DETECTING MOBILE MALICIOUS WEBPAGES IN REAL TIME

GOBERU NAGA SARANYA[1], K.CHANDRAMOULI[2]

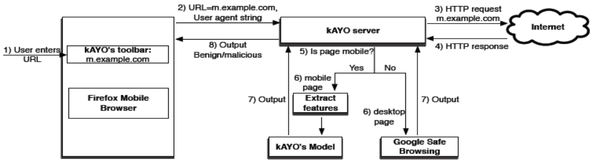
[1]Assistant Professor, Dept. of MCA, NRI INSTITUTE OF TECHNOLOGY, A.P., India.

[2]Student(MCA), NRI INSTITUTE OF TECHNOLOGY, A.P., India.

Abstract — In this paper, we design and implement KAYO, a mechanism that distinguishes between malicious and benign mobile webpages. 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. First, we experimentally demonstrate the need for mobile specific techniques and then identify a range of new static features that highly correlate with mobile malicious webpages. We then apply KAYO to a dataset of over 350,000 known benign and malicious mobile webpages and demonstrate 90% accuracy in classification. Moreover, we discover, characterize and report a number of webpages missed by Google Safe Browsing and Virus Total, but detected by KAYO. Finally, we build a browser extension using KAYO to protect users from malicious mobile websites in real-time. In doing so, we provide the first static analysis technique to detect malicious mobile webpages.

INTRODUCTION

Mobile devices area unit progressively being employed to access the net. However, in spite of great advances in processor power and information measure, the browsing expertise on mobile devices is significantly completely different. These variations will for the most part be attributed to the dramatic reduction of screen size, that impacts the content, practicality and layout of mobile webpages. Content, practicality and layout have frequently been wont to perform static analysis to see spitefulness within the desktop area [1]. Options appreciate the frequency of iframes and therefore the variety of redirections have historically served as sturdy indicators of malicious intent. Because of the numerous changes created to accommodate mobile devices, such assertions could not be true. For instance, whereas such behavior would be flagged as suspicious within the desktop setting, several standard benign mobile webpages need multiple redirections before users gain access to content. Previous techniques conjointly fail to think about mobile specific webpage parts appreciate calls to mobile arthropod genus [2]. to Illustrate, links that spawn the phone's dialer (and the name of the amount itself) will offer sturdy proof of the intent of the page. New tools area unit so necessary to spot malicious pages within the mobile internet. During this paper, we have a tendency to gift kAYO1, a quick and reliable static analysis technique to notice malicious mobile web- pages.



LITERATURE SURVEY

1) VulnerableMe: Measuring systemic weaknesses in mobile browser security

AUTHORS: C. Amrutkar, K. Singh

Porting browsers to mobile platforms may lead to new vulnerabilities whose solutions require careful balancing between usability and security and might not always be equivalent to those in desktop browsers. In this paper, we perform the first large-scale security comparison between mobile and desktop browsers. We focus our efforts on display security given the inherent screen limitations of mobile phones. We evaluate display elements in ten mobile, three tablet and five desktop browsers. We identify two new classes of vulnerabilities specific to mobile browsers and demonstrate their risk by launching real-world attacks including display ballooning, login CSRF and clickjacking. Additionally, we implement a new phishing attack that exploits a default policy in mobile browsers. These previously unknown vulnerabilities have been confirmed by browser vendors. Our observations, inputs from browser vendors and the pervasive nature of the discovered vulnerabilities illustrate that new implementation errors leading to serious attacks are introduced when browser software is ported from the desktop to mobile environment. We conclude that usability considerations are crucial while designing mobile solutions and display security in mobile browsers is not comparable to that in desktop browsers.

2) Measuring SSL indicators on mobile browsers: Extended life, or end of the road?

AUTHORS: C. Amrutkar, P. Traynor

Mobile browsers are increasingly being relied upon to perform security sensitive operations. Like their desktop counterparts, these applications can enable SSL/TLS to provide strong security guarantees for communications over the web. However, the drastic reduction in screen size and the accompanying reorganization of screen real estate significantly changes the use and consistency of the security indicators and certificate information that alert users of site identity and the presence of strong cryptographic algorithms. In this paper, we perform the first measurement of the state of critical security indicators in mobile browsers. We evaluate ten mobile and two tablet browsers, representing over 90% of the market share, using the recommended guidelines for web user interface to convey security set forth by the World Wide Web Consortium (W3C). While desktop browsers follow the majority of guidelines, our analysis shows that mobile browsers fall significantly short. We also observe notable inconsistencies across mobile browsers when such mechanisms actually are implemented. Finally, we use this evidence to argue that the combination of reduced screen space and an independent selection of security indicators not only make it difficult for experts to determine the security standing of mobile browsers, but actually make mobile browsing more dangerous for average users as they provide a false sense of security.

3) Building a dynamic reputation system for DNS

AUTHORS: M. Antonakakis, R. Perdisci

The Domain Name System (DNS) is an essential protocol used by both legitimate Internet applications and cyber attacks. For example, botnets rely on DNS to support agile command and control infrastructures. An effective way to disrupt these attacks is to place malicious domains on a "blocklist" (or "blacklist") or to add a filtering rule in a firewall or network intrusion detection system. To evade such security countermeasures, attackers have used DNS agility, e.g., by using new domains daily to evade static blacklists and firewalls. In this paper we propose Notos, a dynamic reputation system for DNS. The premise of this system is that malicious, agile use of DNS has unique characteristics and can be distinguished from legitimate, professionally provisioned DNS services. Notos uses passive DNS query data and analyzes the network and zone features of domains. It builds models of known legitimate domains and malicious domains, and uses these models to compute a reputation score for a new domain indicative of whether the domain is malicious or legitimate. We have evaluated Notos in a large ISP's network with DNS traffic from 1.4 million users. Our results show that Notos can identify malicious domains with high accuracy (true positive rate of 96.8%) and low false positive rate (0.38%), and can identify these domains weeks or even months before they appear in public blacklists.

PROPOSED SYSTEM

- ❖ A popular approach in detecting malicious activity on the web is by leveraging distinguishing features between malicious and benign DNS usage.

- Both passive DNS monitoring and active DNS probing methods have been used to identify malicious domains. While some of these efforts focused solely on detecting fast flux service networks, another can also detect domains implementing phishing and drive-by-downloads.
- The best-known non-proprietary content-based approach to detect phishing webpages is Cantina

DISADVANTAGES:

- Existing tools such as Google Safe Browsing are not enabled on the mobile versions of browsers, thereby precluding mobile users.
- DNS based mechanisms do not provide deeper understanding of the specific activity implemented by a webpage or domain.
- Downloading and executing each webpage impacts performance and hinders scalability of dynamic approaches.
- URL-based techniques usually suffer from high false positive rates.
- 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.

- In this paper, we present KAYO, a fast and reliable static analysis technique to detect malicious mobile web-pages. KAYO uses static features of mobile webpages 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 webpages vary dramatically
- We experimentally demonstrate that the distributions of static features used in existing techniques (e.g., the number of redirections) are different when measured on mobile and desktop webpages. 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.

ADVANTAGES:

- KAYO also detects a number of malicious mobile webpages not precisely detected by existing techniques such as Virus Total and Google Safe Browsing.

- ❖ The results of our experiments demonstrate the need for mobile specific techniques for detecting malicious webpages.
- ❖ To the best of our knowledge KAYO is the first technique that detects mobile specific malicious webpages by static analysis.
- ❖ Moreover, the mobile specific design of KAYO enables detection of malicious mobile webpages missed by existing techniques.

IMPLEMENTATION

System Model

In the first module, we develop the System environment model. Website providers use JavaScript or user agent strings to identify and then redirect mobile users to a mobile specific version. We note that not all static features used in existing techniques differ when measured on mobile and desktop webpages. Mobile websites enable access to a user's personal information and advanced capabilities of mobile devices through web APIs. Existing static analysis techniques do not consider these mobile specific functionalities in their feature set.

Malicious Pages

We argue that benign webpage writers take effort to provide good user experience, whereas the goal for malicious webpage authors is to trick users into performing unintentional actions with minimal effort. We therefore examine whether a webpage has noscript content and measure the number of noscript. Intuitively, a benign webpage writer will have more noscript in the code to ensure good experience even for a security savvy user.

Identifying relevant static features

We extract static features from a webpage and make predictions about its potential maliciousness. We first discuss the feature set used in KAYO followed by the collection process of the dataset. Structural and lexical properties of a URL have been used to differentiate between malicious and benign webpages. However, using only URL features for such differentiation leads to a high false positive rate.

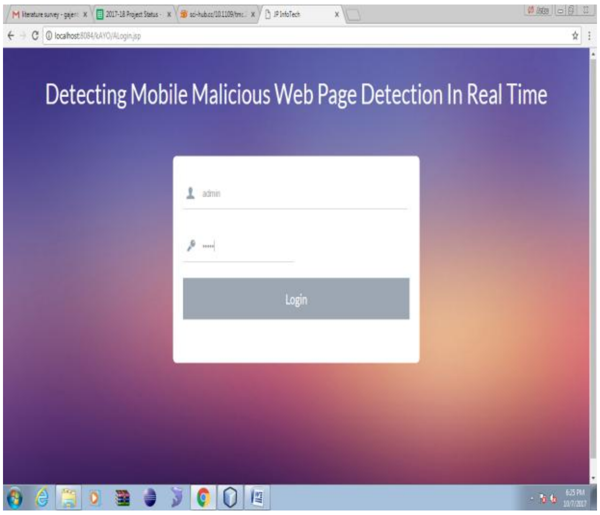
Our data gathering process included accumulating labeled benign and malicious mobile specific webpages. First, we describe an experiment that identifies and defines 'mobile specific webpages'. We then conduct the data collection process. We use these crawls specifically because they are close to the publication of the related work, making them as close to equivalent as possible.

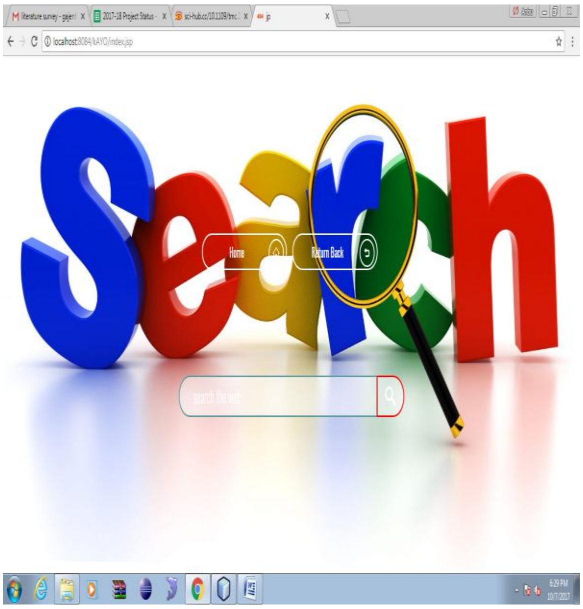
Detect malicious mobile webpages

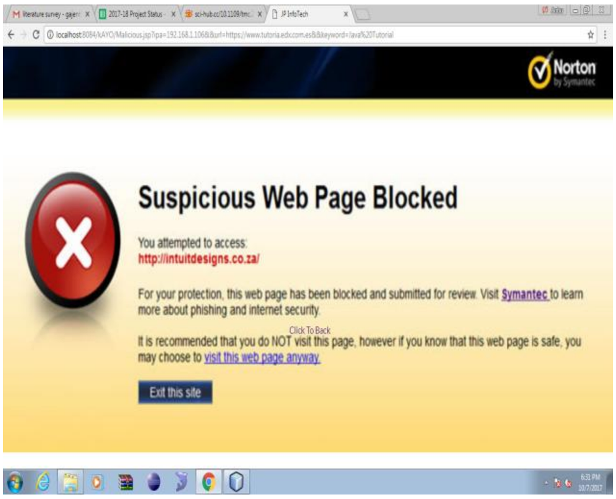
We describe the machine learning techniques we considered to tackle the problem of classifying mobile specific webpages as malicious or benign. We then discuss the strengths and weaknesses of each classification technique, and the process for selecting the best model for KAYO. We build and evaluate our chosen model for accuracy, false positive rate and true positive rate. Finally, we compare

KAYO to existing techniques and empirically demonstrate the significance of KAYO's features. We note that where automated analysis is possible, we use our full datasets; however, as is commonly done in the research community, we use randomly selected subsets of our data when extensive manual analysis and verification is required.

SAMPLE OUTPUT SCREENSHOTS


literature survey - gajen
2017-18 Project Status -
sci-hub.cc/10.1109/tmc
JP InfoTech
localhost:8084/kAYO/ALogin.jsp
Detecting Mobile Malicious Web Page Detection In Real Time
admin
Login
6:25 PM
10/7/2017





localhost:8084/kAYO/Malicious.jsp?ipa=192.168.1.106&&url=https://www.tutoria.edx.com.es&&keyword=Java%20Tutorial

Suspicious Web Page Blocked

You attempted to access:
http://intuitdesigns.co.za/

For your protection, this web page has been blocked and submitted for review. Visit Symantec to learn more about phishing and internet security.

Click To Back

It is recommended that you do NOT visit this page, however if you know that this web page is safe, you may choose to visit this web page anyway.

CONCLUSION

In this paper, 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 do not work well for mobile specific pages. We designed and developed a fast and reliable static analysis technique called KAYO that detects mobile malicious webpages. KAYO makes these detections by measuring 44 mobile relevant features from webpages, out of which 11 are newly identified mobile specific features. KAYO provides 90% accuracy in classification, and detects a number of malicious mobile webpages in the wild that are not detected by existing techniques such as Google Safe Browsing and VirusTotal. Finally, we build a browser extension using KAYO that provides real-time feedback to users. We conclude that KAYO detects new mobile specific threats such as websites hosting known fraud numbers and takes the first step towards identifying new security challenges in the modern mobile web.

REFERENCES

[1] Gnu octave: high-level interpreted language. http://www.gnu.org/software/octave/.

[2] hphosts, a community managed hosts file. http://hphosts.gt500.org/hosts.txt.

[3] Joewein.de LLC blacklist. http://www.joewein.net/dl/bl/dom-bl-base.txt.

[4] Lookout. https://play.google.com/store/apps/details?hl=en&id=com.lookout.

[5] Malware Domains List. http://mirror1.malwaredomains.com/files/domains.txt.

[6] Phishtank. http://www.phishtank.com/.

[7] Pindrop phone reputation service. http://pindropsecurity.com/phone-fraud-solutions/phone reputation service prs/.

[8] Scrapy — an open source web scraping framework for python. http://scrapy.org/.

[9] VirusTotal. https://www.virustotal.com/en/.

[10] Google developers: Safe Browsing API. https://developers.google.com/safe-browsing/, 2012.

[11] Alexa, the web information company. http://www.alexa.com/topsites,2013.

[12] dotmobi. internet made mobile. anywhere, any device. http://dotmobi.com/, 2013.

[13] C. Amrutkar, K. Singh, A. Verma, and P. Traynor. VulnerableMe: Measuring systemic weaknesses in mobile browser security. In Proceedings of the International Conference on Information Systems Security (ICISS), 2012.

[14] C. Amrutkar, P. Traynor, and P. C. van Oorschot. Measuring SSL indicators on mobile browsers: Extended life, or end of the road? In Proceedings of the Information Security Conference (ISC), 2012.

[15] M. Antonakakis, R. Perdisci, D. Dagon, W. Lee, and N. Feamster. Building a dynamic reputation system for DNS. In Proceedings of the 19th USENIX Conference on Security (SECURITY), 2010.

[16] V. A. Balasubramaniyan, A. Poonawalla, M. Ahamad, M. T. Hunter, and P. Traynor. Pindr0p: using single-ended audio features to determine call provenance. In Proceedings of the 17th ACM Conference on Computer and Communications Security (CCS), 2010.

[17] 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.

[18] M. Boodaei. Mobile users three times more vulnerable to phishing attacks. http://www.trusteer.com/blog/mobile-users-threetimes-more-vulnerable-to-phishing-attacks, 2011.

[19] M. Butkiewicz, Z. Wu, S. Li, P. Murali, V. Hristidis, H. V. Madhyastha, and V. Sekar. Enabling the transition to the mobile web with websieve. In Proceedings of the 14thWorkshop on Mobile Computing Systems and Applications (HotMobile), 2013.

[20] D. Canali, M. Cova, G. Vigna, and C. Kruegel. Prophiler: a fast filter for the large-scale detection of malicious web pages. In Proceedings

of the 20th International Conference on World Wide Web (WWW), 2011.

[21] S. Chakradeo, B. Reaves, P. Traynor, andW. Enck. MAST: Triage for Marketscale Mobile Malware Analysis. In Proceedings of the ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec), 2013.