks

[1] Onyeacholem Ifeanyi Joshua*, [2] Omede Edith Ugochi.
[1] Software Developer and Data Scientist, Delta State University, Abraka, Nigeria
[2] Computer Science Department, Delta State University, Abraka, Nigeria.

ABSTRACT: *This paperwork focuses on authenticated and dynamic websites as a sure control against website spoofing attacks. We all love online shopping and it's easier and more convenient to do it on the Internet with a few clicks. But for your online safety, we must be cautious about the sites you visit. There are numerous websites running on the cloud today whose aim is to provide fake information just to gain access to users' data. This paper is not limited to website users in Nigeria only rather, it captured other experiences faced by users globally. Modern web development has many challenges, and of those security is both very important and often under-emphasized. While such techniques as threat analysis are increasingly recognized as essential to any serious development, there are also some basic practices that every developer can and should be doing as a matter of course. So, this paperwork will unveil loopholes in security measures, and highlight various ways we can curtail the challenges faced by companies, organizations, and even users who interact with the website.*
Keywords: — Authentication; Spoofing; Attack; Dynamic.

Received 14 Mar., 2023; Revised 27 Mar., 2023; Accepted 29 Mar., 2023 © The author(s) 2023. Published with open access at www.questjournals.org

I. INTRODUCTION

Over the years, the world has groaned under the yoke fake websites, spoofing attack and users are also falling victims on a daily basis.

Essentially, fraud takes a human approach. Attackers' main focus is to take advantage of victims' weaknesses and carelessness, in the year 2020 Australians lost almost $300,000 as a result of trying to purchase puppy online during the lockdown.

ACCC's (2020) reported more than $634 million lost to fraud, a significant jump from $489.7 million in 2019. With all the technological tools we have, why does fraud continue to be so pervasive? What can be done to mitigate this menace?

The ACCC's (2020), reported that BEC (Business Email Compromise) fraud has increased the number of losses in the year 2019 to $132 million. This usually involves using phishing attacks, and Offenders to intercept payment invoices, or create their own, and funnel victims' funds into their own accounts. Businesses and individuals make their payments as usual but unknowingly pay the offender.

BSC (British Securities Commission) (2020), reported another technique as Investors and dating fraud. Research reports show that the total amount of $126 million, increased from $80 million in 2018. And dating fraud losses totaled $83 million, up from $60.5 million in 2018.

Gillett, Rosalie et al. (2020), states that business email compromise is one of the most used techniques by scammers, BEC fraud affects organizations at large and estimated offenders over $26bn since 2016. Despite the sheer magnitude of these losses, academic research still finds it difficult seeking to better understand this crime type, and prevent it from occurring.

Verizon's (2018), small businesses make (SMB) up 58 percent of the victims of cyber-attacks. In 2016, 14 million SMBs experienced a cyber breach.

*Corresponding Author: Abdalftah Elbori
MODES Department Atilim University Turkey

New York Magazine *(2018),* Over 40 percent of activity on the internet is fake. As the internet becomes more fake, so do its users; stating that more than a 40percent of website running on the internet is fake is not a surprise, but it is interesting to note nonetheless. Some studies have shown that less than 60 of traffic on the internet is human. Bots became so widespread on YouTube in 2013 that developers were afraid that their algorithms would start interpreting bot behaviour as human and human traffic as bots.

This paper is basically designed to investigate and provide ways we can curb these so-called attackers who have made website spoofing a source of earning income.

Yomi Kazeem(2020) said Nigerian Internet fraudsters best known as "yahoo yahoo" who act and pretend to be someone else just to make a claim have now device sophisticated means.

Lance Whitney (2020), in the first quarter of the months in year 2020, generated voucher and payment fraud BEC attacks increased by more than 75%. But there was an increase from April to May, which shot up 200% per week, with a 36% increase in the number of organizations that fall victim to these attacks.

Quartz Africa (2020), In the market competition for developers, Nigerian software programmers have also been identified to participate in a $100 million dollar bet on African development talent by the software giant, Microsoft.

While in Nigeria, policemen who see young men with laptops tend to regard online fraudsters as a way of

extortion and harassment. This act most time have caused fight and protest on the highway and crowdfunding legal aid by the burgeoning tech community.

Deloitte & Touche (2019), one of the oldest indigenous professional services firms in Nigeria states that the main targets for cyber-attackers will be cloud-based systems, user mobile devices, IOTs, and Small & Medium Enterprises (SMEs) as well as organizations in the non-financial sector.

Dell Technologies (2017), observed that the number of spoofing attacks closely to 30,000 and total of 21 million spoofing attacks with the total sum of 6.3 million IP addresses in March 2015 to Feb. 28, 2017. That's what happened to Dyn Inc. two years ago, when a deluge of data triggered from disguised web addresses collapsed 85 leading websites including eBay, Netflix, PayPal, and Sony PlayStation. During the Dyn Inc attack, its servers were pummelled with up to 1.2 terabits — 1.2 trillion digits — of data per second.

Mimecast services (2020) and Okpeki, U.K., Adegoke, A.S and Omede, E.U. (2022). Application of Artificial Intelligence for Facial Accreditation of Officials and Students for Examinations. FUPRE Journal of Scientific and Industrial Research. 6(3). 1-11. spoofing attack is tricky where cyber criminals create a website that closely resembles a trusted brand as well as a domain that is virtually identical to a brand's web domain. Their aim is to get access to user-sensitive information, such as credit card, passwords, of their registered account,

Spoofing techniques

Spoofing attacks can be implemented using various techniques. First, in s situation whereby the attacker and the target are making use of the same subnet.

Ramesh et al (2010), affirmed that attacker can sniff traffic on the network, so as to decrypt pieces of information that were encrypted to launch the attack. While at the transport layer, various techniques can be used to initiate this kind of attack, in the act of carrying out this attack techniques it is worth knowing that the attackers can alter the data stream, spoof addresses, as well as trying to inject sequence figures into packets this is done so as to gain full control in the communication level.

Alternatively, this attack can be carried out by means of obfuscating techniques (blind spoofing), in this case, the attacker and the target are not sharing the same subnet.

Ramesh et al (2010), state that using these techniques, can be very dangerous and it is much more sophisticated and advanced type if fully implemented. For the attacker to succeed here, the guessing method of getting data is used (this means information that the attacker will need to be successful is not available). One of the threatening limitations to this study is that, Web Spoofing works on many browsers such as both Internet Explorer, Firefox and Netscape irrespective of SSL (secured sockets layer), because, SSL protocol authenticate Websites with the use of certificate. The attacker takes notes of the SSL and transmogrify the web pages by creating form submission.

II. METHODS AND SPECIFICATION

This study aimed at the discovering various loopholes which attackers took advantage of in websites interaction and creating a new technique to mitigate these attacks. Take for instance, Jumia, Konga, OLX, do not synchronize users whenever they change location; so, the major aim of this paper is to make sure whenever users change location, they have to pass through authentication methods so as to confirm the real user of that particular account which he/she tends to gain access. The paper will also provide solution to the following techniques such as:

- Fishing attacks
- Web spoofing
- Authentication strategies.

By introducing what is called **"***four-factor authentication***"** into web base applications during online transactions. Four factor system are sometime use in business and government agencies that require extremely high level of security. Due to its higher level of multifactor authentication, has made it so difficult for attacker to fake or steal all the elements involved.

In four-factor authentication method, it requires the following: "knowledge factor" (user name/password) or identification PIN, "possession factor" anything a user must have in their possession to login (OTP token) or a smart phone with an OTP app, "inherent factor" this include biometric user data that are confirmed for login (iris scan, fingerprint scan, and voice recognition) and lastly "user location factor" this is sometime considered a fourth factor for authentication. The ubiquity of smart phone can help to make this easy by enabling the GPS device in order to be able to confirm the login location.

Four-factor Authentication: Is a newer security paradigm than two-factor or three-factor authentication.

Method of Data Analysis

The method used in analyzing the data is to test the probability of attempts made by attacker's trying to inject malicious codes into the website.

To ascertain this, we used **"***Bayes Theorem***"** to determine the conditional probability of attack events with respect to the data gathered. The programming languages used in explaining the various ways of authentication in this study are hyper pre-processor (PHP), JAVASCRIPT, and HTML.

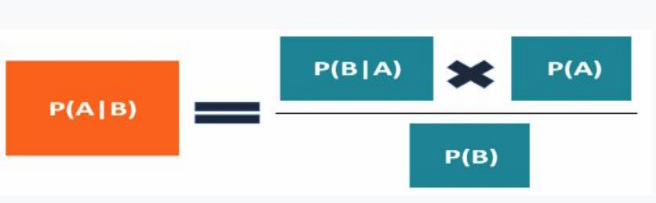

Figure 1: *Bayes Theorem*

III. Discussion

In web spoofing attack, the victim requests a Web page. The following steps occur: **(1)** the victim's browser request the page from the attacker's server; **(2)** the attacker's server request the page from the real server;**(3)** the real server provides the page to the attacker's server; **(4)** the attacker's server rewrites the page;**(5)** then lastly, attacker's server now send(provides) the rewritten version to the victim.

The key to this attack is the strategy known as Man in the middle (MiM) attack in the security literature.

IV. Math Specification: Using the Bayes Theorem:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)}$$

Figure 2: Bayes Theorem

.

P(A) = The probability that attack has taken place before.

P(B) = The probability of attack occurring again.

Where:

P(A/B) ---> The probability that attack has taking place before given that the same attack may likely occurs again.

P(B/A) ---> the probability of event B occurring, given A has occurred.

P(A) ---> the probability of event A

P(B) ---> the probability of event B

The event A and B are independent events (i.e., the probability of the outcome of event A does not depend on the probability of the outcome of event B).

P(A)--> the probability that authentication is increased by 5%.
P(B) --> the probability that there would be no attack.
P(A/B) --> the probability of authentication been increased by 5% given that there will be no attack.
P(B/A) --> the probability that there is no attack given that security authentication has been increased by 5%.
Result Interpretation: Thus, the probability of implementing the four factors authentication in your website will increase security measures by **6.67%.** thereby mitigating attacks with and illegitimate access from web spoofers by **95%.**

V. CONCLUSION

From the result and information gathered, it therefore implies that the more technology is increasing the more attackers find their ways out to gain illegitimate access, but it is expected of software engineers and developers to be alert and make sure all the necessary security measures are put in place to mitigate this attack One distressing attribute of this attack is that it works even when the victim requests a page from via a "secure" connection. If a victim visits a secure website using "secure socket layer" in a false Web, everything will appear to be normal. (The victim browser will be showing that connection is secured. Unfortunately, the secure connection is from the attacker website.

Recommendations

- The fact that a website is showing connection secured does not give that website 100% credit of been save and secured for users.
- If you have to support only web application, go for Cookie or Token based authentication
- On top of above authentication methods, we can also implement One Time Password (OTP), Two Factor Authentication(2FA), ***four-factor authentication,*** Email verification,
- Insist on good password practices for your users to protect the security of their accounts. Passwords should always be stored as encrypted values, preferably using a one-way hashing algorithm such as SHA1 or MD5.

REFERENCES

[1]. British Colombia securities commission (2020): Investment and romance schemes also continue to defraud victims.
[2]. Deloitte & Touche (2019): main targets for cyber-attackers
[3]. Dell Technologies (2017): almost 30,000 spoofing attacks each day.
[4]. FBI's Internet Crime Complaint Centre (May 8, 2020): billion in losses were attributed to business email compromise (BEC) attacks.
[5]. HEIMDAL tm security (2019): TOP ONLINE SCAMS YOU NEED TO AVOID https://heimdalsecurity.com/blog/top-online-scams/#nigerianscam
[6]. HEIMDAL tm security (2019): some dead giveaways that a shopping site is fake
[7]. Lance Whitney (2020): BEC attacks, invoice payment fraud scam,www.techrepublic.com
[8]. Mimecast services (2020): Website spoofing scam.
[9]. Verizon's (2018): victims of cyber-attacks:
[10]. Yomi Kazeem (Lagos April 10, 2020, Quartz Africa): Nigerian software programmers have also been identified to participate in the software giant, Microsoft competition.
[11]. Ramesh Babu et al (2010), sniff traffic on the network, so as to decrypt pieces of information that were encrypted to launch the attack
[12]. Vivek Madurai (2020): Various Authentication Methods, (https://medium.com@vivekmadurai/difrent-ways-to-authentica-a-web-application.