Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 13, Number 7 (2017), pp. 3261-3273

http://www.ripublication.com

Analysing Malware Attacks on Mobile Browsers and Enhancing Security Mechanisms Using Hashing Techniques

[1]T.Senthil Kumar, [2]S.Prabakaran and [3]M.Nirmala

[1,2,3]SRM University, Chennai, Tamil Nadu 603203, India.

Abstract

Accessing the World Wide Web via mobile end devices is increasing steadily. Mobile banking is an option which gives users the possibility to perform various banking through a mobile device such as mobile phone, smartphone or tablet. Forthis, we require various protection standards to keep all private data safe and secure.

When users surf websites that have already been comprised in a blacklist database, the web browsers' security indicator then notifies the user with a warning message indicating that the desired website to be viewed has been identified as a malicious or un-trusted site, and then offers the user the option to continue or to exit the current site. In majority of modern browsers as a means to protect users from malware and/or hosting phishing scams, there is a reputation service provided by Google's safe browsing & Microsoft smart screen stand out as the two most commonly used one. Inevitably in many mobile browsers, the rogue websites have not been protected. In this paper we examine the protection level provided to android based mobiles and as a result. We propose and evaluate an architecture, which can be used to significantly improve the protection of the mobile browsers.

Keywords: Mobile security, Mobile Browsers, SHA 256 Standard, Malwares

INTRODUCTION

Information leakage is one of the major challenges in end to end data exchange. Information misfortune, which implies lost information that happen on any gadget that stores information. It is an issue for anybody that uses a mobile instead of PC.The owner of any organization or business firm having some vital information may need to impart it to third parties. These trusted outsiders may utilize this information for their own particular advantage making reputational and financial harm to the owner‟s organization.

Cell phones are an indispensable piece of our day by day lives. Their utilization is not restricted to operations like telephone calls or content informing. These gadgets are dynamically utilized for applications like managing an account, m-commerce, internet access, entertainment and remote working. Theonly difference between desktop computers and mobile devices in terms of security risk is the challenge to understand the inner workings of the OS on different hardware processor architectures.

Almost every mobile phone today comes with an integrated web browser that can display HTML web pages and execute JavaScript. Almost all major web sites such as news sites, social networks, and shopping sites run websites that are optimized for small displays of mobile phones. Due to the broad use of mobile web access we investigated possible privacy problems of mobile phone web access. We conducted a study where we monitor all HTTP headers sent from mobile phones to our web server. We analyzed the logged data for privacy problems. Through this study we determined that a world wide privacy problem exists when accessing the world wide web from a mobile phone.

The Web is turning out to be more available by convenient, multi-touch remote gadgets. With current development rates, web access from cell phones is probably going to surpass web access from desktop PCs by 2014.It is important to give a solid and simple to utilize strategy for securing these cell phones against unauthorized access and diverse attacks.

RELATEDWORK

Dimitrios Damopoulos focuses on on iPhone device security Which makes a simple malware to be specific iSAM to uncover possible vulnerabilities of current cell phones OS, and show that is relative simple to avoid any security control.The primary aims of a smart malware is to infect the target, self-propagate to other targets and finally connect back to a bot master server.The last activity is highly desirable to update the malwares programming logic by enhancing as of now existed features and

including new ones, or to obey commands and unleash a synchronized attack.The first method is by using iSAMScanner (see next section) which tries to detect jailbroken iPhones having the SSH vulnerability and infects them directly.Future work concentrates on obtaining detailed experimental results e.g. infection and untraceability rates, collector effectiveness etc as well as into modifying iSAM core so as to be able to automatically infect any iOS-based device.[10]

Asaf Shabtai et demonstrate the evaluation framework on two new types of phone virtualization that represent different directions for virtualization that exist in commercial products today and serve as the basis for groups of products: Linux based virtualization and micro kernel based virtualization. Table 2 presents a summary of the comparison between the two virtualization methods. Another product group which provides virtualization like experiences include products which are categorized as general containers but because they don't share a similar design principle or implementation direction, evaluating them as one coherent group will not reflect all of the products' specific details. This evaluation framework can be extended and parts of its criteria substituted with alternative criteria in order to be adapted to different evaluation targets.[1]

RachnaDhamija Analysed website authentication measures that are designed to protect users from man-in-the-middle, 'phishing', and other site forgery attacks.**First, it removes** HTTPS indicators. Next, removes the participant's site-authentication image**.** Finally, replaces the bank's password-entry page with a warning page. It also investigates how a study's design affects participant behavior.[2]

Rahul Shelke et al propose a methodology to evaluate mobile apps based on cloud computing platform and data mining. It also presents a prototype system named AndroidArmour to identify the mobile app's virulence or benignancy. Compared with traditional method, such as permission pattern based method, AndroidArmour combines the dynamic and static analysis methods to comprehensively evaluate an Android app. In the implementation, adopted Android Security Evaluation Framework (ASEF) and Static Android Analysis Framework (SAAF), the two representative dynamic and static analysis methods, to evaluate the Android apps and estimate the total time needed to evaluate all the apps stored in one mobile app market. Evaluation results shows that it is practical to use cloud computing platform and data mining to verify all stored apps routinely to filter out malware apps from mobile app markets. As the future work, AndroidArmour can extensively use machine learning to conduct automotive forensic analysis of mobile apps based on the generated multifaceted data in this stage.[9]

Julie S. Downs et al we first must know how and why people fall for them. This study reports preliminary analysis of interviews with 20 nonexpert computer users to reveal their strategies and understand their decisions when encountering possibly suspicious emails. One of the reasons that people may be vulnerable to phishing schemes is that awareness of the risks is not linked to perceived vulnerability or to useful strategies in identifying phishing emails. Rather, our data suggest that people can manage the risks that they are most familiar with, but don't appear to extrapolate to be wary of unfamiliar risks. We explore several strategies that people use, with varying degrees of success, in evaluating emails and in making sense of warnings offered by browsers attempting to helpusers navigate the web.[5]

Paul C. van Oorschot et al performs the first measurement of the state of critical security indicators in mobile browsers. The goal is not to determine if average users take advantage of such cues, but instead to demonstrate that such indicators are lacking and thus fail to provide sufficient information for even experts. Author created a simple webpage that uses a strong TLS connection to retrieve the top-level resource and embedded a map obtained from a third-party over an unsecured http connection. We rendered this webpage on the candidate browsers and analyzed the browsers for the presence of two basic TLS security indicators: the https URL prefix and the padlock icon. If a browser shows any of these two indicators on a mixed content webpage, it does not follow the W3C guideline.[6]

Neil chou goal is to raise awareness of the web spoofing problem proposed a framework for client-side defense: a browser plug-in that examines web pages and warns the user when requests for data may be part of a spoof attack. A number of tests can be used to distinguish spoof pages from honest pages. We present the tests we implemented and evaluated in three groups: stateless methods that determine whether a downloaded page is suspicious, stateful methods that evaluate a downloaded page in light of previous user activity, and methods that evaluate outgoing html post data.[4]

Joshua Sunshine et al conducted a survey of over 400 Internet users to examine their reactions to and understanding of current SSL warnings. Then later designed two new warnings using warnings science principles and lessons learned from the survey and evaluated warnings used in three popular web browsers and our two warnings in a 100 participant, between-subjects laboratory study. These warnings performed significantly better than existing warnings, but far too many participants exhibited dangerous behavior in all warning conditions. Results suggest that, while warnings can be improved, a better approach may be to minimize the use of SSLwarnings

altogether by blocking users from making unsafe connections and eliminating warnings in benign situations.[8]

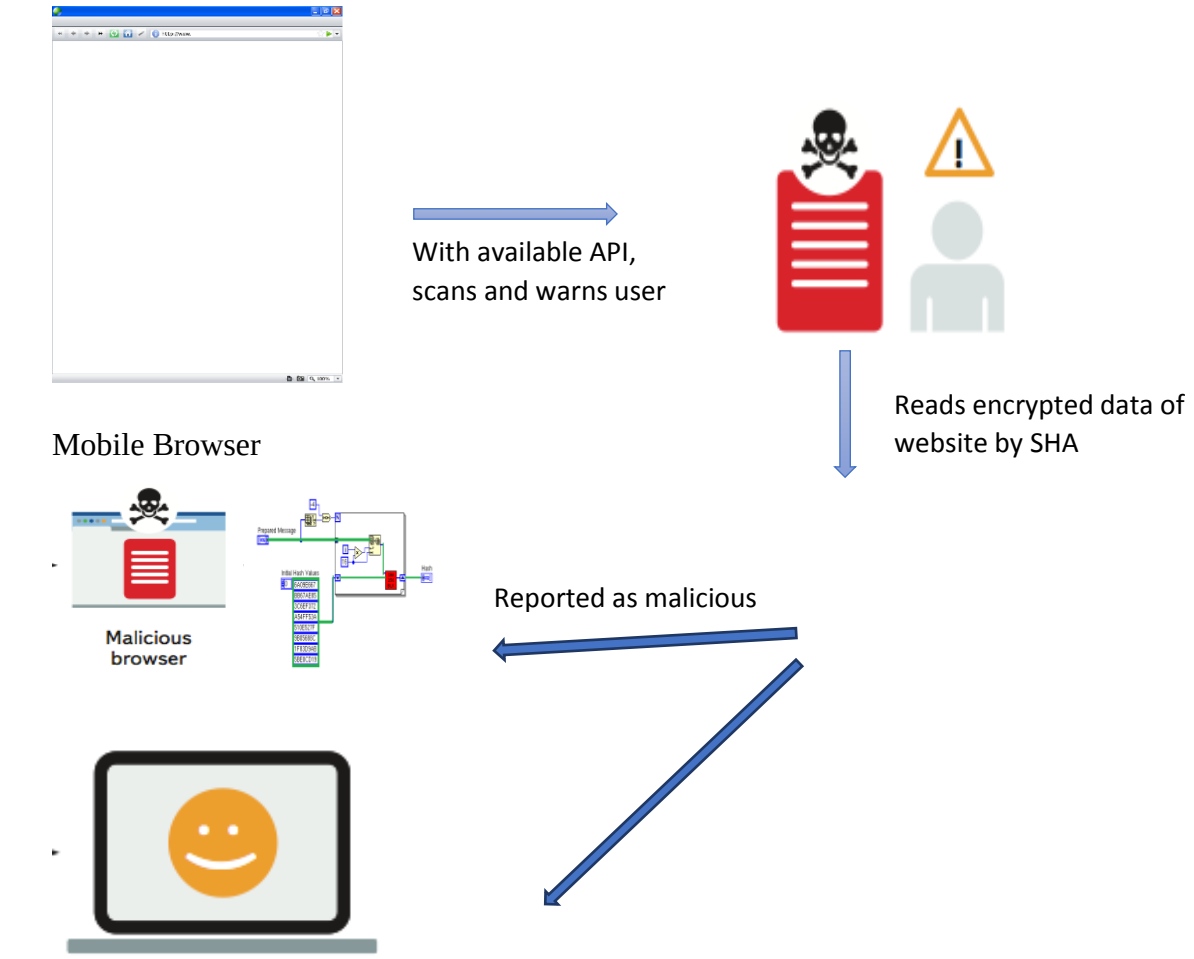
Proposed Work:

Proposed Work involves first stage i.e,Proxy Evaluation which meansSecure proxy to find and focus on malicious sites, It is done by redirecting the site request through our proxy. We have used some scripts which simulates the web requests without using actual browsers. Analysis is done by tracking the total number of blocked URLs and compared them with the results of the browsers. Proxy has been configured in order the downloaded files by using hash and file analysis technique, when the detection results increases as per virustotal api.

The next stage is URL analysis based analysis is done when the URL is sent to the proxy server and getting the response from virus total. For each triggered the average time will be calculated, if the hash was known then without any delay the file or url will be blocked (if the detection is found).If there is no detection then it will be reported. If there is no response for a long time, then it has to be analyzed once again.

Third stage includes Evaluation process that contains hash based analysis. During the collection of multiple blacklists for malicious sites we provide more protection than any individuals. There may be some fails in detection. Those are considered as PE Executables. In this evaluation our secure proxy downloads all the PE executable files and query virustotal for their hashes. Hence it will considered as Hash Based analysis.

The last stage involves File Based Analysis whereany Downloaded files will be uploaded to the proxy server for analysis. Based on the secure proxy it will be reported whether it is malicious or not. Virus total supports all kind of scans. Upon submission of the file the service will query large number suspicious things and checks for any error matches.



Experimental Setup

Fig.1

EXPERIMENTAL SETUP

Phase 1: **Display domain Information**

Enter the URL in the given search box. User will get to know the domain details of the given URL such as IPaddress,domainStatus,IPLocation,Registrar,Registrar Status and Name Servers.

Eg:www.example.com

Phase 2 **: Identify the Url**

Identifying malicious web links with thand identifying the type of attack.It scans the URL and based on the available API's detects whether it is malicious website or a secure website to browse. Before return, it checks whether it is blacklisted or not.

This helps user from malware attacks before it is browsed in mobile, so that user will be aware of malicious activities that is going behind.

Phase **3 : connection check process**

If URI is not backlisted continues with the connection and return the HTTP response (Secure Proxy) .This shows that user can securely browse the website without any trouble.

If the browse is detected as malicious ,then it will show the warning message to user to not to browse or not to go further.

Phase **4 : Implementing SHA 256 standard**

Proxy proceeds and calculates the SHA 256 Hash. Thishash keys are basically used to read encrypted files or unreadable files that are presented in a malicious website .These encrypted file are actually the virus data files that can be read with SHA algorithms and can be help to verify the URL.

SHA-256 transforms an input message into the 256 bits

Following is the SHA 256 Algorithm framework

Step 1: **Message Padding**

Input paired message is added with 1 and padded with O‟s until length = 448 mod 512.The unique message length is then attached as 64-bit twofold number. The padded message's length is a various of 512 bits, which chooses what number of "0" to be padded.

Step 2: M**essage parsing**

The padded message is then parsed into N 512-bit blocks: A(l), (2) … A(N). These A(i) message blocks are passed separately to the message expander.

Step 3: **Message extension**

Each 512 bit block can be divided into 16 32-bit words: A 0 (i), A 1 (i) ….A 15 (i), which are then extended into 64 words labelled W0, W1… W63 under the certain rule prescribed by SHA-2 standard

Step 4: **Message Compression**

The Wt words from Message extension stage are then passed to the SHA compression function. The center uses 8 working factors named A, B,… … ,Z which are then introduced to predefined values Z0 (0) – Z7 (0) toward the begin of each call to the hash function.

TABLE I
Initial Hash Value of SHA-256

A=Z0(0)	6a09e667
B=Z1(0)	bb67ae85
C=Z2(0)	3c6ef372
D=Z3(0)	a54ff53a
E=Z4(0)	510e527f
F=Z5(0)	9b05688c
G=Z6(0)	1f83d9ab
H=Z7(0)	5be0cd19

step5: The algorithm is implemented by 64-cycle iterative computation each block. The eight working variables are labeled A, B, C...Z, which are updating the value during the 64-cycle as follows.

$T2 = Z + \sum 1(E) + Ch(E,F,G)[1] + Kt + Wt$ [1]
$T2 = \sum (A) +) + Maj(A,B,C)$ [2]
$H = G$ [3]
$G = F$ [4]

F = E [5]
E = D + T1 [6]
D = C [7]
C = B [8]
B = A [9]
A = T1 + T2 [10]

step*6*: After 64 iterations of the compression function, an intermediate hash value $H^{(i)}$ is calculated as follows:

Z0^(i) = A + Z0^(i-1) [11]
Z1^(i) = A + Z1^(i-1) [12]
.
.
.
Z7^(i) = A + Z7^(i-1) [13]

The SHA-256 compression algorithm then repeats and begins processing another 512-bit block from the message padder. After all the data blocks have been processed, final 256-bit output Z^N is calculated as follows:-

Z^(N) = Z0^N & H1^N & H2^N &…… Z7^N

Phase 5**: Malicious Report**

If the Hash was known, then it will be reported as Malicious and stops the process. So that user will have a chance to avoid going to malicious website.
If the user encounters malicious website then immediately a warning message will pop out showing “cannot browse”.
Phase 6: **Delivery mode**

If not, it continuous and submit. Deliversto the user by going to the safe website.

RESULTS

Mobile phones have immense public utility, improving communication in social and commercial interactions. Mobile devices are used more than traditional computers for web browsing.
Results show that mobile web browsers have more chance of attacks when compared to desktop. Proper security to operating system as well as to the mobile browser make user browsing secure websites.

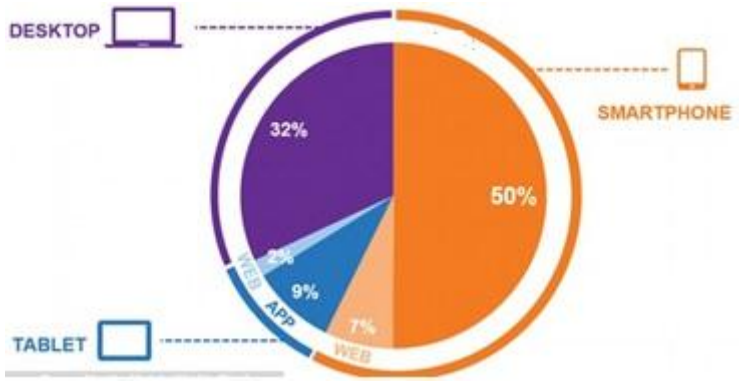


Fig 2: Usage of phone in daily life

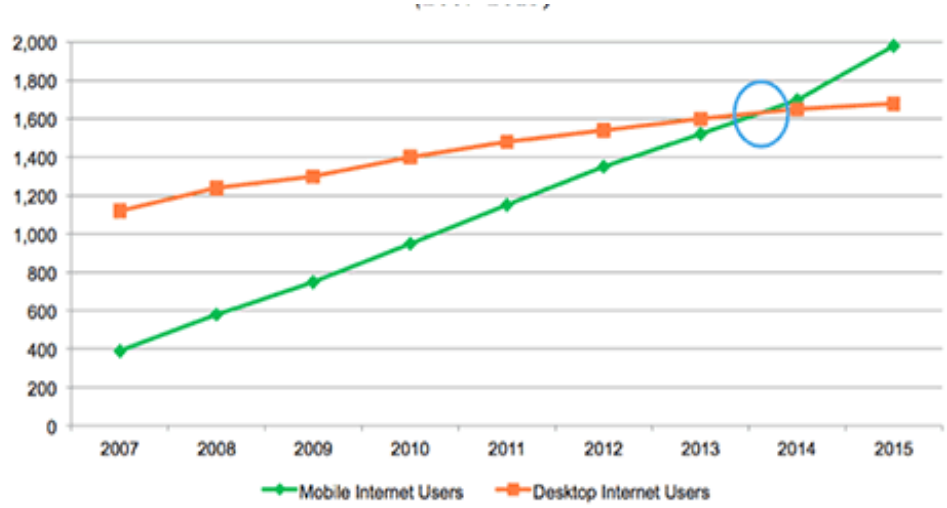


Fig 3: Graph showing usage of mobile browsers to web browsers

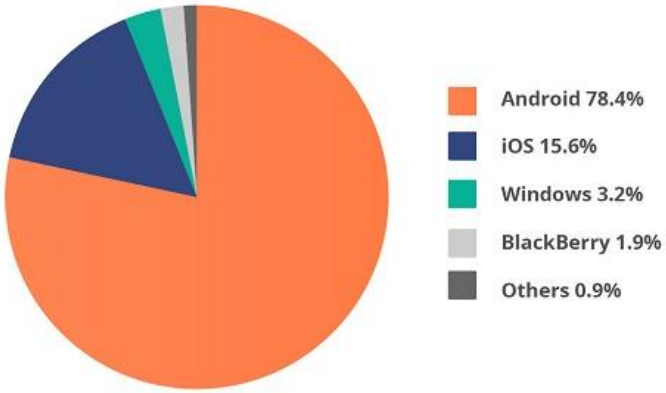


Fig 4: Malware attacks in different devices

The fig shows that android phone are more vulnerable to attacks and chances of visiting to malware/malicious websites every now and then by user .

Fig 4 : Enter Url

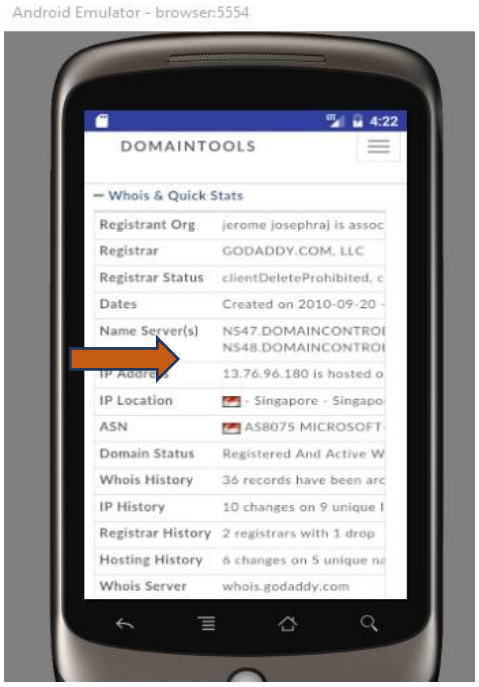
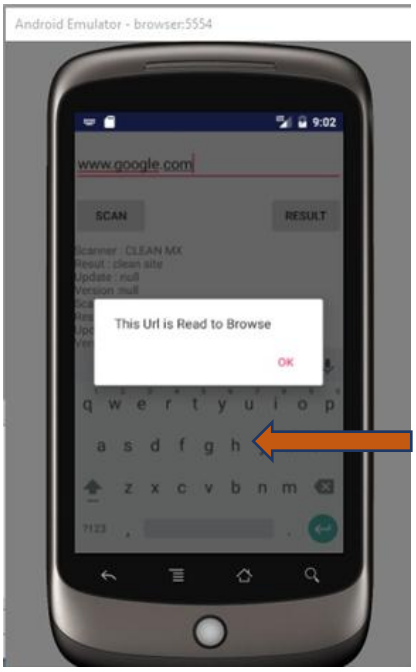


Fig 5 : Domain Information



Url is secure to browse (no malware)

Fig 6 : Secure Url(website)

Fig 7 : Malware affected URL

CONCLUSION

Mobile devices are the major platform for the users to transfer and exchange diverse data for communication. This paper deals with various threats and vulnerabilities that affect the mobile browser and result in damage of mobile device. Since lot of sensitive personal and corporate information, such as login credentials, credit card details, account details, private contact entries, invoices, are being stored or transmitted through these mobile browsers without any proper OS. The growth in the creation and maintenance of secure identities for mobile devices has created challenges for individuals. Mobile browsers fail to meet many of the security guidelines and exhibit tremendous inconsistency in the presentation and availability of SSL indicators in contrast to traditional desktop browsers. Such significant design changes preclude even expert users from discerning clues about the credibility and security of websites, raising serious concerns about the inability of average users to detect security issues. Additionally, we observed that the absence of clear and consistent EV-SSL indications leads to EV-SSL certificates currently adding complexity to the mobile ecosystem without any corresponding benefits. In this paper we examine the protection level provided to android based mobiles and as a result.

We propose and evaluate an architecture, which can be used to significantly improve the protection of the mobile browsers.

REFERENCES

[1] AsafShabtai, Dudu Mimran Yuval Elovici" Evaluation of Security Solutions for Android Systems"

[2] RachnaDhamija, Andy Ozment, Ian Fischer "An evaluation of website authentication and the effect of role playing on usability studies"

[3] ChaitraliAmrutkar , Patrick Traynor and van Oorschot "An Empirical Evaluation of Security Indicators in MobileWeb Browsers"

[4] Neil Chou,Robert Ledesma, Yuka Teraguchi, Dan Boneh,John C. Mitchell" Client-side defense against web-based identity theft"

[5] Julie S. Downs, Mandy B. Holbrook, Mandy B. Holbrook" Decision Strategies and Susceptibility to Phishing"

[6] ChaitraliAmrutkar, Patrick Traynor, and Paul C. van Oorschot" Measuring SSL Indicators on Mobile Browsers:Extended Life, or End of the Road?"

[7] ChaitraliAmrutkar" Towards Secure Web Browsing on Mobile Devices"

[8] Joshua Sunshine, Serge Egelman, HazimAlmuhimedi, Neha Atri," Crying Wolf: An Empirical Study of SSL Warning Effectiveness"

[9] Aditya parashar,nishantpaliwal,Rahulshelke" Cloud Computing Based Forensic Analysis for Mobile Applications Using Data Mining"

[10] DimitriosDamopoulos, Georgios Kambourakis, and StefanosGritzalis"iSAM: An iPhone Stealth Airborne Malware" SEC 2011, IFIP AICT 354, pp. 17–28, 2011.

[11] Senthil Kumar, S. Prabakaran and M. Nirmala : Enhancing Security to mobile browsers by restricting information leakageVolume **:** No.10 (2017) Issue No.**:**11 (2017)