International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

ELSEVIER SSRN

IJIEMR Transactions, online available on 30th Dec 2018. Link :

http://www.ijiemr.org/main/index.php?vol=Volume-07&issue=ISSUE-13

Title: IN REAL TIME: A NOVEL APPROACH FOR DETECTING MALICIOUS MOBILE WEBPAGES

Volume 07, Issue 13, Pages: 693–698.

Paper Authors

PIKKILI BHAVANI, VADAPALLI GOPI

SRI VANI EDUCATIONAL SOCIETY GROUP OF INSTITUTIONS, A.P., INDIA.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

IN REAL TIME: A NOVEL APPROACH FOR DETECTING MALICIOUS MOBILE WEBPAGES

PIKKILI BHAVANI[1], VADAPALLI GOPI[2]

[1]Student[CSE], SRI VANI EDUCATIONAL SOCIETY GROUP OF INSTITUTIONS, A.P., India.

[2] ASSOCIATE PROFESSOR & HEAD OF THE DEPARTMENT, Dept of CSE, SRI VANI EDUCATIONAL SOCIETY GROUP OF INSTITUTIONS, A.P., India.

[1]pikkilibhavani@gmail.com

Abstract —The disclosed technology includes techniques for identifying malicious mobile electronic documents, e.g. WebPages or emails, based on static document features. The static features may include mobile-specific features, such as mobile web API calls, hosted mobile-specific binaries, no script content, or misleading URL tokens visible on a mobile specific inter face. The static features may instead or also include various JavaScript JS features, HTML features, and URL features detected in numbers outside ranges expected for desktop electronic documents. These features may be used with machine learning techniques to classify benign and malicious documents in real time. Recent years have witnessed the increasing threat of phishing attacks on mobile computing platforms. Finally, design a browser extension to protect users from malicious mobile websites in real-time.In this paper, we design and implement kAYO, a mechanism that distinguishes between malicious mobile WebPages. Various methodologies are proposed to detect the malicious websites based on features like web contents, HTML codes, session information, and dynamic behaviours. Apply kAYO to a dataset of over 350,000 known benign and malicious mobile web pages and demonstrate 90% accuracy in classification. Moreover, discover, characterize and report a number of web pages missed by Google Safe Browsing and Virus Total, but detected by kAYO. Finally, build a browser extension using kAYO to protect users from malicious mobile websites in real-time.

Keywords — Malicious Websites, Web Browser, malicious web page tracker techniques.

1. INTRODUCTION

Mobile specific webpages differ significantly from their desktop counterparts in content, layout and functionality. Accordingly, existing techniques to detect malicious websites are unlikely to work for such webpages. The disclosed technology includes techniques for identifying malicious mobile electronic documents, e.g. webpages or emails, based on static document features. The static features may include mobile-specific features, such as mobile web API calls, hosted mobile-specific binaries, no script content, or misleading URL tokens visible on a mobile specific inter face. The static features may

instead or also include various JavaScript JS features, HTML features, and URL features detected in numbers outside ranges expected for desktop electronic documents. These features may be used With machine learning techniques to classify benign and malicious documents in real time. Recent years have witnessed the increasing threat of phishing attacks on mobile computing platforms. Malicious Web pages are increasingly spread while we accessing the web. 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. 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 I frames 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. For instance, links that spawn the phone's dialer (and the reputation of the number itself) can provide strong evidence of the intent of the page. New tools are therefore necessary to identify malicious pages in the mobile web. In this paper, we present MWPT , a fast and reliable static analysis technique to detect malicious mobile web-pages. MWPT uses static features of mobile web pages derived from their HTML and JavaScript content, URL and advanced mobile specific capabilities. We first experimentally demonstrate that the distributions of identical static features when extracted from desktop and mobile web pages vary dramatically. We then collect over 350,000 mobile benign and malicious web pages over a period of three months. We then use a binomial classification technique to develop a model for MWPT to provide 90% accuracy and 89% true positive rate. MWPT's performance matches or exceeds that of existing static techniques used in the desktop space. MWPT also detects a number of malicious mobile web pages not precisely detected by existing techniques such as Virus Total and Google Safe Browsing. 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. For instance, links that spawn the phone's dialer (and the reputation of the number itself) can provide strong evidence of the intent of the page.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

New tools are therefore necessary to identify malicious pages in the mobile web. In this paper, we present kAYO. The coming and the rising fame of systems, Internet, intranets and conveyed frameworks, security is getting to be one of the central purposes of exploration.

2. PROPOSED METHOD

The existing system called Content-based and in-depth inspection techniques to detect malicious websites: Dynamic approaches using virtual machines and honey client systems provide deeper visibility into the behavior of a webpage. Therefore, such systems have a very low false positive rate and are more accurate. However, downloading and executing each webpage impacts performance and hinders scalability of dynamic approaches. This performance penalty can be avoided by using static approaches. Static approaches rely on the structural and lexical properties of a webpage and do not execute the content of the webpage.One such technique of detecting malicious URLs is using statistical methods for URL classification based on a URL's lexical and host-based properties. However, URL-based techniques usually suffer from high false positive rates. Using HTML and JavaScript features extracted from a webpage in addition to URL classification helps address this drawback and provides better results. Static approaches avoid performance penalty of dynamic approaches. Additionally, using fast and reliable static approaches to detect benign web pages can avoid expensive in-depth analysis of all web pages.

PROPOSED SYSTEM:

In the existing system, the system experimentally demonstrates that the distributions of static features used in existing techniques (e.g., the number of redirections) are different when measured on mobile and desktop web pages. Moreover, we illustrate that certain features are inversely correlated or unrelated to or non-indicative to a webpage being malicious when extracted from each space. The results of our experiments demonstrate the need for mobile specific techniques for detecting malicious web pages.

3. LITURATURE SURVEY

Y. Zhang studied the problem that the biggest threat on the mobile web at present is believed to be phishing. The best known nonproprietary content-based approach to detect phishing webpages is Cantina. Cantina suffers from performance problems due to the time lag involved in querying the Google search engine. Moreover, Cantina does not work well on webpages written in languages other than English. Finally, existing techniques do not account for new mobile threats such as known fraud phone numbers that attempt to trigger the dialer on the phone.

Dr. Jitendra Agrawal studies malicious web page detection through classification Technique. Detection of malicious web has become a necessary and hot topic of research as numbers of internet users are increasing at a high pace. There are lots of challenges regarding this detection process. First the number of online URL is very large. Second web environment uses diverse

platform and difficult to find security solution for them. Third now threats are become more and more complex and used various obfuscation techniques to bypass detection techniques. The existing detection techniques are focused only on single type of attacks only. New generated malicious web pages exploit multiple types of attacks for targeting the client. Cloaking type of attacks is difficult to detect because these web respond differently to browser and crawler. Size of web is a big challenge in the process.

Paul C. van Oorschot studies measuring of SSL indicators on mobile browsers. Although these browsers aim for equivalent functionality to traditional desktops, their smaller screen size has resulted in significant changes to the presentation and availability of SSL indicators. Their study presents the first large scale, cross-sectional measurement of this class of applications and compares the security indicators used in the overwhelming majority of mobile browsers to their traditional desktop counterparts.

Davide Canali proposed a filter for the large-scale detection of malicious web pages. A system whose aim is To provide a filter that can reduce the number of web pages that Need to be analyzed dynamically to identify malicious web pages. As malware on the Internet spreads and becomes more sophisticated, Antimalware techniques need to be improved in order to Be able to identify new threats in an efficient, and, most important, automatic way. Adrienne Porter Felt studied and examine the threat of phishing on mobile devices. A successful phishing attack has two parts: the user must be conditioned to enter her credentials in a certain setting, and the attacker must be able to imitate that setting. He studies real mobile applications and web sites to understand the scenarios in which users enter passwords on mobile phones, and then we propose attacks that subvert these scenarios. Many applications and web sites link to each other for the purpose of social sharing and payment, both of which require the user to enter her authentication credentials in contexts where the user has no way to identify who is receiving those credentials. Users are therefore likely accustomed to switching from one application to another and then entering their passwords into the second application, without any way to verify the authenticity of the second application. A malicious application can link the user to a social networking or payment web site, and then present the user with a fake login screen. Alternately, an attacker can intercept the interaction and substitute a fake login screen for the intended target. His research will motivate us in defenses against mobile phishing

4. RELATED WORK

A Framework for Detection and Measurement of Phishing Attacks: Phishing is form of identity theft that combines social engineering techniques and sophisticated attack vectors to harvest financial information from unsuspecting consumers. Often a phisher tries to lure her victim into clicking a URL pointing to a rogue page.

The structure of URLs employed in various phishing attacks. We find that it is often possible to tell whether or not a URL belongs to a phishing attack without requiring any knowledge of the corresponding page data. several features that can be used to distinguish a phishing URL from a benign one. These features are used to model a logistic regression filter that is efficient and has a high accuracy. We use this filter to perform thorough measurements on several million URLs and quantify the prevalence of phishing on the Internet today. Drawback is URL-based techniques usually suffer from high false positive rates.

A Content-Based Approach to Detecting Phishing Web Sites: Phishing is a significant problem involving fraudulent email and web sites that trick unsuspecting users into revealing private information, the design, implementation, and evaluation of CANTINA, a novel, content-based approach to detecting phishing web sites, based on the TF-IDF information retrieval algorithm. The design and evaluation of several heuristics we developed to reduce false positives. CANTINA is good at detecting phishing sites, correctly labeling approximately 95% of phishing sites. CANTINA has comparable or better performance to Spoof Guard (a heuristic-based anti-phishing tool) with far fewer false positives, and does about as well as Net Craft (a blacklist and heuristic-based anti-phishing toolbar). Finally, we show that CANTINA combined with heuristics is effective at detecting phishing URLs in users' actual email, and that its most frequent mistake is labeling spam-related URLs as phishing. Drawback is Cantina suffers from performance problems due to the time lag involved in querying the Google search engine.

Prophiler: a Fast Filter for the Large-Scale Detection of Malicious Web Pages: Malicious web pages that host drive-by-download exploits have become a popular means for compromising hosts on the Internet and, subsequently, for creating large-scale botnets. In a drive-by download exploit, an attacker embeds a malicious script (typically written in JavaScript) into a web page. When a victim visits this page, the script is executed and attempts to compromise the browser or one of its plug-in. To detect drive-by-download exploits, researchers have developed a number of systems that analyze web pages for the presence of malicious code. In this paper, we describe the design and implementation of such a filter. Our filter, called Prophiler, uses static analysis techniques to quickly examine a web page for malicious content. This analysis takes into account features derived from the HTML contents of a page, from the associated JavaScript code, and from the corresponding URL. We automatically derive detection models that use these features using machine-learning techniques applied to labeled datasets. Drawback is Malicious desktop websites will work well on mobile websites is yet to be explored. Cantina does not work well on WebPages written in languages other than English. Finally, existing techniques do not account for new mo- bile threats such as

known fraud phone numbers that attempt to trigger the dialer on the phone.

CONCLUSION

In this paper, proposed the 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 International Journal of Engineering Science and Computing, May 2017 11887 http://ijesc.org/ 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. proposed an application for mobile platforms. 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.

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
,2015.

[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