A Mobile Anti-Phishing System Using Linkguard Algorithm

Elizabeth A. Amusan, Oluyinka T. Adedeji, Oluwaseun Alade, Funmilola A. Ajala and Kayode Ibidapo
Department of Cyber Security Science, Department of Information Systems, Department of Computer Science
Ladoke Akintola University of Technology, Ogbomoso, Nigeria

Received: 17-JUN-2021; Reviewed: 17-AUG-2021; Accepted: 25-AUG-2021

Abstract- Phishing is a type of cyber-attack where the attacker deploys a combination of social engineering and technological skills to trick users into revealing private information like bank account details, usernames and passwords by creating an imitation of an existing web page. This research developed an Android-based anti-phishing system leveraging on the ubiquity of mobile devices and their increasing applications for business and personal purposes. The system was developed by implementing an end-host based algorithm called the Linkguard algorithm which is effective in detecting and preventing both known and unknown phishing attacks. A total of over 500 links which was a blend of both phishing and non-phishing links were collected from Phishtank and Alexa to validate the proposed system which achieved an accuracy of 96%. It is recommended that concerted efforts should be geared towards continuously sensitizing users to improve their phishing awareness as this cybercrime keeps evolving and users play a very crucial role in mitigating it.

Keywords- android, cybercrime, Linkguard algorithm, mobile, phishing

1 INTRODUCTION

Phishing is a cybercrime launched by cybercriminals disguising as genuine individuals in an illegal attempt to get sensitive information from users by using spoofed emails and fake websites. The cyber attackers use a combination of social engineering and technological skills to lure users into revealing private information like bank account details, usernames, passwords and such like (APWG, 2018; Saraninia and Padma, 2014). Unsuspectingly, users or victims give out these pieces of information themselves by clicking on links that appear familiar or similar to that of a trusted contact. Consequently, victims of phishing attacks which could be individuals or corporate organizations are at risk of financial loss as well as loss of confidentiality of valuable information (Joseph and Singh, 2018).

The pervasiveness of mobile devices for business or personal use on the internet and the exponential rise in the number of malware-based campaigns have expanded mobile cyber-threats (Bottazzi et al, 2015). These mobile devices are basically driven by Android and iOS as the two principal operating systems with 99.19% market share distributed as 72.72% for Android and 26.47% for iOS (StatCounter, 2021). While researchers have proposed various approaches to combat this cybercrime, most anti-phishing techniques exist as solutions in desktop environments (Saraninia and Padma, 2014; Joseph and Singh, 2018; Akinyede, Adelakun and Olatunde, 2018; Mohith et al, 2020; Dhanawde, Dhanje and Waghmare, 2020). From literature, very few studies resulting in tools supporting mobility have been reported despite the enormity of activities carried out with these mobile devices (Amro, 2018; Shahriar, Klintic and Clincy, 2015).

Furthermore, several machine learning-based approaches designed and implemented to mitigate phishing are difficult to use by the average non-technical user (Mohith et al, 2020; Sahingo and et al, 2019). This is worsened still with the fact that such algorithms are computationally complex and resource-intensive, thereby limiting their support of mobility.

This paper therefore seeks to develop an Android-based phishing detection system through the implementation of Linkguard algorithm which is an efficient and lightweight end-host based algorithm capable of detecting both known and unknown phishing links.

The rest of this paper is structured as follows: section 2 presents the literature review followed by methodology in section 3. Implementation as well as evaluation results are presented in section 4 while conclusion and future work are covered in section 5.

2 LITERATURE REVIEW

Studies have proven that there is almost no difference between the genuine links and the phishing hyperlinks, however, under listed here are some characteristics that the phishing hyperlinks share in common (Naresh, Sagar and Reddy, 2013; Jain and Gupta, 2017; Gupta, Singh and Jayant, 2019; Joseph and Singh, 2018):

i. The visual (displayed) link and the actual link are not the same.
ii. The impostors or cybercriminals regularly use dotted decimal IP address in place of the DNS.
iii. Special tricks are used to maliciously encode the hyperlinks.
iv. The impostors regularly use fake DNS names that appears like that of the target site though not exactly the same.

2.1 CLASSIFICATION OF PHISHING ATTACKS

The classification of phishing attacks is done on the basis of the strategies deployed by impostors in order to access victims’ information. It typically incorporates social

*Corresponding Authors

http://dx.doi.org/10.46792/fuoyejet.v6i3.666

© 2021 The Author(s). Published by Faculty of Engineering, Federal University Oye-Ekiti. This is an open access article under the CC BY NC license. (https://creativecommons.org/licenses/by-nc/4.0/)

http://journal.engineering.fuoye.edu.ng/
engineering and technical subterfuge (Gupta, Singh and Jayant, 2019).

**Social Engineering-Based Attacks:** Cyber-attacks in this category leverage mental and emotional manipulation of people thus luring them into completing some actions that will consequently disclose their private information. Social engineering based phishing attacks are further classified as: spoofed email phishing and fake websites. Furthermore, spoofed email phishing could be spear phishing, if the attack is aimed at a particular person or group of persons or whaling if aimed at a high-ranking person or employee (Almomani, Gupta and Wan, 2013). Fake websites that have similar visual appearance like a genuine one are equally used to phish a user.

**Technical Subterfuge:** Phishing attacks here are perpetrated in such a way that the cybercriminal sends malicious codes alongside emails or websites. It could be any of: cross-site carpeting (XSS), malware phishing, DNS poisoning and session hijacking (Almomani et al, 2013).

### 2.2 Phishing Detection Approaches

Different anti-phishing approaches have been proposed, these approaches are content-based techniques, black lists, and white lists, visual similarity and URL based. In content-based techniques, the content of the website is used to determine whether it is a phishing site or not (Mao et al, 2017). While black lists and white lists compare the requested URL against either a black list of phishing URLs, or a white list of non-phishing ones (Memon and Khan, 2013). Visual similarity approach determines similarity features like text pieces, images and the overall visual appearance between two web pages and calculates this similarity by comparing the features thereby computing a similarity score (Dhanawde, Dhanije and Waghmare, 2020). URL detection are often carried out using common detection algorithms like Random forest, Support Vector Machine, Decision trees, etc. where length of URL, number of special characters, IP address are the commonly used features.

Shahriar, Klintic and Clincy (2015) provided a mobile anti-phishing taxonomy that highlights all possible phishing attacks and corresponding mitigation techniques. The authors stressed the dearth of solutions developed specifically for mobile devices apart from the black and white lists.

In Bottazzi et al. (2015), authors proposed a framework for the detection of phishing in mobile devices using machine learning algorithms as classifiers whose performances were evaluated in terms of precision, accuracy, true positive rate and false positive rate. However, in an attempt not to overload the computational capability of the mobile devices, the classifiers were built outside the mobile device which makes it challenging for constant update of the model.

Arising from the review of related works, most of the mobile anti-phishing solutions do not perform their detection directly on the mobile devices, rather, they employ a server module to carry out the detection remotely. This is observed as a trade-off in terms of performance, scalability and constant update hence this work therefore proposed a phishing detection system that is mobile and simple to use through the implementation of Linkguard algorithm which is an efficient and lightweight end-host based algorithm capable of detecting both known and unknown phishing attacks.

### 3 Methodology

#### 3.1 Linkguard Algorithm

This algorithm is efficient in detecting and preventing both known and unknown phishing links. It operates by analysing the difference between the actual links and the visual (presented or displayed) link, thus calculating the similarities of URI (Uniform Resource Identifier) (Sarannia and Padma, 2014). Figure 1 shows the composition of the Linkguard algorithm while Figure 2 presents the actual steps:

1. Communication: this component collects data associated with user input, as well as send the information to the analyzer.
2. Database: this part is responsible for the storage of the whitelist, blacklist, as well as the URL supplied by the user.
3. Analyzer: it is a very important component as it is responsible for the analysis of data supplied by the communication and database, it also sends the corresponding output to the alert component and logger.
4. Alert: it alerts the user as soon as it receives a warning message from the analyzer.
5. Logger: it serves to archive related information for reference purpose.

![Fig. 1: Architecture of the Linkguard Algorithm (adapted from Sarannia and Padma, 2014)](https://example.com/fig1.png)

#### 3.2 Model Design of The Proposed System

The purpose of this research is to design an open-source android-based system that is capable of detecting phishing URLs using the operations of the Linkguard algorithm by classifying links as either phishing or non-phishing links. Figure 3 is a flowchart of the proposed anti-phishing system which works by prompting users to input a suspected link in a text button. The system has properties of a web browser embedded in it which categorizes the links based on the result generated from the Google safe browsing archive. The result generated is in form of a visual display on the screen which confirms phishing or otherwise. For the legitimate URLs, the link will load successfully on the mobile app, otherwise, the user will be alerted accordingly.
3.3 ALGORITHM IMPLEMENTATION FOR URL DETECTION

The classification of phishing and non-phishing links is done when the system:
1. Checks for auto login requests from the host.
2. Checks for http response code 401 and 402 which is the most common phishing logic.
3. Check if the websites produce an SSL error. An SSL (secure socket layer) certificate error is when a browser cannot verify the SSL certificate installed on a website which means that website is insecure. It is a standard security technology for encrypting information between a visitor’s browser and your website. It helps to keep sensitive information like passwords and payment information safe. Safe sites can be identified by HTTPS in their URLs and the padlock icon in the address bar.
4. Check if the host of the link is flagged by Google Safe Browsing which is the most important factor. Google Safe Browsing is one of the numerous public API services offered by Google which provides a list of URLS for web resources. These web resources have malwares or phishing contents.

The features used for the extraction of links are: Suspicious char, http, Host flagged by Google safe browsing, Prefix Suffix, SSL error, Auto login request and http response code 401 and 402.

3.4 IMPLEMENTATION ENVIRONMENT

The implementation environment for the development of the mobile anti-phishing system include: an Android operating system (Android 5.0 lollipop and above), any android phone of 512MB RAM upwards and with 8GB internal storage.

4 RESULTS AND DISCUSSION

A prototype of the android-based phishing detection system in form of an Android-based application, Kayphish was developed. To verify the effectiveness of KayPhish anti-phishing system for the link detection section, 500 phishing links were collected from PhishTank and Alexa archive and tested based on search results returned by Google safe browsing. Presented in this section are some snapshots of the developed system shown in Figures 4-7.
Figure 4 represents the home page of the link scanner where a user is allowed to supply the URL of the link to be scanned. When a link has been supplied, it is then highlighted for scanning as shown in Figure 5. The outcome of the scanning would result in classifying the link as either phishing or non-phishing as displayed in Figures 6 and 7 respectively.

4.1 SYSTEM EVALUATION

Because the Linkguard algorithm is a rule-based heuristic algorithm, its performance was evaluated in terms of accuracy and precision which are derivatives of True Positives, False Positives, False Negatives and True Negatives. True Positive (TP) indicates that a phishing URL or link is correctly classified as phishing. False Positive (FP) indicates that a non-phishing URL is incorrectly classified as phishing. False Negative (FN) indicates that a URL is indeed a phishing link but incorrectly classified as legitimate. True Negative (TN) indicates that a non-phishing URL is classified correctly as non-phishing.

Precision indicates the ratio between True Positives and the total number of links tested.

\[
\text{Precision} = \frac{\text{TP}}{\text{TP} + \text{FP}} \quad (1)
\]

Accuracy is the measure of overall correct classifications given by:

\[
\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{TN} + \text{FP} + \text{FN}} \times 100 \quad (2)
\]

Of the 500 links tested, we have:

- TP = 250
- TN = 230
- FN = 11
- FP = 9

<table>
<thead>
<tr>
<th>Metrics</th>
<th>Results</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precision</td>
<td>0.97</td>
</tr>
<tr>
<td>Accuracy</td>
<td>96%</td>
</tr>
</tbody>
</table>

Table 1. System Evaluation Results

5 CONCLUSION AND FUTURE WORK

This research has implemented the Linkguard algorithm in the development of an Android-based anti-phishing system due to the expanded cyber-threats towards mobile communications and the increasing spread of Android phones for business and personal use. The use of this system provides security against phishing attacks in real time with simple and friendly user interface coupled with
warnings when a link is not trusted. The accuracy of the developed system could be further improved on. Also, it is recommended that users be continuously educated to increase their phishing awareness as cyber-attack keeps evolving and users play a crucial role in mitigating it.

REFERENCES


