International Journal of Latest Trends in Engineering and Technology
Special Issue SACAIM 2016, pp. 149-156
e-ISSN:2278-621X

SECURITY MEASURES FOR PREVENTING PHISHING ATTACKS ON MOBILE COMPUTING PLATFORMS

Alston de Souza[1], Suman Nagaraj[2] and CG Thomas[3]

Abstract- Recent years have witnessed the increasing threat of phishing attacks on mobile computing platforms. In fact, mobile phishing is particularly dangerous due to the hardware limitations of mobile devices and the habits of mobile users. In this paper, we did a comprehensive study on the security vulnerabilities caused by mobile phishing attacks, including web page phishing attacks, application phishing attacks, and account registry phishing attacks. Existing schemes designed for web phishing attacks on personal computers cannot effectively address the various phishing attacks on mobile devices. Hence, we propose MobiFish, which is a novel automated lightweight ant-phishing scheme for mobile platforms. MobiFish verifies the validity of web pages, applications, and persistent accounts by comparing the actual identity to the claimed identity.

Keywords –Mobile Computing, Phishing Attacks, Security Protection, Mobifish, Appfish, Webfish, Accountfish

I. INTRODUCTION

Phishing attacks attempts to steal private information, such as user's private information and credit card information, often for a malicious reason. Many anti-phishing schemes have been proposed by security researchers but phishing attacks have not been diminished. On the one hand, there is a rapid expiry and revive on phishing sites. According to the Anti-Phishing Working Group (APWG), 4.5 days is the average time for a phishing site to stay online. Phishing attackers keep finding better techniques so that their new attacks are able to find a way around existing anti-phishing tools. In social media such as Facebook, Twitter, and Google+ phishing is a continual threat. Hackers could create a duplicate of a website and ask the user for their personal information, which is then emailed to them. Hackers then take advantage of these sites which are used by people at their workplace, homes, or in public in order to steal their private or security information that can affect the user or company (if in a workplace environment). Phishing attacks takes advantage of the user's trust, since the user may not be able to predict whether the site that is visited or program being used, is not real. In such cases, the hacker has the opportunity to gain the personal information of the targeted user. Mobile phishing is one of the phishing attacks which is an emerging threat targeting mobile users of financial institutions, online shoppers, and social networking companies. Mobile based phishing targets users into entering their credentials in fake websites or fake mobile applications. They also trick mobile

[1] *AIMIT (St. Aloysius College), Mangalore, Karnataka India*
[2] *AIMIT (St. Aloysius College), Mangalore, Karnataka India*
[3] *AIMIT (St. Aloysius College), Mangalore, Karnataka India*

users by conventional phishing web pages (designed for personal computer (PC) browsers) when browsing with their phones.

Nowaday, all Internet services are supported by powerful browsers, people are habitual to online banking, online shopping, online socializing, etc. Users are intimate with being requested to provide private information so they subsequently provide personal information and user credentials to the websites. Current phishing detection schemes can be divided into two categories: heuristics-based schemes and blacklist-based schemes. Blacklist-based, here only the only the phishing sites that are on the blacklist are detected, and they cannot detect zero-day phishing attacks such as those that have only appeared for a certain period of time. It is possible that user credentials have already been stolen by new phishing sites or have expired before being added to the blacklist. Heuristics-based schemes depend on features that have been selected or obtained from URL and HTML source code, and to determine the validity, other techniques, such as machine learning, are used to. However, we find that the features extracted from HTML source code could be inaccurate, and phishing sites can easily bypass those heuristics.

Phishing attackers are involved in the development of fake apps or repackage legitimate apps so that they could upload these phishing applications to unofficial app markets. When the attack is successful, the phishing server will be sent victim's credential. It is difficult to detect Phishing apps compared to phishing web pages. For web pages, the action attribute in the form tag helps us to decide the point of leaving form data from HTML source code (action attribute in the form tag). However, for mobile apps, there is no facility available which can check if user credentials are sent to the legitimate authentication server or the attacker's server. Hence, we can conclude that phishing attacks on mobile phones are more complex than those on PCs. It is very important to propose effective mobile phishing defense schemes for both web applications and web pages.

II.RELATED WORK

A block diagram of the phishing methods which are carried out which include Web Fish, App Fish, and Account Fish [1]. In the below diagram we will be using the WebFish method where the URL will be taken as the input, URL domain name verification followed by the download HTML page, check for the form presence, extract text from the form and match it against sensitive text and warnings will be sent to the user in case the page contains any phishing links. [2] In AppFish when the app is being installed App name verification, app login screen captures and verifies the sensitive data and during launching checks outgoing SMS for sensitive text and checks outgoing URL for that domain will be done and warn the user, AccountFish main process is to check if the account name is null then it is a malicious app and if the account name is the same as the app name it is set as a new app and added to the main menu and connection will be established.

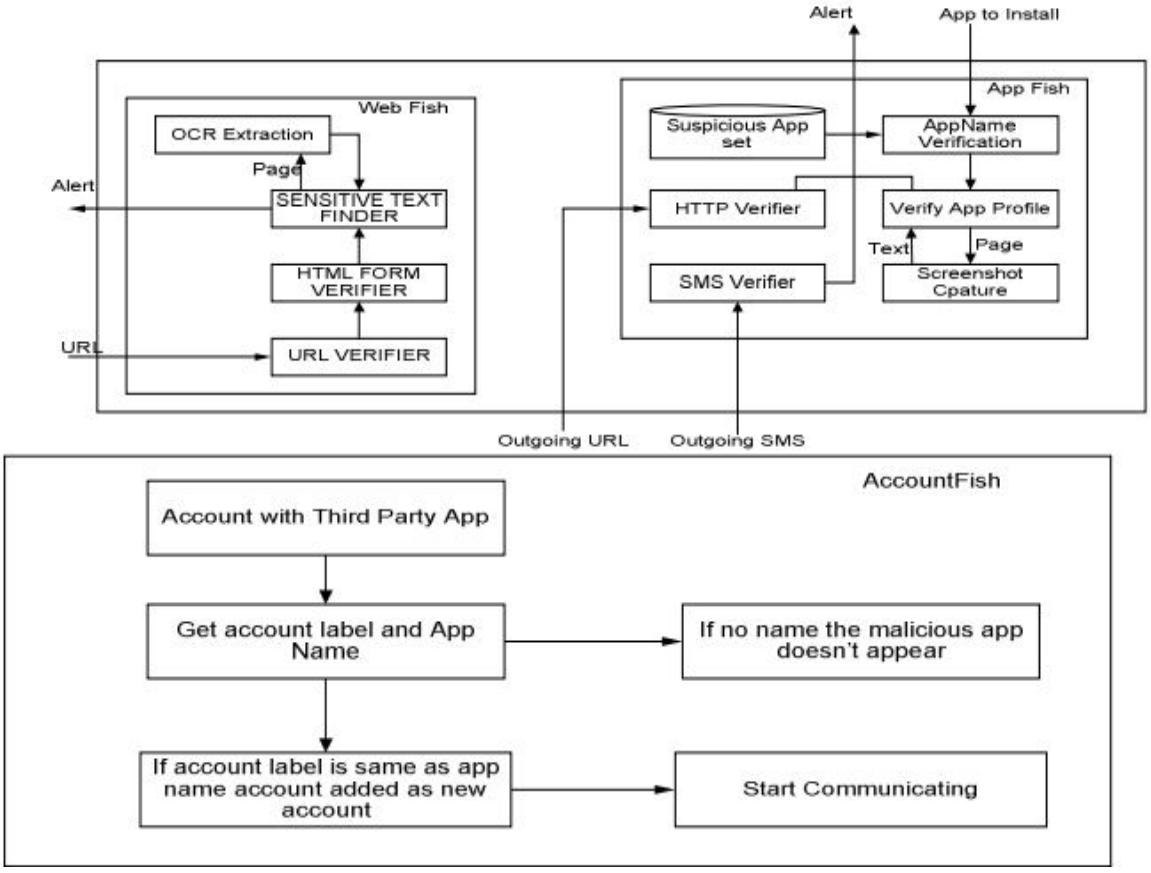

Figure 1. Block diagram of the proposed system

[3] In this paper, we propose MobiFish technique for defending against mobile web pages, apps, and persistent accounts. WebFish, AppFish, and AccountFish includes different methods for recognizing malicious app, these includes different methods like Optical Character Recognition (OCR) to extract text from screenshot for checking URLs, second level domain name (SLD), suspicious App set (SAS) this contains untrusted apps and account mapping white list (AMWL) that contains all inconsistent legitimate apps.

A. *The Workflows for WebFish–*

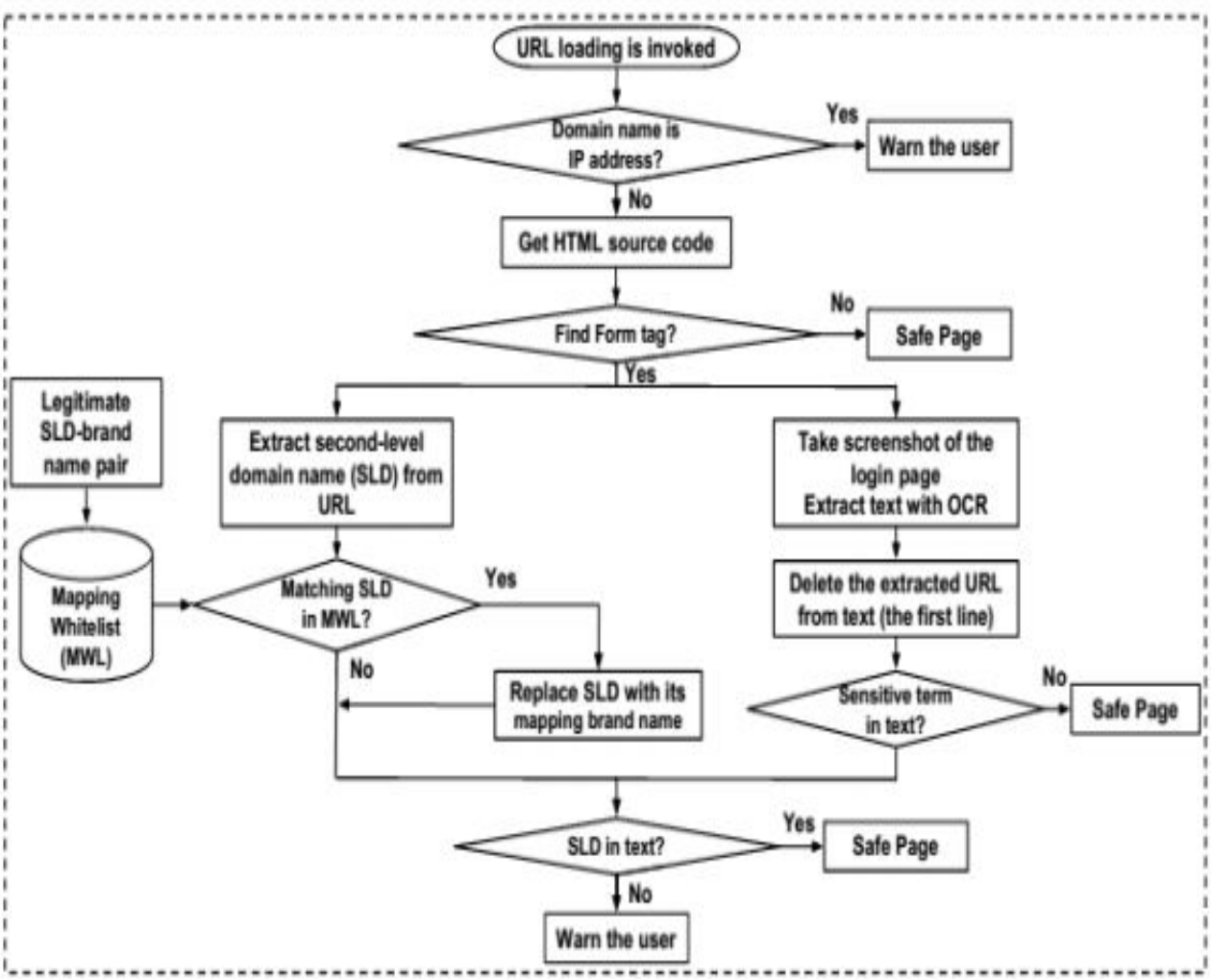

Figure 2. workflow diagram for WebFish

This scheme starts with URL loading[4]. It first scans URL to check domain name is an IP address, if domain name contains IP address it warns to the user, If not it obtains the HTML source code of the loading page, and checks for the form tag. If form tag is found, it starts the extraction and verification of the identity, if the form is not found then the page is safe.

On one hand Web Fish extracts SLD brand names as some of the branded enterprises use the brand name as their second level domain name for their websites.[5] The SLD from the URL that contains the actual identity of the site, and then the SLD extracted is indexed in Mapping White-List (MWL) in which it checks the name with legitimate SLD brand pair. If any match found with SLD-Brand name, then the original SLD is replaced if the SLD is not matched or not found then the site is considered as malicious and warns the user.

On the other hand, the screenshot of the login page is taken and text from the screenshot is extracted with the Optical Character Recognition (OCR) technique, OCR is a mechanical or electronic conversion of an image to machine-encoded text[6]. Before checking sensitive terms, it removes the first file from the text which may contain the phishing link and then it sends the sensitive terms to map extracted SLD with MWL. If it is not found, then the site is marked as a phishing site and it warns the user and if SLD is found then the legitimate brand name will be

replacing with existing. The design is based on the assumption that if the domain name of the phishing site appears in the fake login page of a legitimate entity, the user will check for the validity of the page.

B. *The Workflows for AppFish–*

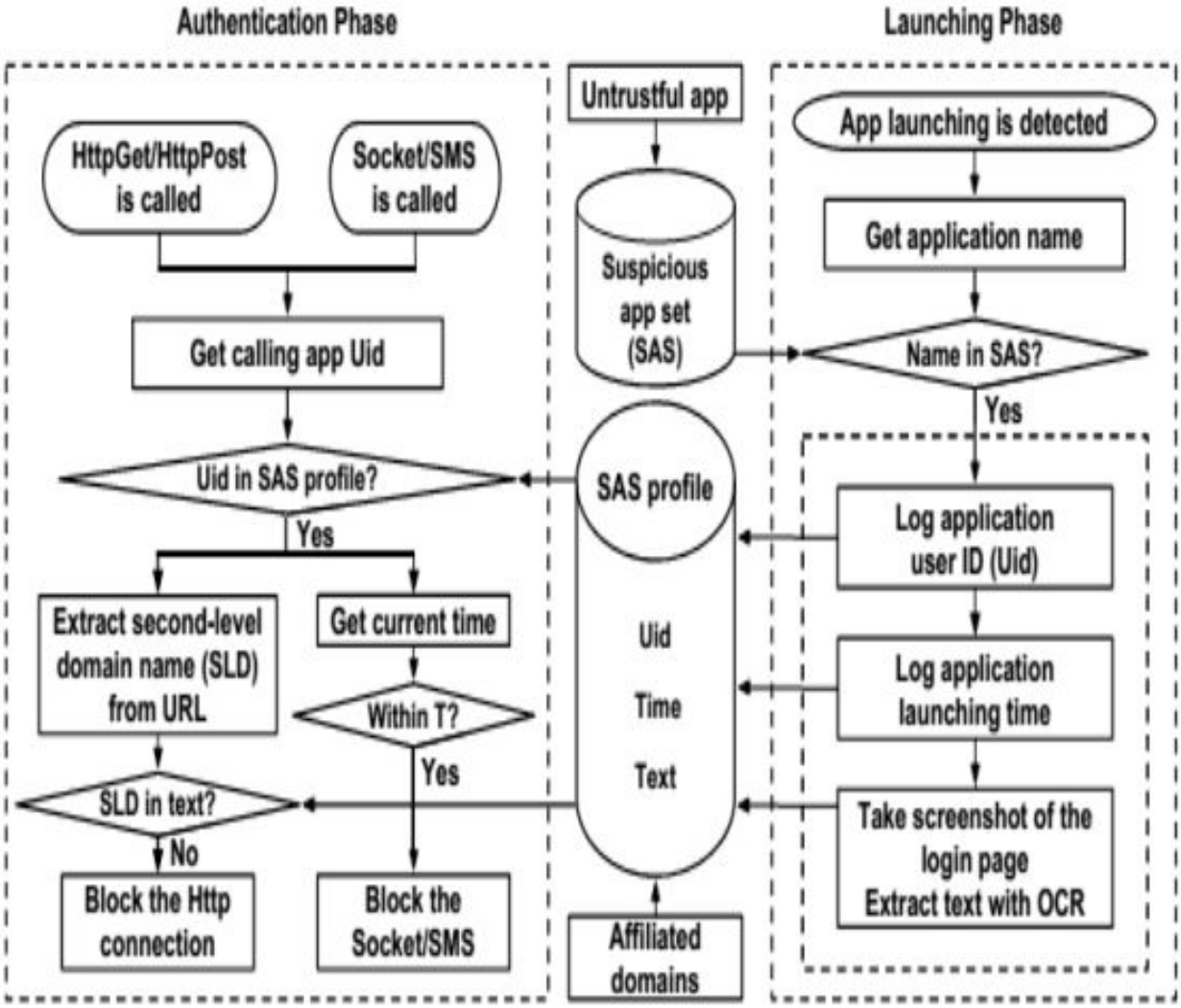

Figure 3. workflow diagram for AppFish

AppFishis designed to check the malicious apps present in the mobile, it maintains a database called Suspicious App Set (SAS) it contains user ID, launching time and screenshot[7]. The app that is downloaded may be malicious and some of the malicious application can be identified while downloading app from the unauthorized site, this scheme works in two phases: launching phase and authentication phase, in launching phase, AppFish takes the name of each launching application and check for that name in SAS which contains all the untrusted app details. If it is

found it takes a screenshot of the login page and extracts the text using OCR technique then the text along with application Uid, launching time of that app and profile details of the app.
After user enter the details and click submit the authentication phase starts legitimate application sends the user details to remote server and loads the data after identification are verified, the application loads data belonging to that account, if the application is malicious it will be unable to load the user data as it does not contain any user information, that is designed only to get user detail and ask re-entering information by showing user has entered wrong login id or password [8]. The information may be requested through SMS or through web notifications that need user login, so AppFish before sending information it checks it is in SAS. If found HTTP connections are filtered till then other connections will be blocked for certain period of time T, by that time the user notices the malicious app and remove the app, and meanwhile, AppFish ensures SLD name or domain name in SAS profile and notices it is malicious app. If the app does not contain any such malicious activities, then it will be installed and used.

C. *The Workflows for AccountFish–*

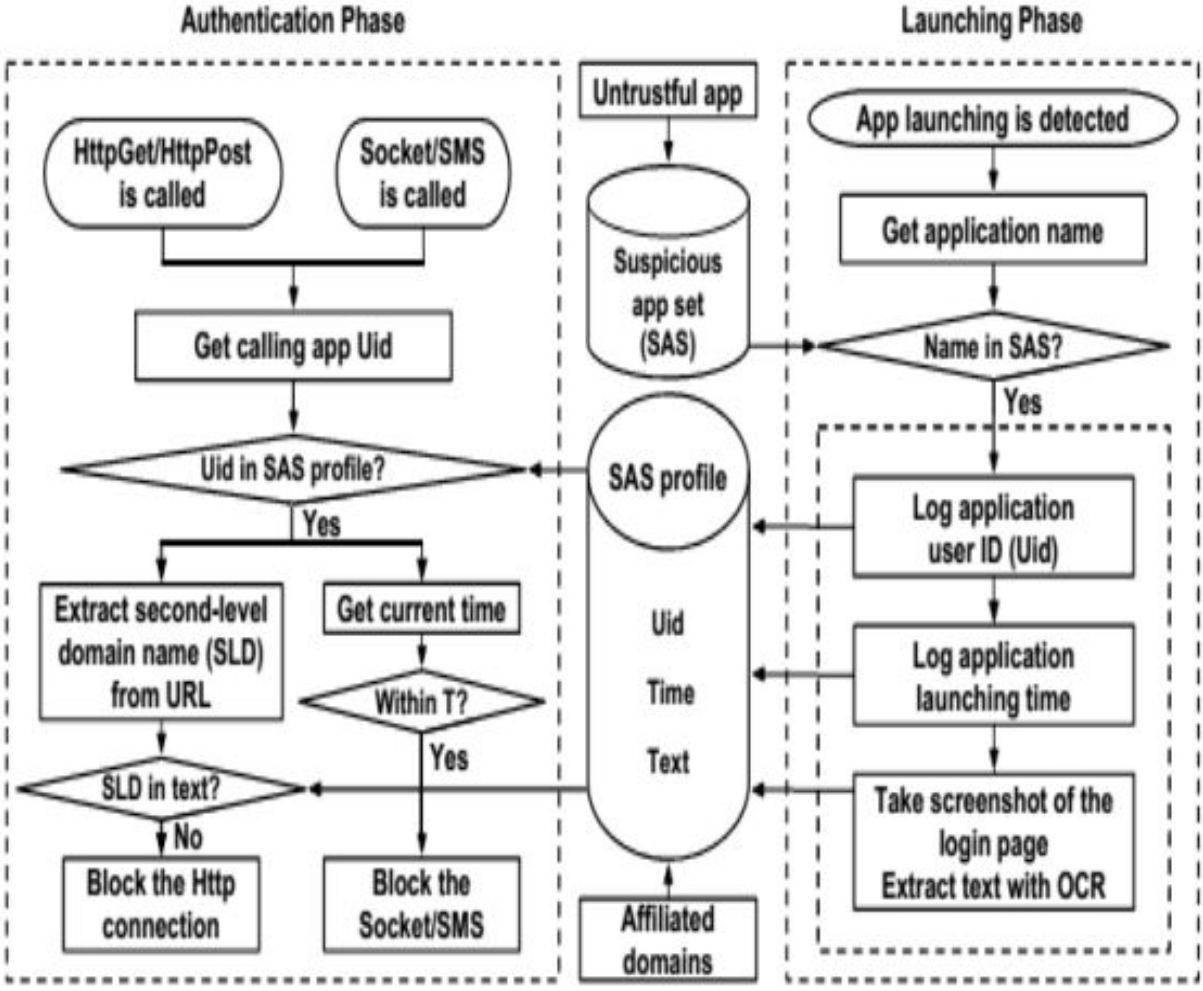

Figure 4. workflow diagram for AccountFish

AccountFish application is used to check accounts that are registered and are used to attack registered accounts which exist or occur over a prolonged period, the account scan can be of three types based on the type of the infected application[9]. The first type of attack is basically where the user downloads an app from a third party source which looks similar to the application available on the play store, which on download the application acts like a normal app but behaves like another application. The second type of attack is basically the application is not visible to the users and on the app list on installation but can see the details only on the storage or settings of the mobile. The detection mechanism provides account label and application full name of the first type and second type and compares the application name in the main menu and account label in the account list. The third type of attack is where the infected application shows as a target application

It should be able to check the account registration of during runtime that can be accomplished by modifying Android source code[10]. If account label and account name are different then the app may be malicious but some of the legitimate app labels are not same as resultant app names that problem is solved using account mapping white list (AMWL), which contains all suspicious app details where we check all legitimate AL with AN pairs. The mechanism used to detect C is similar to type C similar to AppFish the malicious activities cannot be found until the transformation of the information is done. Here we have bound to Authenticator function that finds user action whileadding account and monitor the process the app name will be used to check or filter the outgoing connections. Only the URLs with SLD will be allowed to communicate and suspicious activities sites are blocked for a certain amount of time and user will be warned if it is malicious.

III.CONCLUSION

As technology has advanced hackers have learnt various way to get users private information like username and password which is used in various websites from banking to social in order to avoid this many such issues these mechanisms have been introduced but that is not enough hence users can make use of MobiFish which protects the users from all the possible ways the hacker would make a user give his private information which could be used by the hackers to cause damage. MobiFish is lightweight as it works without using external search engines or machine learning techniques.

REFERENCES

[1] Markus Jakobsson and Steven Myers "Phishing and Countermeasures"-Understanding the Increasing Problem of Electronic Identity Theft.

[2] Dr. M. Nazreen Banu and S. Munawara Banu "A Comprehensive Study of Phishing Attacks" ISSN:0975-9646

[3] S.S. Kulkarni, Mayank Tomar, Aastha Mittal, Sneha Arondekar, Aniket Nayakawadi "Survey on Phishing Attacks" ,ISSN: 2277 128X, February 2015.

[4] Soumya.M.S, Prof. Phani Ram Prasad, "Safe Guarding Mobile Phones against Phishing Attacks Using MobiFish" ,ISSN(Online): 2320-9801, May 2016.

[5] C. Marforio, R. J. Masti, C. Soriente, K. Kostiainen, and S. Capkun,“Personalized security indicators to detect application phishing attacks inmobile platforms,” CoRR, vol. abs/1502.06824, 2015.

[6] A. Bergholz, J. De Beer, S. Glahn, M.-F. Moens, G. Paaß, and S. Strobel, “New filtering approaches for phishing email,” Journal of ComputerSecurity, vol. 18, no. 1, pp. 7–35, Jan. 2010.

[7] A. P. Felt and D. Wagner, “Phishing on mobile devices,” In Proceedings of W2SP’11: WEB 2.0 Security and Privacy, pp.1-10, 2011.

[8] Y. Zhang, J. I. Hong, and L. F. Cranor, “Cantina: a content-based approach to detecting phishing web sites,” in Proceedings of the 16th international conference on World Wide Web (WWW), pp. 639-648, 2007.

[9] A. Bianchi, J. Corbetta, L. Invernizzi, Y. Fratantonio, C. Kruegel, and G. Vigna, “What the app is that? deception and countermeasures in theandroid user interface,” in Proceedings of the IEEE Symposium on Security and Privacy (SP),pp.931-948, May 2015.

[10] Gunter Ollmann, "The Phishing Guide" - Understanding & Preventing Phishing Attacks.