Study on Protection Against Password Phishing

Hiba Zuhair Zeydan, Ali Selamat and Mazleena Salleh

Faculty of Computing, Universiti Teknologi Malaysia, Johor, Malaysia

Abstract: Phishing attack is a new type of network attack that becomes a major nuisance on the internet. The rapidly progressing phishing attacks make the present secure socket layer not able to provide and protect users from fraudulent websites. The attacks have been targeted at non-cryptographic security protocols like Transport layer security and secure socket layer protocols. These protocols are not sufficient to tackle phishing attacks and need additional mechanisms. In this paper, we discuss phishing attacks and related weaknesses of Secure socket layer (SSL) protocol. Further, we discuss and evaluate some proposed solutions against phishing and web spoofing attacks.

Key words: Password • Phishing • Trust • Security • Attack

INTRODUCTION

Recently, the information and communication technologies play a significant role in various fields such as health, transportation, industries, etc [1, 2]. However, these services need to protect their credentials during exchanging their data. The Transport layer security (TLS) and Secure socket layer (SSL) protocols are the most popular technologies for protecting e-commerce applications. These technologies establish a cryptographic secure channel and authenticate the web server between the user and the web server. The user is using a public key certificate or validation method for authentication. This information is passed over the established SSL/TLS channel. The use of SSL is not secure and not working properly against phishing attacks [3]. Basically, in phishing attacks, the phishing spoofs a genuine website via fake websites. The fake website is the same as the original one and has the same images and logos. Recently, banks and websites have been faced with phishing attacks. The first attack was found in the US where 57 million internet users received a phishing email link and 2 million of them lost their confidential and sensitive information [4]. The most phishing crimes take place with the help of spam emails. In email messages, the attackers attract the user to click and use fake websites through email links and provide them with personal information such as account number, credit or debit card number, passwords and user names, etc. The attackers use this information to carry out identity theft. The boosting trend in phishing shows that current authentication approaches are inadequate to defend internet users from fake websites. In another research, the author identified that some phishing attacks have influenced up to 5% of their recipients to offer susceptible information to spoofed websites.

Nowadays, the SSL and TLS are rely on public key infrastructure (PKI) to authenticate each other. In PKI, the certification Authority (CA) is responsible as a third party to sign digital certificates. The certificate is binding the public key of an entity to its identity and public key is authenticated if the signature verification of the digital certificate with certificate authority public key is valid. The implementation of secure socket layer (SSL) needs that only server is authenticated. Attackers take benefits from these certificates issued to phishing websites and falsely issued to unauthorized individuals from these falsely issued certificates. The attackers easily attack to imitate the legitimate website. It is very difficult if users are with less knowledge of digital certificates and not easy to detect the attacks. Even though if users are experienced, they also need to examine detection attacks thoroughly.

Corresponding Author: Hiba Zuhair Zeydan, Faculty of Computing, Universiti Teknologi Malaysia, Johor, Malaysia.
In this paper, we illustrate about phishing attacks and discuss current certificate based SSL protocol and its weaknesses and limitation to provoke attackers for phishing attacks. Most current phishing attacks and solutions are also discussed with analysis.

**Phishing Attacks:** Phishing attacks have become an important threat for internet users. Through fake emails and websites these attacks deceive user personal and financial information. Users can also tricked through installing and downloading hostile software and these small programs searches the users computer and monitor online activities to steal private information. According to the anti-phishing workgroup, 2870 phishing sites are appeared in 2005 [6]. During last decade most of organizations have extended online services to their clients. In 2011 most of Americans and European regularly shopped online and pay their bills online, check their bank details online. Such a usage and online financial services increases security risks [7]. Phishing is a criminal activity and new identity theft crime. The phishing web sites are visually similar to real web sites and a new client can easily deceived by this type of scam. In Figure 1 shows the phishing site designed for eBay users and on the other hand Firefox 2 phishing warning mechanism prevent through message from fake web site to the user.

**Phishing Attacks Limitations and Weaknesses:** The implementation of secure socket layer (SSL) rely on public key infrastructure (PKI) in order to authenticate the user. Most of users have no knowledge about Certification Authority (CA) trust and some experts and experienced users specifying the CAs to sign the SSL certificates [8]. These weaknesses help the attackers to launch phishing attacks. In one Earthlink this problem users faced this problem, where the attackers register a real certificate for their bogus website and use that fraud SSL certificate with lock icon. Because in this situation the certificate has been registered and match with URL of bogus page imitating the Earthlink website. If users examine the certificate then they detect the attack. There is another option in which some adversaries can configure their web server and SSL certificates will not activated as an alert in browser. Through this process SSL encoding change into plain text [9]. Most of the SSL servers are disabled; most of web browsers support this. Due to plain text no central CA is consulted and the message about certificate should accepted because plain text does not use certificate and SSL lock icon not showing encrypted channel. This type of SSL connection not with the intended server. Some other cases are about CA unintentionally certificates issued to malicious adversary. The Class 3 code signing digital certificates issued by VerisignInc for individual who fraudulently claimed to Microsoft [10]. Although Verisign cancel the certificates because not browsers are not support CRL-checking mechanism to locate and use CRL. Users are install patch from Microsoft website to prevent from these attacks.

**Types of Phishing Attacks:** The different types of threats are available and related to internet and they are in the shape of host program, logic bombs, Torjan horses, virus, zombie and worms. The phishing spam mails are new type of attack and threat for users. Phishing attacks are fall into many categories such as spoofed email, exploit based and real world spoofed web site-based phishing attacks.

The visual spoofing is a type of phishing attack where the browser secures connection indicators (BSCIs) tampers to make a foolish about real status of connection [11]. Adelsbach et al. (2005) [11] described that many browser secures connection indicators like padlock icon indicates SSL/TLS connection, where information is available in certificatedialogue about current SSL and server certificate and the location bar shows the URL and menu bar shows status of SSL connection. The visual spoofing utilizes for browser graphic interface and replace real BSCIs with fraud and fake ones.

In another study author presented some possible visual spoofing attacks [8]. The most of users are confused and not recognize the hyperlink image and actual one. This will come with another technique of attackers where they display an image of the legitimatehyperlink and hiding the real address of website. Another problem with distinguish between security indicators from images. Most of users confuse from SSL lock icon because these icons present in different locations on the browser to indicate secure connection. The Figure 2 shows the visual email example.

Another type of phishing attack is SSL protocol using in fraudulent certificate, where SSL protocol is between client and server before secure transaction takes place. For example if user wants to use any bank website for transaction SSL protocol establish secret key for secure communication shows in Figure 3.

Figure 3 shows four phases of SSL handshake process, where the process is about client and phisher web server. In first phase client clicks on URL and directing to the phisher website instead of original one.
Fig. 1: (a) A phishing site to attack on eBay users (b) Warning mechanism in Firefox 2

Fig. 2: Phishing email example that tries to lure user

Fig. 3: SSL Handshake Process

SSL protocol begin for establishing the connection between user and web server and establish security like protocol version, session ID, compression and cipher suite and initial random numbers. Client send hello message to the server and server send acknowledgment message back to the client. In phase 2 the phisher web server will send the certificate with SSL certificate signed by CA to the client. This message contains the public key of phisher web server and CA signature of certificate. The SSL handshake will continue and user believe that web site is secure but actually user establishes the connection with phisher web server. The server will send the server exchange key and Diffie-Hellman (DH) used. In last the server sends server Hello done message to show the end of the server hello and associated messages. In phase 3 the client check the message from server and certificate and client send the certificate verify messageto the server. In next step the user sends client key exchange message. In last phase the user indicates change cipher specification message and send the finished message. The server responds with its own change cipher spec and finished message.
Table 1: Phishing solutions

<table>
<thead>
<tr>
<th>Solutions</th>
<th>Function</th>
<th>Limitations</th>
</tr>
</thead>
<tbody>
<tr>
<td>Plug-in</td>
<td>Using as a web browser extension and firstly discovered solution against phishing attacks.</td>
<td>This solution has some limitations like it only protect inexperienced user from spoofed e-mails.</td>
</tr>
<tr>
<td>Toolbars</td>
<td>Generate the passive warning against phishing attack.</td>
<td>Not active and easily ignored from users.</td>
</tr>
<tr>
<td>Spam Filters</td>
<td>These filters categorize the mails before harmful mail</td>
<td>The solution is rule and machine mechanism based and both are not efficient.</td>
</tr>
<tr>
<td>Prevention against Malware software</td>
<td>Some emails have secret code when user click on these mails these malicious software get automatically downloaded</td>
<td>Use some new and latest antivirus to protect against such virus.</td>
</tr>
</tbody>
</table>

In this example the user disclosed all credentials to phisher web server instead of original server.

Related Work: The many approaches have been proposed for phishing attack. Some of them are based on third party certification models and compared to present use of PKI by the SSL protocol. In PKI the CA will sign a digital certificate and binding the public key of an entity to its identity. The drawbacks of these certificate-based SSL are falsely issuance and lack of understanding of digital certificate. The one third party solution proposed where web of trust approach used to distribute trust. Some other approaches also used third party approach such as Verisign [12] and TrustE [13]. However, these techniques are not so effective because these techniques easily copied.

Some other schemes are based on authentications and used a combination factors like password, biometric and personal identification numbers, etc. The most popular examples belongs to this approach are America Online passcode program. In this the devices are distributed with RSA secure ID to its members [14]. However through this method the attackers collect the primary and secondary passwords [8]. The shared secret schemes to help users to identify known servers have some disadvantages like the server must display its shared secret for authentication. If the secret key is captured the image can replayed until the user realizes and changes it. There are some other approaches on the application layer for phishing attacks. These works are in the form of web browser plug-in to prevent from attacks. The most popular examples in this area is Spoof Guard [15], Pwd Hash [16] and Dynamic security skins [8]. Most of these applications are application specific and not applied to other applications.

In another approach author examined that attacks are on different levels and if the attack is in initial stage like 0 or 1, so easier detect compare to 2 and 3 stages [17]. Chick How Tan et al. (2007) [18] proposed an ID-based protocol to overcome the limitations and weaknesses of SSL and offer efficient protection for users against phishing attacks. Author claimed that his protocol is able to prevent phishing attacks but still have some weaknesses.

Analysis of Solutions: In this section we analyze some proposed phishing prevention methods. Some of the popular technical preventions are discuss below in detail.

- **Anti-Phishing Plug-in**: In this type of solution the web browser has capability to warn to user if something is wrong.
- **Toolbars**: In this technical type the toolbars are not capable to categorize contextual data which is done by email filters. The toolbars simply generates truth rating belongs to web site which is cancel from user side without paying notice to the warning.
- **Spam Filter**: This solution work on the context of the e-mail and also on URL for observing.
- **Machine Learning Protocol**: This solution work on prediction based known properties learned from the training set.
- **Phi Stank**: In this solution all the information is related to the links and have record of previous phishing attackers. But the main disadvantage of this is if information is older then it delete and if same attackers attack after this so the link is new to the phi stank [19].

CONCLUSION

The phishing attacks growths have been rapidly boosted in recent years. The main reason behind this growth is due to limitations and weaknesses in the present implementation of SSL protocol. In this paper, we highlighted these limitations and weaknesses and also discuss phishing attacks with examples. In last we summarize some technical phishing solutions with limitations. This work will help full for those researchers who find and work to develop an effective phishing approach to protect user credentials from attackers.
REFERENCES


