Scientific Journal Impact Factor (SJIF) : 1.711
International Journal of Modern Trends in Engineering and Research
ISSN (ONLINE) : 2349 - 9745
ISSN (PRINT) : 2393 - 8161

Privacy and Security using Traffic padding in web application

Sajeena Salim[1], Sharika T R[2]
[1,2]*Department of Computer Science, IIET, Nellikuzhi*

Abstract- A Web application is a program that can be accessed through a network connection using HTTP. Most web- based applications run inside the Web browser. Web based applications, which can be client-based, but the processing is done over the Internet. In existing work the padding is used to decrease the attack rate of useful information using the single user input. Here we propose a new technique called the splitting method which is used to decreases the attack rate. So, this paper will protect the useful information from hacking. Here, in this paper we design a splitting algorithm as modified algorithm for the experimental results and then finally compare the existing work and the proposed work through the experiments.

Keywords- Attack Rate, Internet, security, Padding, Splitting

I. INTRODUCTION

Almost all the web requests are send to the web server and the response for that request are executed by Hyper Text Transfer Protocol. The web browsers will communicate with the web server through HTTP. Various ways in which the sensitive information will be sent through an insecure network using the symmetric or the asymmetric keys. The traffic padding technique which is used in the PPTP produces the cipher text as output, even when in the absence of the plain text. The random data stream also generated. Whenever the plain text is available for encrypting, it is encrypted and transmitted. Random data can encrypted and transmitted through the network when the absence of plaintext as the input. Many of the random padding techniques are used for protect the useful information from data detection, but the protection is not strong enough. A side-channel attack means that the information which is gained from the physical implementation. There is a similarity between the privacy preserving data publishing and privacy preserving traffic padding issues were considered.

Timing attacks means the attacks based on measuring how much the time varies computations that takes to perform. There is also an efficient derivation of security for the web applications was a main techniques. Whenever the user performs an action on the web based application, this may cause the messages to be exchanged between the server-side and the client-side and the attacker which observes the bursts of network packets that corresponding to each of the web-object[5]. Side-channel attacks also show that the pervasive and the fundamental to most of the web applications due to the various intrinsic characteristics of the web applications, like diverse resource objects, low entropy inputs, and stateful communications. Web application presents the new privacy and security challenges because of the untrusted internet which can carry the continuous interaction between the users and the servers. Many of the web application may also disclose the sensitive data which leads to the security breaches of the user side privacy.

II . RELATED WORKS

Several recent papers had shown that the sensitive information may also often be extracted from the encrypted traffic by patterns in the packets sizes and timing. The main aim of the traffic morphing method is that to provide the users who can encrypt their network data with an efficient technique of preventing the information leakage that induces less overhead than that of padding[10]. Many side

channel attacks faced a serious problem in previous papers. Someone were visited based on the traffic timings and packet sizes, that means, website finger printing in previous paper on traffic analysis shown that it can often possible to identify the website.

The existing system introduces the traffic padding method in single web request. But the protection of the useful information was not strong enough[1]. Many of the security challenge has comes with the popularity of the web based applications has become a serious matter. The protection of the useful data sent back and has become a serious issue. To prevent the information leakages for the encrypted data a browser based technique was proposed [3]. There is many side channel leakages had been a crucial matter in the literature survey. In the previous work the privacy preserving data publishing issue is associated with another privacy preserving traffic padding. Traffic analysis means that the way of inferring sensitive useful information from the communication patterns. Furthermore, many of the recent research work shown that the traffic analysis had applied to the network communications be used to compromise user based privacy and secrecy[12].

The privacy preserved issue has been become a significant attentions in the various domains, like data mining, data publishing, network security, web services, websites, multi-party computation , web applications etc. Many of the side-channel leakages has been the context of web applications in encrypted web traffic have been identified in the literature survey that will allows for profiling the web applications by themselves and also their internal states.

Model

The traffic padding issues have two main perspectives: first one is the interaction between the users and the other one is the observation made by these interactions. Mainly two models are considered that is SVMD and MVMD model.

***SVMD*:** In the SVMD model, only one source and one destination but many of the flow actions can be performed between the source and destination. In SVMD model, there is only one key and the figure 1 shows the SVMD model.

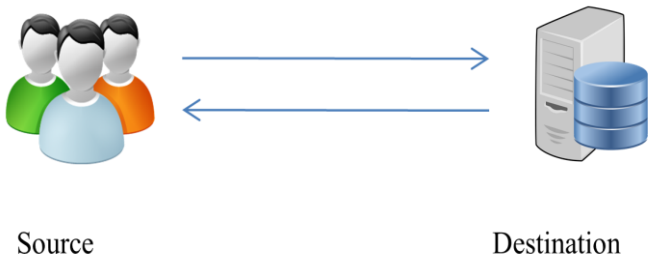

Fig. 1. SVMD

***MVMD*:** In the multi-vector multi-dimension case, there is only one source and but different servers. Here also many of the flow actions can be performed between these client and the servers. Figure 2 shows the MVMD model and those exchanges the different keys for different servers.

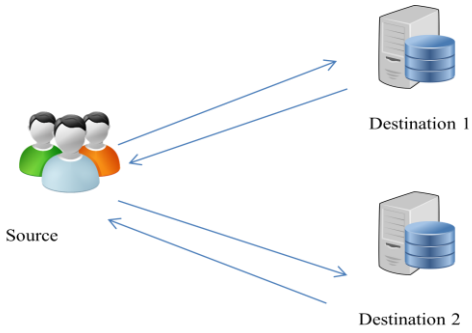

Fig. 2. MVMD

III. PROPOSED WORK

The primary goal of the proposed work is to protect the useful information from the hackers. The problem faced in the previous paper is that the hackers can detect the useful information while using the traffic padding and also there is not enough strong protection. Web applications may also present new privacy and security issues, this is because that the untrusted internet has been most essentially become an integral part of such applications which can carries the continuous interaction between the users and the servers. The figure 3 shows the proposed system architecture. Various popularly web applications may be actually will disclose the highly sensitive useful data, and proportionally leads to some crucial breaches of the secrecy of the user privacy.

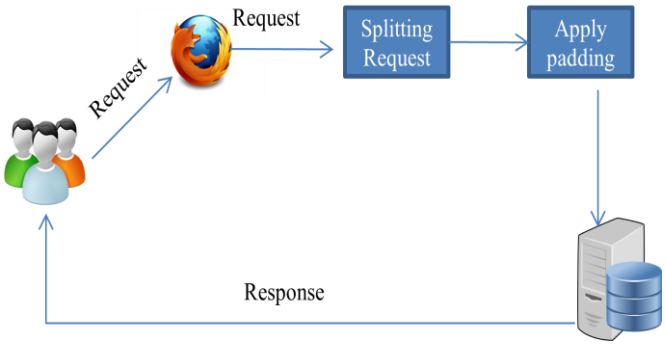

Fig 3. Proposed architecture

This proposed paper is identified as three folded: First fold is the normal method. In the normal phase, the browser sends the request as normal form to the web server. After that the web server receives the web request from the web browser in the normal form. Second fold is the padding technique. In this phase, traffic padding method is used. Traffic padding is that by simply inserting the dummy bits into the gap of a data stream to increase the number packet to protect it from the intruders. A continuous randomized data stream will be generated. Many different methods are used for the padding.

Third method which is used in the proposed work is the split method which one is the main modification of the proposed paper. In this method, whenever the browser sends the web request to the web server, the secret key will be exchanged between the web browser and the server. The split technique will split the incoming web request into multiple parts. The web server will then receive the padded request. After that the web server will report these received requests including the traffic padding. Finally, the web server removes the padding from the original split incoming request and sends back the response.

From various research works we introduced a new technique called split method in this paper to simplify the problem. Along with the new split technique the existing method called traffic padding technique is also used. Split method which means that when the browser sends the web request then the split method divides the incoming request into multiple parts. After splitting, we use the traffic padding method which means that the multiple requests is padded so that the number of packets and the number of bytes will increase. Detection of the useful sensitive information can be protected when the packet size increases. From these sequence of experiments, we compare the normal method, traffic padding and the split method so that the result can found better than the previous work.

Algorithm

Input : No: of Request
Output : packets, bytes

Method

1. Let ‘d’ be the packets size
2. Let ‘b’ be the no: of bytes
3. The web request is send from the browser
   Keys are exchanged
4. If it is a single flow vector, same key k and the action flow set f_1.....f_n;
5. Else
   Different keys
6. Split the incoming request pattern
7. Padding the split request
8. Server receives the padded multiple request.
9. Report the received request including padding.
10. Remove these padding, then send the response.
    Return b
    Return d

From this algorithm the browser before sending the request, exchanging the key between the browser and the server. The browser sends the web request and then split these web request into two different parts. Then pad these split request. Then padded request are send. The web server then reports the entire request. Remove the padding. The web server sends back the response.

IV. RESULTS

In this section, experimental results are the comparison between the normal, traffic padding and the split method. The figure 4 shows the collation with the number of request over number of bytes. Let N be the normal phase, T be the padding and L be the split method. If $N \leq 1000$ which will be lesser number of bytes, $T \geq 1000$ means that the padding method will provide extra bytes than the normal method. L will be thrice than of the normal phase and twice than that of padding method due to the multifarious part of requests.

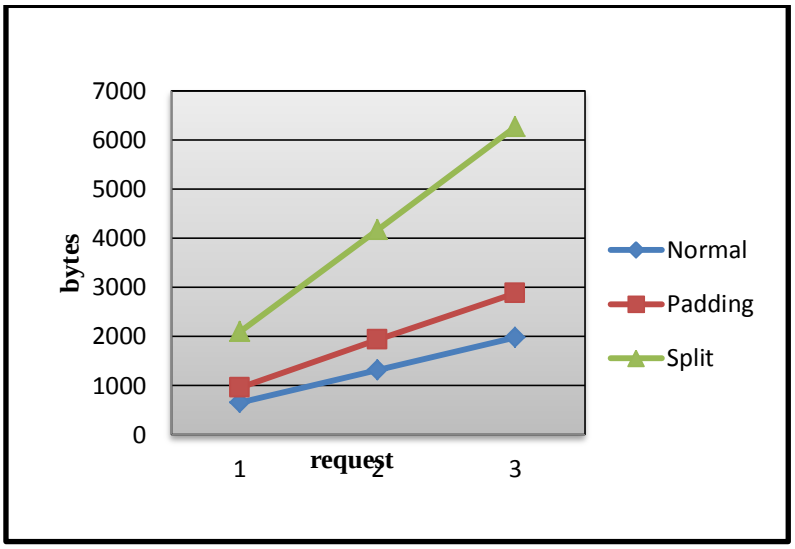

Fig 4. comparison of requests over bytes

Figure 5 shows that the various request over the number of packets. If N ≤ 5 then that is the normal method, if t ≥ 5 then that is the traffic padding technique. When it is the split method, then L will provide more packets than the P. From these two collations, the performance of the speculative result is better than the previous papers. One of the main advantage of this paper work is that protection is strong enough than the previous work due to the number of packets and the number of bytes increases.

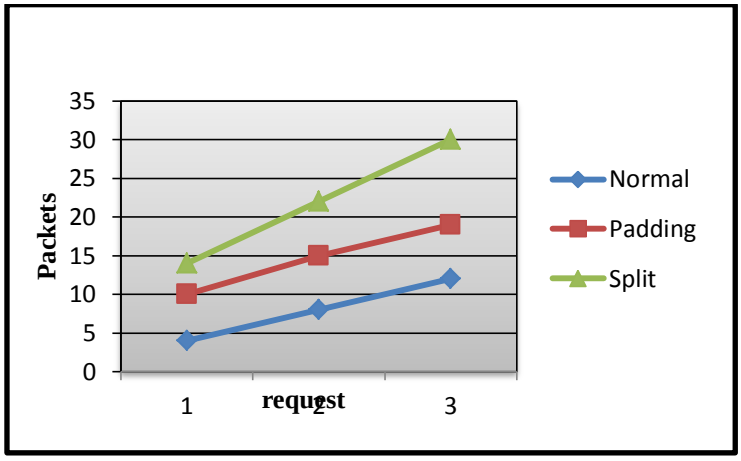

Fig 5. comparison of requests over packets

V. CONCLUSION

Web based applications always face various privacy and the security pitfalls. Numerous traffic padding techniques were used in previous papers but it does not yield a powerful enough protection. This paper presents a new technique with the previous traffic padding for the security issue. This will be applicable in web security, web services, and web based applications and so on. We also develop an algorithm for the experimental results. From the result, we can securely protect the useful information from hackers.

REFERENCES

[1] Wen Ming Liu, Lingyu Wang, Pengsu Cheng, Kui Ren, Senior Member, IEEE,Shunzhi Zhu, and Mourad Debbabi," PPTP: Privacy-Preserving Traffic Paddingin Web-Based Applications", IEEE trans. On dependable and secure computing, vol. 11, no.6, Nov/Dec 2014

[2] P. Chapman and D. Evans, "Automated Black-Box Detection of Side-Channel Vulnerabilities in Web Applications," Proc. 18th ACM Conf. Computer and Comm. Security (CCS '11), pp. 263-274, 2011.
[3] X. Luo, P. Zhou, E.W.W. Chan, W. Lee, R.K.C. Chang, and R. Perdisci,"HTTPOS: Sealing Information Leaks with Browser-Side Obfuscation of Encrypted Flows," Proc. Network and Distributed System Security Symp. (NDSS '11), 2011.
[4] A. Askarov, D. Zhang, and A.C. Myers, "Predictive Black-Box Mitigation of Timing Channels," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 297-307, 2010.
[5] M. Backes, G. Doychev, and B. Kopf, "Preventing Side-Channel Leaks in Web Traffic: A Formal Approach," Proc. 20th Network and Distributed Systems Security Symp. (NDSS '13), 2013.
[6] C. Castelluccia, E. De Cristofaro, and D. Perito, "Private Information Disclosure from Web Searches," Proc. 10th Int'l Conf. Privacy Enhancing Technologies (PETS '10), pp. 38-55, 2010.
[7] K. Zhang, Z. Li, R. Wang, X. Wang, and S. Chen, "Sidebuster:Automated Detection and Quantification of Side-Channel Leaks in Web Application Development," Proc. 17th ACM Conf. Computer and Comm. Security (CCS '10), pp. 595-606, 2010.
[8] M. Backes, G. Doychev, M. Durmuth, and B. Kopf, "Speaker Recognitionin Encrypted Voice Streams," Proc. 15th European Conf. Research in Computer Security (ESORICS '10, pp. 508-523, 2010.
[9] L. Sweeney, "K-Anonymity: A Model for Protecting Privacy," Int'l J. Uncertainty, Fuzziness and Knowledge-Based Systems, vol. 10, no. 5, pp. 557-570, 2002.
[10] C.V. Wright, S.E. Coull, and F. Monrose, "Traffic Morphing: An Efficient Defense Against Statistical Traffic Analysis," Proc. Network and Distributed System Security Symp. (NDSS '09), 2009.

.