Anti Phishing for Mid-Range Mobile Phones

Imran Khan Memon and Muhammad Khalid Khan

Abstract—E-commerce has been the centre of attraction for millions of users, because people now want to perform important activities like buying and selling etc. over internet through personal computers or mobile phones. This has compelled service providers to devise reliable and secure ways for Ecommerce through which users can perform transactions without any risk.

E-commerce trade has experienced the largest number of cyber crimes that includes various types of security attacks. Phishing attack is the one most common among these all, as the mobile banking is getting popular, hence protecting the mobile users from phishing attacks is very important; particularly mid-range mobile users, because these users are easy target of attackers as mid-range mobile phones do not support feature like anti-virus or anti-phishing tool.

A mobile based anti phishing mechanism is proposed as shown in experiments, particularly for mid-range mobile phones that would protect users and their critical financial information from phishing attacks by generating three types of warnings such as vibration, flashing and text alert based warning, hence user would be restricted to visit any fake Webpage.

Index Terms—Cyber crime, mobile banking security, phishing.

I. INTRODUCTION

Most phishing attacks associated with e-mail messages that spoof banks accounts, misuse of credit cards etc. These emails appear to come from a trustworthy financial institution or partner. The e-mail redirects users to an official looking website where they are asked to type their personal information, when users gives their personal information, such as user name and passwords, then that information will be submitted on attacker's email rather than genuine website, and some message would be appear there just like "Currently database or services are down please try again in few hours", these message assured to user that due to some problem user can't perform their activities, hence user leave that website for few hours, then phisher take advantage of that time frame and used these information illegally to misuse of victim's financial resources.

Desktop users can protect them selves from phishing attacks through the tools available in the web browsers but the mobile Users especially mid-range mobile users can not do that because there is no such tools for them. So they became an easy target. Smart phones or similar type mobile

phones which supports "SIS" format installer packages can install the anti phishing tools however Mid-range mobile phones supports only "JAD" and "JAR" formatted installer packages, which are not capable to install such applications like anti-virus or any other security applications. on other end browser based phishing detection mechanisms are limited on iPhone only, also required updating of phishing database directly on mobile phone rather than server side, which waste GPRS bandwidth and time to updating database every time. Some anti-phishing mechanism generates low-level or ignorable warnings whenever phishing websites has detected, hence some times user ignore these warning unintentionally. In this paper We have presents AntiPhishing Apps, a mobile based anti-phishing application which works on all Java supported mobile phones; and updating phishing database automatically on server side rather than user end, it is also efficient to warn user by three way warning system, such as dialog-box, flashing, and vibration alert. Hence user can't ignore these warnings unintentionally.

This paper is structured as follows: The section 2 presents a brief survey of related works. Section 3 describes the architecture of the proposed approaches. Section 4 presents results on different emulators which shows that how "AntiPhishing apps" generates warning on different mobile phones. Section 5 presents future work and Section 6 concludes the paper.

II. RELATED WORK

This research investigates issues related misuse of credit cards, bank accounts, security threats, particularly loosing of an important credentials by Phishing attack. Account numbers and passwords stealing become critical issue, as trading over internet increasing day by day. Hence user must be careful while using e-commerce based services their personal computers or mobile phones.

A. Phishing Blacklist Database

Blacklist generator mechanism is efficient against phishing attacks, because it updates blacklist phishing database automatically. Blacklists websites are used to fight with spam in a very specific way. When spam is reported to one of the relevant spam fighting organizations the IP address the spam originated from is added to a banned or blacklisted IP address list. Proposed blacklist generator works efficient against blacklist phishing websites, however it's difficult to determine of page related to same websites. An efficient information-sharing based anti-phishing system is proposed, which capable to authenticate black list and white list data, this model has client side proxy as browser's plug-in, that would verify authenticity of websites by checking white list, black list and heuristics, without given warnings to user, this

Manuscript received August 10, 2012; revised October 7, 2012.

Imran Khan Memon is with the Department of Data Communication, National Telecommunication Corporation Karachi, Pakistan (e-mail: dr.imranmemon@gmail.com).

Muhammad Khalid Khan is with the Department of Computer Science, Karachi Institute of Economics & Technology, (PAF KIET), Karachi, Pakistan (e-mail: khalid.khan@pafkiet.edu.pk).

system working automatically [1]. An information-sharing based anti-phishing system which is effective to authenticate black list and white list, system has client side proxy as browser's plug-in, and that would verify authenticity of websites by checking white list, black list and heuristics, without given warnings to user, this system working automatically, 1st of all whenever user try to enter URL into browser, the algorithm check user input URL into browser, algorithm verify White/black list, if website found in blacklist database algorithm suddenly block that website. If website found in white list database algorithm will check for any suspicious activity, if system found Spoof value greater than threshold value; then system generated report and send to user also blocked that site, if spoof value less than threshold value, then system warn user and provides alternate sites. In-case no blacklist no suspicious activity found, then system check only domain IP pool if found normal then user would allow continue browsing, if found any suspicious activity then system use IP in the pool [2].

B. E-Banking Based Anti-Phishing

A fuzzy Data Mining (DM) technique is effective tool to identifying phishing websites basis on quality factors rather than exact values [3]. Multifactor mutual authentication process is much effective to detects and prevents phishing, pharming, and man in the middle attacks, existing phishing detection and identification technique for e-banking environment have lack of security which encourage to man in the middle attack that would be very difficult to mitigate due to some uncertainty factors are involved in detection process of phishing websites [4].

C. Ticket and Image Matching Anti-Phishing

Web Bugs and Honey token technique is much efficient to detect phishing from actual IP source of Phisher machines. Duplicate Image Finder techniques can be used for detection of phishing through similar logo and images on fake websites [5]. An effective approach to phishing webpage detection is proposed, which uses Earth Mover's Distance (EMD) technique that would used to measure webpage visual similarity. First convert the involved webpages into low resolution images and then use color and coordinate features to represent the image signatures, and use EMD to calculate the signature distances of the images of the webpage [6].

Image-based anti-phishing scheme is proposed that uses the Contrast Context Histogram is efficient to detect fake WebPages with high accuracy and low error rates. Existing techniques of content analysis or HTML code analysis do not provide high accuracy to detect fake webpages, because phishers are countering these detection techniques by designing fake webpages with non-analyzable elements, hence user may be cheated easily [7].

D. Frameworks Based Anti-Phishing Technique

Phishpin, anti-phishing mechanism that integrates partial credentials sharing and client filtering techniques to prevent from phishers easily masquerading as legitimate online entities [8]. Keywords detection based technique assist for detection of phishers. This activity also known as keyword research. A domain keyword extraction and time-invariant keyword extraction methods which reduce false detection

rate from 14.0% to 7.6%, in order to providing high accuracy to detection of phishing [9]. Link-Guard, technique which is based on the derived characteristics, is efficient to detect known as well as unknown phishing attacks. Unknown attacks are quickly becoming the next great information security challenge for today's organizations. As the window of time between the disclosure of a new vulnerability and the emergence of unique threats that operate against it continues to diminish, so does the effectiveness of many conventional countermeasures, including patch management [10].

Phishing Alarm system is efficient technique to alert user from phishing fraud. Phishing Alarm system warns users without increasing user workload. Alarm system consists of four parts, first part Resolver which decrypts information sent by the Management Centre and send correlative content to Verifier and Analyzer, second part Analyzer which check URL and test whether there is procedure recording keyboard entry or intercepting frame, triggering Annunciator when abnormal, check whether importing is needed, seek submitting address, third part is verifier which verify description provided by resolver, and report of website from analyzer, after verification verifier it pass information to annunciator. Forth part is Annunciator, It is spring dialog box to remind user when triggered. When website checked from this process it will give an alert to user about website whether it is harmful or not [11]. Bogus Biter client-side anti-phishing tool that would protect users from phishing attack. This tool is proficient to not just warn users for fake website but also prevents users automatically from phishing attacks. Bogus biter is useful to prevent user from fake website by injecting a relatively large number of bogus credentials into phishing sites, for confusing to attacker. Bogus Biter is designed either a browser's build-in component or an extension to web browser such as Firefox 2 or internet explorer7 [12].

E. Communication Based Anti-Phishing Techniques

A novel based method for anti-phishing for smart phone mobiles, is efficient to detect phishing WebPages over these mobile phones, because it used some plug-in for executing fake websites, hence attackers can't make fake login for such devices. The Smart mobile devices provide more powerful computing capabilities to manage personal information [13]. An Anti-Phishing authentication (APA) technique is efficient to detect and prevent real-time phishing attacks. APA is based on SPEKE which is a cryptographic method for password authentication key agreement. SPEKE uses passwords to resist against man in the middle attacks. It performs a 2-way authentication and resists on-line and off-line dictionary attacks. SPEKE is used in APA with some modifications [14].

III. APPROACHES AND METHODOLOGIES

This research focuses to protect mobile users from phishing attacks, particularly Mid-Range mobile phone's which supports technologies such as Wireless Application Protocol (WAP), Global Packets Radio Service (GPRS), Enhanced Data Rates for GSM Evolution (EDGE) technologies for access internet over these mobile phones through built-in web browser or commercial web browsers

such as Opera Mini, Bolt etc. These browsers support few protocols and languages such as Http, Wap, Xml etc, but doesn't support any rich type security applications such as Anti-Virus, or Anti-Phishing tools, that would protect or warn their users to open any fake websites. Hence we proposed a unique mechanism that would protect java based mobile users from phishing attacks.

A. Proposed Security Mechanism

A solution (as shown in Fig) for given problem statement consists of three components that not only warn users to visit any fake webpage but also restrict user unintentionally access over fake websites.

The proposed mechanism has been divided into three parts.

- Anti-Phishing Generator
- Blacklist Phishing Sites Database
- Web-Browser

Fig. 1. Architecture of proposed mechanism.

1) Anti-phishing generator

Anti-Phishing Generator consists of address Bar for getting input from user in form of URL (http://), when user enter URL into application, then it will compare given URL into blacklist phishing database, and get response from DB in form of True or False.

If response comes True from blacklist phishing DB, then application generate Warning Message along with vibration alert for few seconds, to warn user that this website is infected with Phishing attack and gives option to go back to re-enter another URL, or close to application.

If response comes False from blacklist phishing DB, then application redirect user's request to default or Built-in Web Browser of that Phone, to execute that website on browser.

2) Blacklist phishing database

Blacklist phishing database is gathering from "Phishtank" which is a community based Phishing verification system, and responsible to detect and update phishing websites into their database, our application verify user's given URL into phishtank database and getting True and False response, if that website found into phishing DB means website is blacklist, then response comes True otherwise False.

3) Setup of phishing database

Phishtank database is available for public in four formats Xml, Csv, Php, Json, we have chosen Csv formatted for our application. First of all we have created MySql connection at our private hosting www.getinfo.pk.com, then download phishing database from www.phishtank.com and updated on private host, currently database updating manually once in a day on private host, later may create cron job that would update database automatically on hourly basis.

4) Online verification of phishing websites

There is alternate way to verify website that it is phished or not, we have to check website from any desktop web browser by visiting at www.getinfo.pk.com/myproj/query.php?url= we may type URL after "=" sign, then response will comes in True or False, if response comes in True that means website is phished, if response comes False it means website is clean.

5) Default mobile web-browser

Default Mobile Web-Browser, is responsible to execute website after getting True or False response from Anti-Phishing generator, web-browser execute any webpage only when response comes in false condition.

Fig. 2. Flow chart about how application works.

IV. IMPLEMENTATION

The Proposed application developed in Net Beans IDE and successfully tested over different build-in emulators of Net Beans and J2ME based Mobile Phones. The results shows that our proposed solution is effective against detection of Phishing WebPages by generating dialog box, flashing and vibration alert, that would not be ignorable for user to bypass it unintentionally.

An Anti-phishing application consists of two classes:

- Anti Phishing class:

It is a main class, this class consists of URL field, GO and Exit buttons, News Ticker, Vibration Alert, Flashing, and Warning dialog boxes.

Fig. 3. Anti phish class.

- My http Data class:

It is a supplementary class which holds Http response and event handling of Http Service.

Fig. 4. My http data class.

A. Demonstration on Emulators

Net beans IDE have several different kinds of emulators that would help us to demonstrate our application on different kind's mobile devices, without actually having to acquire the actual hardware. Our result detects phishing WebPages over different phones templates, this application also successfully tested over Nokia Series 40 and Series 60 based mobile phones.

Fig. 5. Simulation 1- result for phishing detection on touch phones

Touch Phone emulator provides same functionality like touch phones, our application is successfully tested over touch phone emulator. First we have entered fake websites taking from our phishing database, we shows that JavaFx touch phone based emulator successfully detects phishing webpage, and given alert whenever phish webpage found.

Fig. 6. Simulation 2- result on high-end phones or smart phone.

Smart phone emulator provides same functionality of Smart phone such as blackberry, or symbian phones, our results shows that application is capable to detect phishing WebPages on these phones.

Fig. 7. Simulation 3- result on mid-range phones.

Mid-Range or dumb phone emulator, our result shows that application working also on Mid-Range mobile phones. We have also demonstrated application is real Mid-range and Symbian phones.

V. FUTURE WORK AND OPEN ISSUES

Currently this application working on all Java supported mobile phones only; Future work is based on making compatible this application with Non-Java based mobile phones.

In future this application should be embed into any third-party or build-in mobile Web browsers, through any add-ons or any other technique, and that browser should be compatible with all kinds of mobile phones.

VI. CONCLUSION

In this research, we presents an anti-phishing application for Java supported mobile phones, our proposed application is tested over Net beans built-in emulators, and some Java based mobile phones, we analyzed that our application is capable to detects and prevents mobile users from phishing attack, particularly Mid-range mobile users, by generating three way alerts, by Dialog box, by Flashing, and by Vibration alert.

Existing mobile based anti-phishing mechanism designed for smart phones only, also have low accuracy, because these solutions required time to time updating of phishing database on mobile phones rather then on web server, our proposed application working effectively on all kinds of Java based mobile phones, with accuracy also doesn't required updating phishing database on user end.

REFERENCES

- [1] A. Phishing and B. Generator, *Computer Engineering Department Iran University Science and Technology*, 2008.
- [2] Y. Cheng, Z. Yuan, L. Ma, and R. H. Deng, "An information-sharing based anti-phishing system," *First International Symposium on Data, Privacy and E-Commerce*, 2007
- [3] M. Aburrous, M. A. Hossain, K. Dahal, F. Thabatah, and Modelling, "Intelligent phishing detection system for e-banking using fuzzy data mining," *International Conference on Cyber Worlds*, 2009.
- [4] A. S. Martino and X. Perramon, "Defending e-banking services: Antiphishing approach," *Proceedings of the 2008 Second International Conference on Emerging Security Information, Systems and Technologies*, 2008
- [5] D. Birk, S. Gajek, F. Grobert, and A. Sadeghi, "Phighting the phisher: Using web bugs and honey tokens to investigate the source of phishing attacks," *Second International Conference on Internet Monitoring and Protection*, 2007

- [6] A. Y. Fu and L. Wenyin, "Detecting phishing web pages with visual similarity assessment based on earth mover's distance (EMD)," *IEEE Transactions on Dependable and Secure Computing*, vol. 3, 2006
- [7] K. Chen, J. Y. Chen, C. Huang, and C. Chen, "Fighting phishing with discriminative keypoint features of webpages".
- [8] H. Tout and W. Hafner, "Phishpin: An identity-based anti-phishing approach," *International Conference on Computational Science and Engineering*, 2009
- [9] S. Nakayama, H. Yoshiura, and I. Echizen, "Preventing false positives in content-based phishing detection," *Fifth International Conference on Intelligent Information Hiding and Multimedia Signal Processing*, 2009
- [10] J. Chen and C. Guo, "Online Detection and prevention of phishing attacks," *National Natural Science Foundation of China (NSFC)*.
- [11] M. Qi and C. Yang, "Research and design of phishing alarm system at client terminal," in *Proceeding for IEEE Asia Pacific Conference on Service Computing*, 2006
- [12] C. Yue and H. Wang, "Anti-phishing in offense and defense".
- [13] W. Han, Y. Wang, Y. Cao, J. Zhou, and L. Wang, "Anti-phishing by smart mobile device," *IFIP International Conference on Network and Parallel Computing – Workshops*, 2007
- [14] M. Sharifi, A. Saberi, M. Vahidi, and M. Zorufi, "A zero knowledge password proof mutual authentication technique against real-time phishing attacks," *ICISS 2007*
- [15] Series 40 Platform: Designing XHTML Mobile Profile content. [Online]. Available: <http://www.forum.nokia.com>.
- [16] PhishTank Database. [Online]. Available: <http://www.phishtank.com>

Imran Khan Memon was born in Nawabshah, Pakistan on 15-03-1984, I have done MS (Computer Science) Specialization in Networks and Telecom from Paf Kiet Karachi, Pakistan, in 2009 Currently He is working as Assistant Manager (Networks) in National Telecommunication Corporation, Karachi, Pakistan Mr. Memon is member of PSQCA and WMO and Many other organizations related to my area.

Muhammad Khalid Khan was born in Karachi, Pakistan, He have done MS (Computer Science) from SZABIST Karachi, Pakistan. Currently He is working as Director of Science and Engineering Dept at Paf Kiet, Karachi, Pakistan. Mr. Khalid is cooperate training of Viorous Banks Such as State Bank, ABL, HBL.