National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

Design the Framework for Detecting Malicious Mobile Web-Pages in Real Time

Sushma K[1], Dr. K. Thippeswamy[2]
*[1]M.Tech in CS&E, VTU PG Centre, Mysuru, Karnataka, India
[2]Professor and Chairman, DoS in CS&E, VTU PG Centre, Mysuru, Karnataka, India

ABSTRACT

Mobile specific web pages differ significantly from their desktop counterparts in content, layout and functionality. Accordingly, existing techniques to detect malicious websites are unlikely to work for such web pages. The disclosed technology includes techniques for identifying malicious mobile electronic documents, e.g. web pages or emails, based on static document features. In this paper, we design and implement kAYO, a mechanism that distinguishes between malicious and benign mobile web pages. kAYO makes this determination based on static features of a webpage ranging from the number of iframes to the presence of known fraudulent phone numbers. We then apply kAYO to a dataset of over 350,000 known benign and malicious mobile web pages and demonstrate 90% accuracy in classification. Moreover, we discover, characterize and report a number of web pages missed by Google Safe Browsing and Virus Total, but detected by kAYO.

I. INTRODUCTION

Internet connected mobile devices are going to outnumber humans [2]. Moreover, global mobile data traffic is expected to increase 13-fold between 2012 and 2017. Both platform specific applications ("native apps") and browser-based applications ("web apps") enable mobile device users to perform security sensitive operations such as online purchases, bank transactions and accessing social networks. The distinction between native apps and web apps on mobile devices is increasingly being blurred. HTML5 becomes universally deployed and mobile web apps directly take advantage of device features such as the camera, microphone and relocation, the difference between native and web apps will vanish almost entirely. A recent study of Smartphone usage shows that more people browse the Web than use native apps on their phone. The trend and the increasing use of web browsers on modern mobile phones warrant characterizing existing and emerging threats to mobile web browsing. Although a range of studies have focused on the security of native apps on mobile devices, efforts in characterizing the security of web transactions originating at mobile browsers are limited. Mobile web browsers have long underperformed their Desktop counterparts. However, recent improvements in processing power and bandwidth have spurred significant changes in the ways users experience the mobile web. Modern mobile browsers provide rich functionality equivalent to their desktop counterparts using web technologies such as HTML, JavaScript, and CSS. Furthermore, browsers on mobile platforms now build on the same or similarly capable rendering engines used by many desktop browsers. Mobile users are three times more likely to access phishing websites than desktop users [3]. Mobile devices are increasingly being used to access the web [1]. However, in spite of significant advances in processor power and bandwidth, the browsing experience on mobile devices is considerably different. These differences can largely be attributed to the dramatic reduction of screen size, which impacts the content, functionality and layout of mobile web pages. Identify the malicious URLs based

on dynamically extracted lexical patterns from URLs. They developed a new method to mine their URL patterns, which are not assembled using any pre-defined items and thus cannot be mined using any existing frequent pattern mining methods. It can provide new flexibility and capability malicious URLs algorithmically generated by malicious programs. Content, functionality and layout have regularly been used to perform static analysis to determine maliciousness in the desktop space. Features such as the frequency of iframes and the number of redirections have traditionally served as strong indicators of malicious intent. Due to the significant changes made to accommodate mobile devices, such assertions may no longer be true. For example, whereas such behavior would be flagged as suspicious in the desktop setting, many popular benign mobile web pages require multiple redirections before users gain access to content. Previous techniques also fail to consider mobile specific webpage elements such as calls to mobile APIs.. Static features of mobile webpages derived from their HTML and JavaScript content, URL and advanced mobile specific capabilities. Our design detects a number of malicious mobile webpages not precisely detected by existing techniques such as Virus Total and Google Safe Browsing. Finally, we discuss the existing tools to detect mobile malicious webpages and phishing attack and build a browser extension.

II. MOTIVATION

Static analysis techniques to detect malicious websites often use features of a webpage such as HTML, JavaScript and characteristics of the URL. Usually, these features are fed to machine learning techniques to classify benign and malicious web pages. These techniques are predicated on the assumption that the features are distributed differently across benign and malicious web pages. Accordingly, any changes in the distribution of static features in benign and/or malicious web pages impacts successful, these static analysis techniques have been used exclusively for desktop web pages. Mobile websites are significantly different from their desktop counterparts in content, functionality and layout. Consequently, existing tools using static features to detect malicious desktop web pages are unlikely to work for mobile web pages.

III. PROPOSED WORK

Proposed work includes the following –

- The proposed method focus on mobile specific threats. Proposed method work on the mobile specific web pages. Existing technique to detect malicious websites are unable to work on mobile. Here determination is based on the static as well as dynamic features.

- The proposed method is outlined in figure this system use URL to get malicious content.

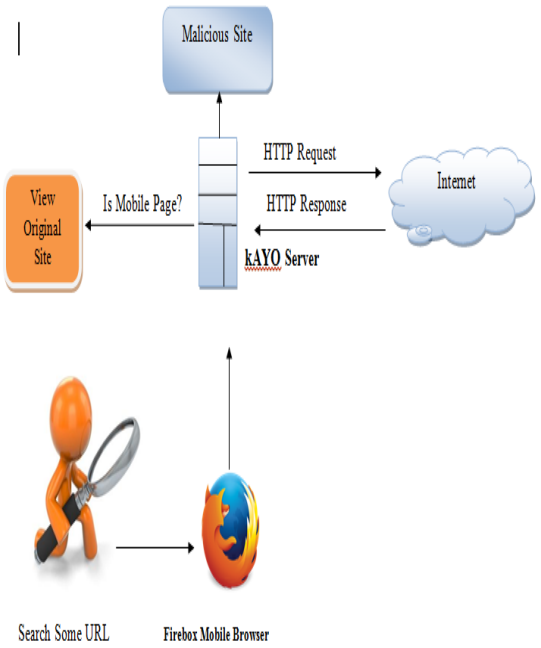

Figure 1. proposed methodology

- Our application is use to check the malicious function. Here OCR (optical character recognition) technique is also introduced. OCR is technique that convert image into text to detect valuable phishing attack.
- User enters the URL he wants to visit in the extension toolbar. The extension then sends the URL backend server over HTTPS.
- If the URL is not malicious and free from phishing attack according to our app, then it will open webpage in the browser automatically.

- Otherwise, a warning message is shown to the user recommending them not to visit the URL or visit on their own risk.

- If application identifies that the pages are malicious then the proposed method will generate an output i.e it detect a malicious webpages or phishing site.

IV. CONCLUSION

In this way, we study the framework for detecting malicious mobile webpages in real time. Mobile webpages are significantly different than their desktop counterparts in content, functionality and layout. Therefore, existing techniques using static features of desktop webpages to detect malicious behavior for mobile specific pages. We designed and developed a fast and reliable static analysis technique that detects mobile malicious webpages and also detect phishing sites. Our application provides greater accuracy in classification, and detects a number of malicious mobile webpages in the wild that are not detected by existing techniques such as Cantina. Finally, we build a browser extension that provides real-time feedback to users. We proposed an application for mobile platforms. Our application resolves this issue by using OCR, which can accurately extract text from the screenshot of the login interface so that the claimed identity of phishing attacker can be verified. We conclude that our application detects new mobile specific threats such as websites hosting and takes the first step towards identifying new security challenges in the modern mobile web.

V. ACKNOWLEDGEMENT

I take his opportunity to express my hearty thanks to my guide Dr. K. THIPPESWAMY Professor and Chairman, Department of studies in CS&E VTU regional Office, Mysuru for his guidance and sharing his findings for technical guidance and direction. Suggestions given by him were always helpful in this work to succeed. His leadership has been greatly valuable for me to work on this project and come with best out of it.

VI.REFERENCES

[1]. Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor, Senior Member, IEEE "Detecting Mobile Malicious
Webpages in Real Time" Chaitrali Amrutkar, Young Seuk Kim, and Patrick Traynor, Senior Member, IEEE

[2]. Charles Arthur, "Mobile internet devices 'will outnumber humans this year'." http://www.theguardian. com/ technology/ 2013/feb/07/ mobile-internet-outnumber-people.

[3]. Chakradeo, S., Reaves, B., Traynor, P., and Enck, W., "MAST: Triage for Market-scale Mobile Malware Analysis," Tech. Rep. GT-CS-12-01, College of Computing, Georgia Institute of Technology, 2012.

[4]. N. Provos, P. Mavrommatis, M. A. Rajab and F. Monrose, "All Your iFRAMEs Point to Us", Proceedings of the 17th Conference on Security Symposium, SS, USENIX Association Berkeley, (2008); CA,USA.

[5]. D. Canali, M. Cova, G. Vigna, and C. Kruegel. Prophiler: a fast filter for the large-scale detection of malicious webpages. In Proceedings of the 20th International Conference on World Wide Web (WWW), 2011.

[6]. L. Bilge, E. Kirda, C. Kruegel, and M. Balduzzi. EXPOSURE: Finding malicious domains using passive DNS analysis. In Proceedings of the 18th Annual Network and Distributed System Security Symposium (NDSS), 2011.

[7]. A. P. Felt and D. Wagner. Phishing on mobile devices. In Web 2.0 Security and Privacy (W2SP), 2011.

[8]. "Cross-site Scripting (XSS) Attacks and Defense
Mechanisms: classification and state-of-art" by Shashank Gupta and B.B Gupta ,14 September,2015, Springer.

[9]. Dr. Jitendra Agrawal, Dr. Shikha Agrawal, Anurag Awathe, Dr. Sanjeev Sharma. "Malicious Web Page Detection through Classification Technique: A Survey". In Proceeding of the IJCST March 2017.