International Journal of Research in Advent Technology (IJRAT) Special Issue
E-ISSN: 2321-9637
Available online at www.ijrat.org
National Conference on "Role of Information Technology in Social Innovations"
26th & 27th February 2019

PhishX: An Android Mobile App for Phishing Attack Detection through Delusory Login Simulation

Mrs. Parvati Bhadre[1], Akshay kumar[2], Akshay Agrawal[3], Mayank Agarwal[4], Rakhi Awari[5]
D. Y. Patil College of Engineering
Akurdi, Pune[1,2,3,4,5,], SPPU,Pune[1,2,3,4]
Email: paru.nadgeri@gmail.com[1], akshaykumar.19996@gmail.com[2]

Abstract-Attackers use clever social engineering techniques to convince their victims into clicking a malware or deceptive login-based webpages. Most solutions for this particular problem focus more on helping desktop computer users than mobile device users. Mobile device users are more vulnerable than their desktop counterparts because they are online most of the time and they have device limitations such as smaller screen size and low computational power. This paper presents PhishX, an effective mobile application prototype that takes advantage of a particular weakness of phishing sites: they accept any kind of input information for authentication. PhishX enables a mobile device user to create fake login account, with fake login credentials, that mimics user login procedure every time the user opens a login webpage and generates an alert to her. PhishX determines whether the current login page shifts to another webpage after an authentication attempt. It does so by monitoring has hcode changes of the URL when the page is loading, listens to HttpURL Connection status code, and then makes a decision on whether the website is fraudulent or not. They measured the effectiveness of PhishX by conducting a user experiment on android platforms and tested its detection accuracy, memory and CPU performance. The results show that PhishX uses a very small amount of computational power and it is effective in assisting users to identify phishing attacks with an accuracy of 96.

Index Terms-Phishing; Android; Information Security

1. INTRODUCTION

Phishing is a web-based attack that fraudulently aims to obtain user's sensitive information such as ID and password. The stolen information is used to perform illegitimate activities on the targeted websites. An attacker is usually motivated by financial gain. Phishing attacks have become simple to launch with greater magnitude of impact. In some cases, an attacker does not create a fresh login page, instead; she just downloads the original login page from a targeted website and changes the back-end connection mechanism. A clone of an original login page makes it difficult for a user to easily realize the phishing fraud by relying on visual cues only. It is even more difficult for mobile device users due to their limitations such as smaller screen size and limited webpage rendition contrary to their desktop counterparts. Although, currently, there are many security tools for addressing phishing attack issues, little has been done to consider mobile device users. Moreover, attacks targeting user-application interaction remain a sophisticated problem. Successful attacks are presented with high credibility webpages. Their presences are so impressive such that it is harder for a victim to pay attention to security indicators installed on web browsers.

Most research classify phishing detection techniques into three main categories: content-based approaches that depend on web features, non-content-based approaches that do not use web contents to detect phishing and visual similarity approaches that detect phishing using their visual similarity with legitimate sites. Practitioners deploy these techniques frequently to web phishing attacks. However the content-based approach takes too long, an average of 76 seconds, to examine web features hence makes it unsuitable for a real-time detection. The same applies to visual similarity approach, which is also too slow for an online detection. The non-content-based approach is dependent on the Universal Resource Locator (URL) lexical and host features that may not detect an attack on a well-presented phishing website. Additionally, Purkait conducted an extensive survey that classifies phishing countermeasures into eight groups that are:

- Phishing at the e-mail level
  1. security and password management toolbars;
  2. restriction list;
  3. visually differentiate the phishing sites;
  4. two-factor and multi-channel authentication; takedown, transaction anomaly detection, log files;
  5. anti-phishing training; and
  6. legal solutions.

2. LITERATURE SURVEY

This section describes previous works that show how a user can avoid entering login credentials manually and instead use an external device or password manager plugins on web browsers. For example, a user of a smart device such as smartphone can authenticate herself to another device such as a laptop or another mobile device through a close range Bluetooth communication. Han et al. introduced a Bluetooth-enabled smart device as a platform to store the login information of the users such as ID and password. A smart device pre-stores information features of a login user interface. Then before the user enters the authentication information in another device, a plugin of his web browser communicates with the smart device through Bluetooth to verify the login credentials. After passing the login credential verification, the smart device automatically fills the login information to the login page on behalf of the user.

Similarly, Bridge et al. introduced a method for automatically submitting login credentials, seamlessly, for a user of a web service. The login information corresponding to a login form of a web service is stored, whereas the login information that is comprised of a login endpoint of the web service authenticates the user for a session of that web service. A login token, generated by the web service, and its expiration date are tracked. The login credentials are then automatically submitted, without user intervention, to the web service based on the login endpoint and the expiration date of the login token. The challenges with these solutions are the requirement of an extra Bluetooth-enabled device and browser plugins.

Another important approach to address phishing attacks is by testing the trustworthiness of the login webpage by injecting random login inputs into the webpage form fields.

However, most of these works are browser-based plugins, particularly, Mozilla Firefox browser. Yue et al. proposed Firefox browser-based solution to protect against phishing attacks with bogus bites. A Firefox browser extension transparently inputs a relatively large number of bogus credentials into a suspected phishing website, rather than at- tempts to prevent vulnerable users from biting the bait. These bogus bites conceal victims real credentials among bogus credentials, and enable legitimate websites to identify stolen credentials in a timely manner. However, the installation must be done at both client and server side. Users need to install BogusBiter and the legitimate server needs to deploy the defensive line enabled by BogusBiter. Moreover, the other concern regarding a massive deployment of BogusBiter is that if the login page of a legitimate website is wrongly flagged as a phishing page, the load on the authentication web server will increase significantly due to a large number of bogus bites.

Shahriar et al. proposed and implemented a desktop-based testing tool named Phishtester. Phishtester works by testing the trustworthiness of a number of suspected websites through a provision of unknown random inputs to the login page. The tester checks the login page response against the pre-established known symptoms for a malicious site. This solution uses Finite State Machine (FSM) and only works based on a trigger that depends on certain conditions, signifying phishing attempt, to be true as pre-specified. Like any other rule-based system, if all the antecedent(s) of a rule are true, then the system is triggered. This might not be suitable to all problem domains, it is only suitable when a system behaviour can be decomposed into separate states with well-defined conditions for state transitions.

Wu et al. proposed MobiFish mobile application, which is similar to PhishX. However, it is deployed through Optical Character Recognition (OCR) for checking visual similarities between malicious and legitimate websites. Visual similarity approaches have a tendency of missing well-presented phishing webpages.

3. REQUIREMENT SPECIFICATION

3.1. *Hardware Requirement*

1. CPU Quad Core and above and
2. RAM 8 GB and above
3. Hard Disk 500GB and above

3.2. *Software requirement*

1. CPU Windows 8/10, Linux Operating System
2. Android Studio
3. XAMPP Server
4. All Android devices with PhishX and Google chrome browser

5. MySQL DatabaseQuad Core and above and

4. SYSTEM ARCHITECTURE AND PROPOSED SOLUTION

Sub-headings most anti-phishing solutions are only effective on desktop computers due to computational power issues. By considering the unsuitability of those solutions for low-powered mobile devices, we propose and develop an android application prototype, PhishX, which simulates user authentication procedure through lightweight Java classes and methods. PhishX intercepts a login page opened by a user and simulates the login procedure with fake credentials. Technically, an authentication attempt to a login webpage with incorrect login credentials tests the trustworthiness of that page. However, a user needs to have a prior knowledge and remembers to do so every time she encounters a suspicious page. They believe, in small size devices, this procedure is tedious when done manually. The work addresses these issues by automating the login procedure through android application on mobile devices.

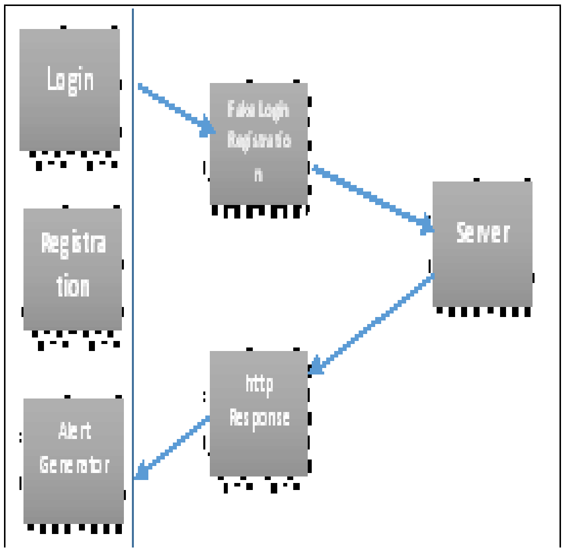
4.1. *Scope and Assumptions*

The work focuses on mobile devices that use an android operating system. However, it is not limited to android- based devices only, it can be re-developed for other device operating systems such as iOS (formerly iPhone OS). Since the solution depends on RFC 2616 [13] industrial standard response for client requests, they are limited to legitimate websites that conform to that standard. Some web servers, such as http://www.nike.com, that implement such server standards for an authentication failure, fit well into the solution scope. Together with other criteria, it is easier to deduce a phishing site when it does not behave like a legitimate one. The standard information can be a certain response code equivalent to a client request such as HTTP 401 Unauthorized or 403 Forbidden. To capture this information they customize and implement several Java classes in PhishX.

4.2. *System Model / Architecture*

Following Fig. 1 shows system architecture.

Fig. 1 System Architecture



4.3. Implementation

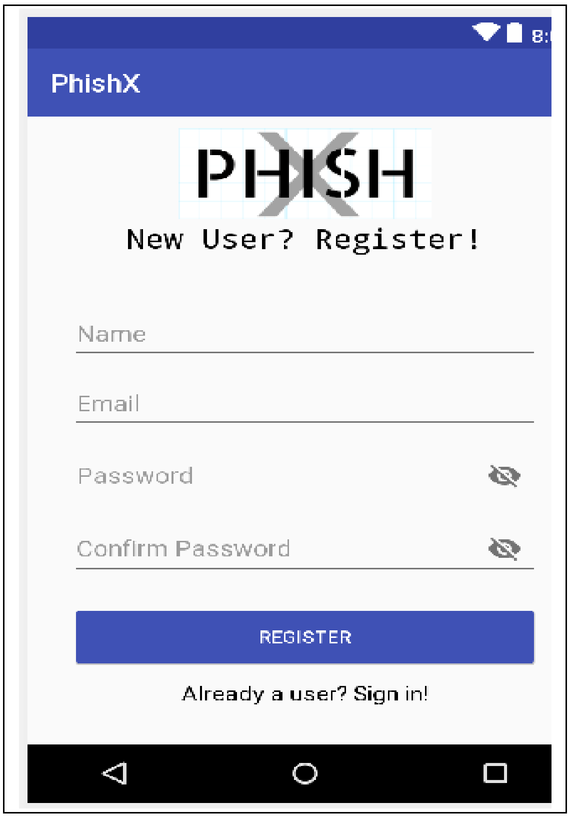


Fig. 2 User Registration

5. CONCLUSION

Social engineering techniques are used by attackers to convince their victims into clicking a malware or deceptive login-based webpages. Most solutions focus on helping desktop computer users than mobile device users. Mobile device users are more vulnerable than their desktop counterparts because they are online most of the time and they have device limitations such as smaller screen size and low computational power. Our system PhishX, an effective mobile application prototype that takes advantage of a particular weakness of phishing sites: they accept any kind of input information for authentication. PhishX enables a mobile device user to create fake login account, with fake login credentials, that mimics user login procedure every time the user opens a login webpage and generates an alert to her. The results show that PhishX is effective in assisting users to identify phishing attacks with an accuracy of 96%.

REFERENCES

[1] Yue, C. and Wang, H., 2008, December. Anti-phishing in offense and defense. In Computer Security Applications Conference, 2008. ACSAC 2008. Annual (pp. 345-354). IEEE.
[2] Marforio, C., Masti, R.J., Soriente, C., Kostiainen, K. and Capkun, S., 2016, October. Hardened Setup of Personalized Security Indicators to Counter Phishing Attacks in Mobile Banking. In Proceedings of the 6th Workshop on Security and Privacy in Smartphones and Mobile Devices (pp. 83-92). ACM.
[3] http://www.tomsitpro.com/articles/advanced-persistent-threats-apt-101,2-526.html (Accesed on February 2017)
[4] Nguyen, L.A.T., Nguyen, H.K. and To, B.L., 2016. An efficient approach based on neuro-fuzzy for phishing detection. Journal of Automation and Control Engineering Vol, 4(2).
[5] Arachchilage, N.A.G., Love, S. and Beznosov, K., 2016. Phishing threat avoidance behaviour: An empirical investigation. Computers in Human Behavior, 60, pp.185-197.
[6] Purkait,S.,2012.Phishing counter measures and their effectiveness literature review. Information Management & Computer Security, 20(5), pp.382-420.
[7] Afroz, S. and Greenstadt, R., 2011, September. Phishzoo: Detecting phishing websites by looking at them. In Semantic Computing (ICSC), 2011 Fifth IEEE International Conference on (pp. 368-375). IEEE.
[8] Zhang, Y., Hong, J.I. and Cranor, L.F., 2007, May. Cantina: a content- based approach to detecting phishing web sites. In Proceedings of the 16th international conference on World Wide Web (pp. 639-648). ACM.
[9] USA Information Resources Management Association, 2011. Cyber Crime: Concepts, Methodologies, Tools and Applications.
[10] Jensen, M., Durcikova, A. and Wright, R., 2017, January. Combating Phishing Attacks: A Knowledge Management Approach. In Proceed-ings of the 50th Hawaii International Conference on System Sciences.

(A.1)