ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 3, March 2015

Categorizing Client Side Scripts Based On Multi Level Data Fetching Monitoring Scheme To Mitigate Phishing Attacks And Restricting Client Scripts

G.Kalaiarasi[1] , Dr.P.Vasudevan [2]
[1] Associate Professor,Dhanalakshi Srinivasan College Of Engineering and Technology, Chennai.
[2] Professor,Department Of Chemical Engineering, Anna University, Chennai.

ABSTRACT: The phishing attacks are the most threatening fact which affects the most online business information and the malicious users steal various sensitive financial and business information by running anonymous client side scripts. Most of the times the user will ignore running scripts and popup which runs set of background process and send some sensitive information to the some of the remote site. To solve this problem, restrict the client side scripts in stealing such sensitive information, there are many approaches which have been discussed but suffers with the problem of identifying such client side scripts in efficient manner. An effective and extended approach is proposed which categorizes the client side scripts according to various factors like the amount of information being transferred by the script, the parent process information and the type of information the script is being accessing.

Keywords: phishing attacks, sensitive information, script, storage

I. INTRODUCTION

The modern world people spend their most of the time in the internet surfing and they perform their most activities through the web. There are malicious nodes or servers which learn the information and these information are most sensitive, personal about a person. There are many malwares which sit on the storage of user systems and send many information to a dedicated malformed server.

In few other situations, there are scripts which are running at the web pages to collect tiny information from the user and send to the server where the web page is available. For example, in ajax kind of web pages, only a part of the web page gets refreshed and there will be only a little amount of data transfer between the server and client side. The user may be visiting some financial banking web pages and does not notify that there are scripts running on the background. What happens is there some malwares which read the sensitive and secret information of the user and send them to the remote site. The process of stealing

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 3, March 2015

such sensitive information is called as phishing attack which is performed mostly with the help of client side scripts which have to be restricted.

Nowadays, there are many advertisements being generated while viewing the web page and each has different purpose. Generally the web user does not care about the advertisements being displayed and they simply ignore the advertisements. If there is any malware presents in the machine then the malware can monitor the web pages being visited and trace the keyboard reading or the web page content. The captured user data could be transferred to another malware controller located somewhere in the world. The captured information can be used to perform variety of threats towards not only financial stability but also against the information stability of the country also.

The client scripts running on the client side can be categorized according to the data what they are fetching and from where they are fetching. Such categorization could help to identify the phishing attacks and stop the client side scripts from stealing the information from the user side.

II. RELATED WORK

There are many approaches which have been discussed for the restriction of client side scripts and few of them are discussed.

Identity-Based Secure Distributed Data Storage Schemes (Jinguang Han et al 2013), proposed two identity-based secure distributed data storage (IBSDDS) schemes. The proposed schemes can capture the following properties: i) The file owner can decide the access permission independently without the help of the private key generator (PKG) ii) For one query, a receiver can only access one file, instead of all files of the owner iii) The proposed schemes are secure against the collusion attacks, namely, even if the receiver can compromise the proxy servers, he cannot obtain the owner's secret key. Although the first scheme is only secure against the chosen plaintext attacks (CPA), the second scheme is secure against the chosen cipher text attacks (CCA). To the best of our knowledge, it is the first IBSDDS schemes where access permissions is made by the owner for an exact file and collusion attacks can be protected in the standard model.

Modeling the Pairwise Key Predistribution Scheme in the Presence of Unreliable Links (Osman Yağan & Armand M. Makowski 2013), present conditions on how to scale the model parameters so that the network i) has no secure node that is isolated and ii) is securely connected, both with high probability, when the number of sensor nodes become large. The results are given in the form of zero-one laws, and exhibit significant differences with corresponding results in the full-visibility case.

NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems (Chun-Jen Chung et al 2013), repose a multi-phase distributed vulnerability detection, measurement, and countermeasure selection mechanism called NICE, which is built on attack graph based analytical models and reconfigurable virtual

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 3, March 2015

network-based countermeasures. The proposed framework leverages Open Flow network programming APIs to build a monitor and control plane over distributed programmable virtual switches in order to significantly improve attack detection and mitigate attack consequences. The system and security evaluations demonstrate the efficiency and effectiveness of the proposed solution.

All the above discussed approaches have the problem of identifying the malicious client side script and do not produce efficient mitigation of phishing attacks.

III. PROPOSED METHODOLOGY

The proposed client side script monitoring mechanism has various stages namely Multi Level Data Fetch Monitoring, Script Classification, and Script Elimination. Each of the functional components are discussed in detail in this section.

3.1 Multi level data fetch monitoring

The multi level data fetched by the client side script is monitored by the proposed method. The method identifies the parent process of the script and it computes the runtime of the client script, then the level of information it accesses is identified, then amount of information being accessed or transferred is computed. The method classifies the information into different categories like system, user, and financial information. The monitored results are stored in the web log trace and will be used to classify the client side script.

3.1.1 Algorithm

Input: Web Log Wl.
Ouput: Client Script Feature Fv
Step1: start
Step2: Identify the parent of the script Pp = Parent(Client script).
Step3: Compute the runtime of script Rt = Cs.StopTime – Cs.StartTime
Step4: Identify the type of information accessed TI = CS.Type$\in \{system, personal, financial\}$
Step5: Compute amount of information accessed IA = $\int \frac{Cs.Transfer}{Time}$
Step6: FV = {Pp, Rt, Tl, IA}.
Step7: stop.

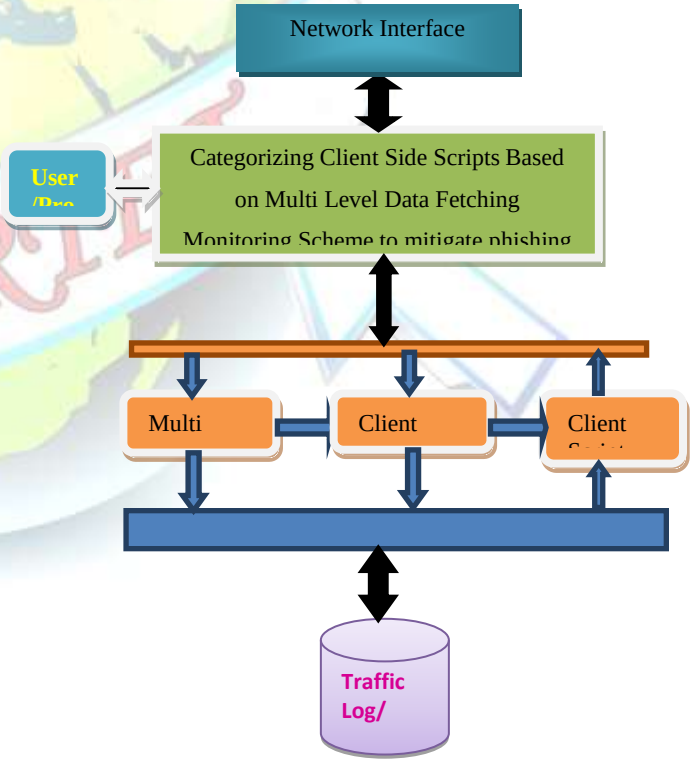

Figure 1. Proposed System Architecture.

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 3, March 2015

3.2 Client script classification

The client script classification is performed based on the features of the client side script monitored. Based on the features of the client side script, three different measures like information security measure, bandwidth security measure and network access measure are computed. Using all these measures, finally we compute the client script trustworthy score using which the script is classified as normal, optimal and dangerous.

3.2.1 Algorithm

Input: Web log Wl, Feature Vector FV.
Output: Class C
Step1: start
Step2: compute bandwidth security measure

$$BSM = \int \frac{\sum_{i=1}^{size(wl)} (Wl(i).Id == Fv.Id).payload}{Fv.payload}$$

Step3: Compute Information security measure ISM =

$$\int \frac{\sum_{i=1}^{size(wl)} (Wl(i).Id == Fv.Id).Type \times \mu}{Fv.Type}$$

μ=0.8 for system information
μ=0.6 for financial information
μ=0.2 for normal information
Step4: compute network access measure

$$NAM = \int \frac{\sum Wl.id == Cs.id}{cs.Time}$$

Step5: compute script trustworthy measure
STM = BSM*ISM*NAM
Step6: Classify scripts using STM.
If STM <= NTh
Assign Normal
If STM >NTH && STM<=Genuine
Assign genuine.
Else
Eliminate Script.
End
Step6: stop.

3.3. Client script elimination

The client script elimination is performed based on trustworthy measure computed for any script which is computed using various factors of the client side script. Based on the measures being computed the client side script is identified as normal, genuine or dangerous. The method computes the script trustworthy measure and classifies the script according to the STM value and assigns a label for that. Based on the label being assigned the client script is controlled.

IV. EXPERIMENTAL RESULT

The proposed multi level data fetch monitoring based client script categorization approach has been implemented and tested for its efficiency and accuracy. The approach has produced good results on restriction accuracy and has produced efficient results with less time complexity.

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 3, March 2015

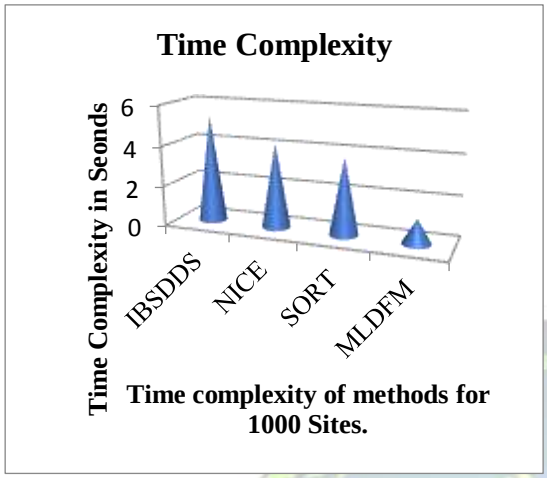

Figure 2. Shows The Time Complexity Of Different Methods For 1000 Sites.

The figure2 shows the time complexity achieved by different methods for 1000 URL's and their log base. It shows that the proposed multi level data fetch monitoring method has produced less time complexity values.

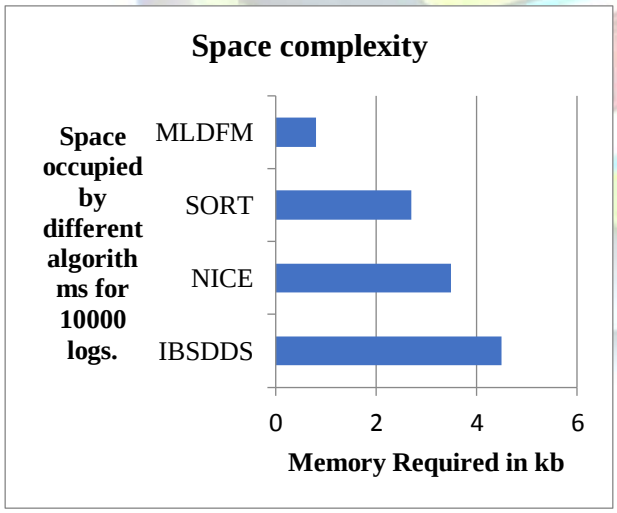

Figure 3. space complexity of different approaches.

The figure3 shows the space complexity achieved by different approaches, and it shows that the proposed approach has taken less memory to process the same set of logs and it shows that it has produced less space complexity than other methods.

CONCLUSION

Multi level data fetch monitoring approach is proposed for client side script restriction and the method computes different measures like information security, bandwidth security, network access measure to compute the trustworthy of the client side script being identified. Based on the trustworthy measure, the script being assigned with a class using which the script is classified. The proposed method has produced efficient results in all the factors of network security. The analysis is performed even for the trusted web sites and scripts by computing the memory access traces performed by the scripts of authorized web sites. The proposed method has produced higher efficient security and better results. Also the proposed method has produced less time and space complexity values.

REFERENCES

[1]. K. J. Houle and G. M. Weaver, "Trends in Denial of Service Attack Technology," CERT Advisory(2001).

[2]. C. P. Pfleeger, Security in Computing, Prentice Hall(1996).

[3]. Jinguang Han, Student Member, IEEE, Willy Susilo, Senior Member, IEEE, and Yi Mu, Senior Member, IEEE-"Identity-Based Secure Distributed Data Storage Schemes"-IEEE TRANSACTIONS ON COMPUTERS (2013).

[4]. Elhadi M. Shakshuki, Senior Member, IEEE, Nan Kang, and Tarek R. Sheltami, Member, IEEE, "EAACK—A Secure Intrusion-Detection System for MANETs", IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS (2013).

All Rights Reserved © 2015 IJARTET

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 2, Issue 3, March 2015

[5]. Osman Yağan, Member, IEEE, and Armand M. Makowski, Fellow, IEEE "Modeling the Pairwise Key Predistribution Scheme in the Presence of Unreliable Links"-IEEE TRANSACTIONS ON INFORMATION THEORY(2013).

[6]. Chun-Jen Chung, Student Member, IEEE, Pankaj Khatkar, Student Member, IEEE, Tianyi Xing, Jeongkeun Lee, Member, IEEE, and Dijiang Huang Senior Member, IEEE-" NICE: Network Intrusion Detection and Countermeasure Selection in Virtual Network Systems"- IEEE TRANSACTIONS ON DEPEDABLE AND SECURE COMPUTING(2013).

[7]. Larry A. Dunning, Member, IEEE, and Ray Kresman- "Privacy Preserving Data Sharing With Anonymous ID Assignment"-IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY(2013).

[8]. Guilin Wang, Jiangshan Yu, and Qi Xie, "Security Analysis of a Single Sign-On Mechanism for Distributed Computer Networks", IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS(2013).

[9]. Ahmet Burak Can, Member, IEEE, and Bharat Bhargava, Fellow, IEEE-"SORT: A Self-ORganizing Trust Model for Peer-to-Peer Systems"- IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING (2013).

[10]. Sangho Lee, Student Member, IEEE, and Jong Kim, Member, IEEE "WARNINGBIRD: A Near Real-time Detection System for Suspicious URLs in Twitter Stream"- IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING(2013.)

[11]. Seda Gurses and Claudia Diaz "Two tales of privacy in online social networks", IEEE Security and Privacy (2013).

[12]. Indrajeet Singh, Michael Butkiewicz, Harsha V. Madhyastha, Srikanth,V. Krishnamurthy, Sateesh Addepalli "Twitsper: Tweeting Privately" IEEE(2013).

[13]. Ngangbam Herojit Singh and, A.Kayalvizhi, M.Tech. "Combining Cryptographic Primitives to Prevent Jamming Attacks in Wireless

All Rights Reserved © 2015 IJARTET