Detection of Malicious Web pages in Mobile

Syeda Farheen Sultana[1] Dr. Sameena Banu[2]
[1]PG Student [2]Professor & Course Co-ordinator
[1,2]Department of Computer Science & Engineering
[1,2]K.B.N College of Engineering, Kalaburgi, Karnataka, India

Abstract— Web security is becoming an important concern. As mobile malicious web pages that exploit user's vulnerabilities, is a threat to the security of the user. Hence, there has been an interest in developing a systems to prevent the end user from accessing such pages. Mobile web pages is different in their design, and content. Hence, existing methods to identify maliciousness are improbable to work for such mobile website pages. In our paper, we propose and execute kAYO, a program that identify malice website pages. We begin with, presenting the requirement for the mobile and then static features are obtained .We at that point apply kAYO to a dataset of more than 350,000 known benevolent and malevolent portable pages and show 90% of correctness in order. Additionally, we find, various report of website pages skipped by Google Safe Browsing and Virus Total, which is found by kAYO. Thus, we develop a program which uses kAYO to defend users from malicious site pages.

Key words: Web Security, Vulnerability

I. INTRODUCTION

To access the web, Mobile devices are used. And the Mobile browsing experience is different in spite of all the advances. These differences are due to small size of the screen, which impacts the content, functionality and layout of mobile web pages. Content, functionality and layout are utilize to do static analysis, to figure out maliciousness of webpage. Some of the Features like iframes frequency and the number of redirections have served as strong pointer to malevolent. Before users gain access to content, benign mobile web pages require many redirections. Previous techniques fall short to consider mobile specific. Webpage elements such as mobile APIs call. Therefore, new tools are required to identify mobile malicious web pages. In this paper, we present kAYO, a speedy and suitable static analysis strategy to detect malicious web page in mobile.

II. LITERATURE SURVEY

P. Kolari, et.al [1] the author tells that Weblogs have significant method to publish data, rise in popularity of these blogs has leads to search and analysis engines concentrating on the "blogosphere". An important need of these system is to recognize blog across the Web. While this assure blog are registered. In this paper, author identify blogs using Support Vector Machines (SVM). Compare results and bring new features for blog detection.

A. Markopoulou et.al [2] the author tells that Phishing is increasing rapidly, it is an advanced strategy to steal sensitive data. In this paper, we found how to differentiate phishing URLs. First and foremost, we take lexical highlights of the URLs that prevent from attack. Next, we consider calculations, and we forth put to use an online strategy (AROW) that can surmount noisy information .Based on knowledge we draw from our research, we propose Phish Def, a phishing recognition method that make use of just URL names to detect phishing. Phish Def is a correct technique (when checked with approaches over true datasets), lightweight (fit for on the web and client implementation), proactive (on the basis of online grouping in lieu of blacklist), and strong enough to tolerate information imprecision (hence, enabling the use of data that is noisy).

A. Ikinci, et.al [3] the author tells that malicious websites on client side exploit vulnerability which causes serious threat to security of the innocent client. At present, there is neither a broad database of threat on the Web nor tools to construct such database. In this work, author present the Monkey-Spider venture [Mon]. Considering it as a client honeypot, we take the challenge and evaluate our system as a fast, and a t Internet-scale examination to construct a database of threat.

III. SYSTEM ARCHITECTURE

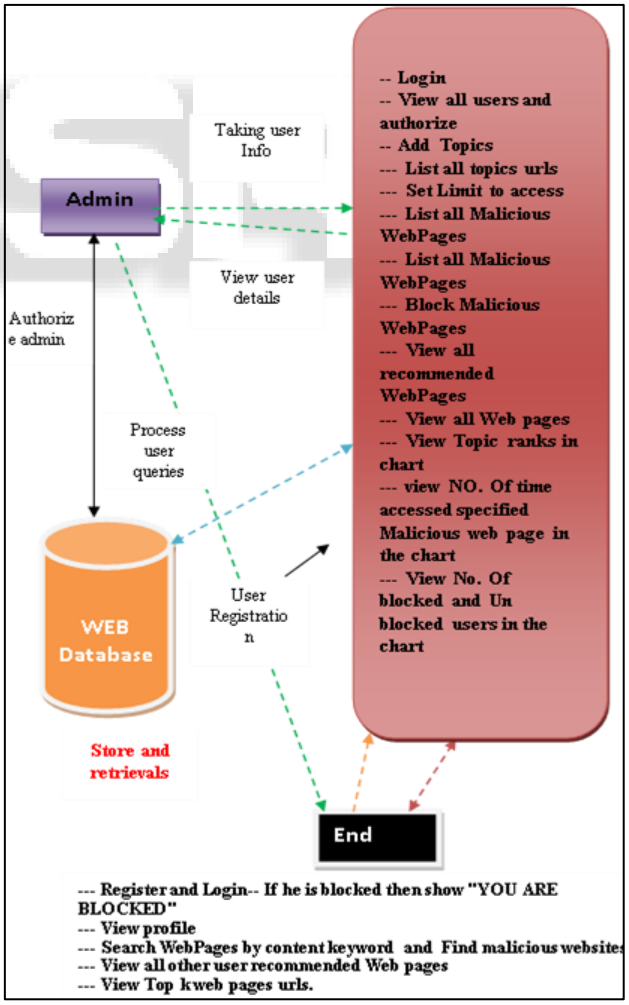

Fig. 1: System Architecture

IV. IMPLEMENTATION

A. Modules

There are three modules used in this project:

- Admin
- User
- Attacker

B. Module Description

1) Admin

- First and Foremost admin has to login with a valid username & password.
- After login admin is authorized to see all the topics, add the topics, list all webpages that are malicious.
- Also, admin has the privilege to block or unblock the users.

2) User

- User needs to register itself before searching the contents.
- After successful registration the user can login by entering valid user name and password.
- After successful login the user is authorized to do some operations --- View profile, Search keyword content - Click on topic name to view all the details.

3) Attacker

In this module, First the attacker login, then he will add the malicious site URL and the related information and he can see the information of malicious site post adding to the malicious site.

V. RESULT ANALYSIS

A. Screen Shots

1) Admin Login

Here the admin login first.

Fig. 2: Admin Login

Fig. 3: Admin Adding Topic

2) User Login

Registered User First Login Then He Search Webpage Content Using the Keyword

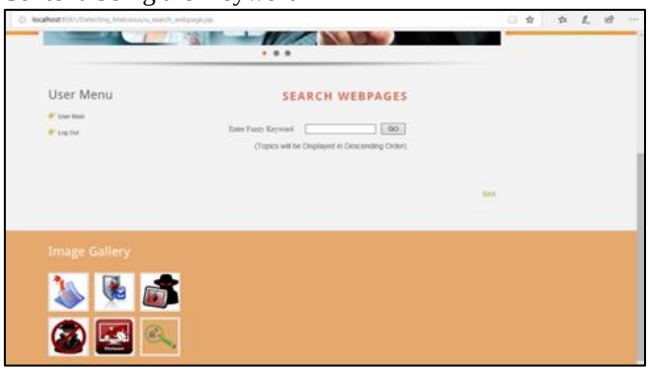

Fig. 4: User Search Web Pages Using Keyword

Fig. 5: Malicious Web Pages Alert

3) Attacker

After login, attacker will add the malicious site URL and its related info

Fig. 6: Adding Malicious Webpage Topics

VI. CONCLUSION

Web pages are wholly unique in relation to their area of work, usefulness and format. So, existing techniques using static highlights to distinguish maliciousness doesn't work well for mobile webpage. We frame and built up a fast and suitable static analysis system called kAYO which recognizes malicious web pages. kAYO makes these recognitions by calculating 44 mobile highlights, from which 11 are latest highlights. kAYO foresee 90% exactitude in characterization, and recognizes diverse malicious website pages that existing procedures are unable to distinguish , for instance, Virus-Total. And Google-Safe Browsing. Ultimately, we develop a program using kAYO that gives alert to the users. We deduce that kAYO recognizes menace and provide security to the users.

ACKNOWLEDGEMENT

I take his opportunity to thank my guide Prof. Dr Sameena Banu for her guidance and sharing her findings for technical guidance and direction. Her valuable Suggestions given by her were always helpful in this work to succeed.

REFERENCES

[1] P. Kolari, T. Finin, and A. Joshi. Svms for the blogosphere: Blog identification and splog detection. In Proceedings of AAAI Spring Symposium on Computational Approaches to Analysing Weblogs, 2006.
[2] Le, A. Markopoulou, and M. Faloutsos. Phishdef: Url names say it all. In Proceedings of IEEE International Conference on Computer Communications (INFOCOM), 2011.
[3] Ikinci, T. Holz, and F. Freiling. Monkey-spider: Detecting malicious websites with low-interaction honeyclients. In Proceedings of Sicherheit, Schutz und Zuverlassigkeit, 2008.

