Review Paper on
The Countering the DOS or the XDOS Attack for Securing the Web Services

Mahesh Maurya
Asst Prof. Computer science Department
M.P.S.T.M.E., NMIMS University
Ville Parle, Mumbai, India

Amit Vinayakrao Angaitkar
M-tech Student, Computer Science Department
M. P. S. T.M. E., NMIMS University
Ville Parle, Mumbai, India

Abstract

In this decade the use of web services consist of different and interacting technologies and application in all field like defense, banking, transportation, marketing, finance. In such a case web technology play a important role to every field, it becomes main important part of today's communication world. But the web services get vulnerable to the attack like Denial of services (DOS) or XML denial of services (XDOS) attack which hamper web services by crashing the service provider and its services. So for curbing such activity, there are some practices that newly introducing like traceback architecture, framework, grid, authentication and the validation. Service such as services hub and verifier which acting as a mediator in between the client and the service provider which avoided direct communication between client and the server, so that tracing of IP address can't be done. The proposed system which is traceback architecture detects the IP address of the attacker so that system comes to know address of it and accordingly system block particular IP requests.

Keywords – *XDOS , XML , SOAP , SOTA , X-Detector , DPM., N.M. –Normal mode , Attack mode, DPM Deterministic packet marketing , PPM probability packet marketing.*

1. Introduction

Nowadays Internet has been a part of life for day to day activities, because it provides many important services in business, commercial and house hold applications. The Internet usage has been increased the ratio in exponential manner, users and systems been used, had been increased the same ratio, etc. from millions to billions. There is vast necessity of providing security to users of the Internet about their information and service provider, who providing service to the user for their request. An interruption of service provided by Internet causes inconvience to users. These interruption activities are due to Distributed denial of service (DDOS) \ XML denial of service (XDOS) attacks which done by the attacker for the material gain access or popularity or personal reasons .

DOS attacks can be done from either a single source or multiple sources. Denial-of-service (DOS) attacks commonly overwhelm their victims by sending a vast amount of packets from multiple sources like attack sites. As a result the victim spends its key resources to processing the attack packets so that legitimate clients cannot get the service. During very large attacks, DOS traffic also creates a heavy congestion in the Internet core which disrupts communication between all Internet users whose packets cross congested routers. [11].We services are spread all over the world, such web services built in the XML which is largely accepted because of its extensibility and simplicity. Since it is simple it is vulnerable to all attacks.

Web services are built on the SOAP protocol that represents data in XML format, XDOS is another technique used by the attackers to launch attacks against service providers. An XDOS attack will exhaust the system resources of the server hosting a web service when the server processes SOAP messages.

XDOS attack(s), according to Padmanabhuni [15]et al, Jenson et. al. and Chonka et. al. can affect the following area:
Firstly, a network can be flooded with XML messages (instead of packets), in order to prevent legitimate users to network communication.
Secondly, if the attacker floods the web server with XML requests, it will affect the availability of these web services.
Lastly, attackers manipulate the message content, so that the result web server gets crash.

An XDOS attack mainly uses three strategies

2.Strategies

2.1. Oversized payload -

The amount time that require to process the message which come from the client side to the server that is depend upon the size of the request message . In oversized payloads attack, an attacker sends an excessively large payload message to deplete the victim's system resources.

2.2. External entity references

The size of a SOAP message affects the amount of time needed to process the message. In oversized payloads attack, an attacker sends an excessively large payload to deplete the victim's system resources. A SOAP message contains references to external entities (e.g. an XML file residing on a different server). These references are substituted with the actual contents when the SOAP message is processed. An attacker can send a SOAP message containing a large amount of references to external entities to force the service provider to (a) open a large number of TCP connections to download the actual contents of the entities and (b) use a large amount of CPU cycles to process the downloaded contents.

2.3. Entity expansion

In entity expansion attacks, an attacker defines a deeply nested structure to represent the value of an entity. This could force the server to use an exponential amount of memory to hold the value of the entity when the server expands the entity according to the definition of the entity [5].

In all the attacks attacker must do one thing most carefully he hide its identity by spoofing or he used zombies for the attacks towards the victims.

I find out the researchers avoiding the direct communication between the client and service provider by using firewall. Authors of papers[1][9][4][3] many proposed techniques which I have studied, on the basis of that this review paper is written . This paper divide in the section first discus some propose techniques and its working and then performance evaluation and then the comparison measure

3 Methods

3.1The Scheme

The scheme of this technique hiding location of the web service provider from client or public. Because the client does not know the location of the service provider then the attacker can’t able to exhaust the system. For this purpose operation provider subscribe service hub. The service hub act as mediator between client and the server .There are two modes which are as follows.

3.1.1 Normal mode

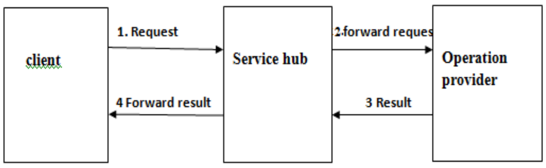

Fig: 1 Normal mode

In the normal mode client send request to the service hub then such request send to the operation provider. Service hub sends the request to the operation provider who processes the request, and then result sends back to the service hub. At last the service hub sends result to the client.

3.1.2. Attack mode

In the attack mode there is need of verification and the validation for such case, service hub subscribe the new system which do work of verification and validation called as verifier .

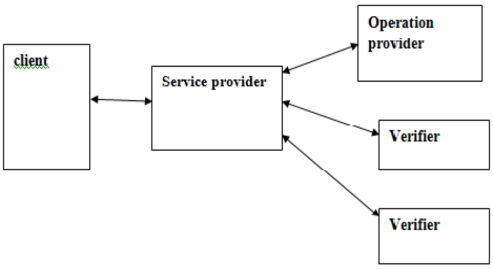

Fig: 2 Attack mode

Here verifier plays the vital role to avoid the XDOS attack or the DDOS attack. It checks every request authenticity by symmetric key algorithm and X.509 certificate

In the under-attack mode, the service requests need to be authenticated and validated before being processed. After successfully authenticated and validated the operations provider only processes a service request. So that the result is, the service provider does not waste system resources to process the attacker’s requests. But for the authentication and validation mechanism also require system resources. By sending large no of message in the form request an attacker can still deplete the victim’s system resources and force the victim to authenticate and validate[1].To avoiding such attacks service provider subscribe new system for authentication and validating. Coming request towards the service provider, that are all authentication and validation done by subscribing service called as verifier. So that verifiers do the authentication of request so that attacker can’t able to exhaust operation provider system. Operation provider and verifier provide service through the service hub which act as mediator. Only the service hub knows the IP address of the operation provider and verifier and service hub responsible for the exchanging the message . Hence attacker can’t sends message directly to the service provider .

3.2. SOAP Serialization and Deserialization

In this proposed architecture, describe process on SOAP message. When sends a request to the web service then request is serialized into a SOAP message and sent over the network. On reaching the server side, this SOAP message is deserialized and the web service reads the request from the client. Depending on the client request, web service performs required operations and generates responses. This response is serialized into SOAP message at the server and deserialized at the client side. Similarly, the SOAP message is serialized at the server and deserialized at the client side when the response is sent from the server to the client. Thus the SOAP message goes through a process of serialization and deserialization both at the client and the server side. With the help of this architecture operation provider can avoid the XDOS attack.

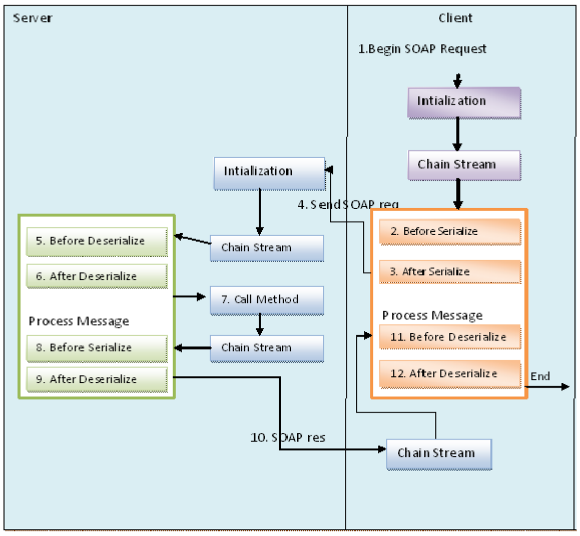

Fig: 5 SOAP serialization and Deserialization

3.3. SOTA Framework

The main objective of Service-Oriented Traceback Architecture (SOTA) is to apply a SOA approach to traceback methodology, so that the true source of a DDOS or XDOS attack can be identify . SOTA is based upon a popular form of packet marking called Deterministic Packet Marking (DPM) [16]. DPM is a packet marking algorithm that marks the ID field and reserved flag within the IP header [16]. As each incoming packet enters an edge ingress router it is marked, outgoing packets are usually ignored. The marked packets will remain unchanged for as long as the packet traverses the network. Authors proposed, in a SOTA framework, to employ some of the DPM methodology by placing our own Service-Oriented Traceback Mark (SOTM) within a web service message. If current web security services are being employed already, SOTM will replace the ‘token’ that contains the client identification with its own. The SOTM tag contains the real source identification, which is afterward placed inside the SOAP message, as the message enters the edge router. This tag will not change throughout the network as it traverse all over the network. With this SOTM tag, the victim will detect DOS attack and then such thing

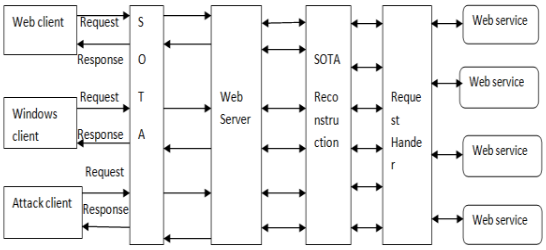

Fig: 3 SOTA Framework

After placing SOTM tag within the SOAP header. As a result, all service requests are first sent to SOTA for marking. Some of the consequence of placing SOTA before the web server are, this proposed technique effectively remove the service providers address and prevent a direct attack.

3.4. Grid web service Architecture

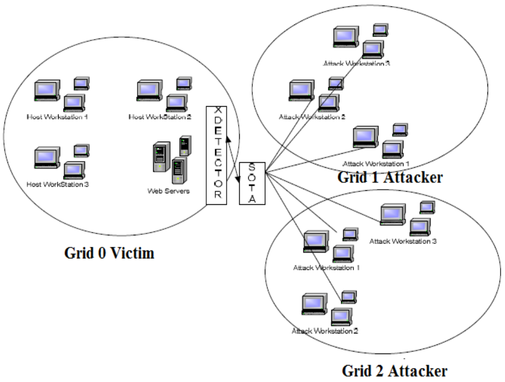

Fig: 4 Grid web service

SOTA does not directly remove a XDoS or DXDOS attack message. This work is left for the filter section of a defense system ie XDetector. SOTA's have two main objectives of XDOS, which are as follows :

Firstly exploit a known vulnerability, in order to bring down system. These vulnerabilities could be found in communication channels (flooding for example) or known exploits within the services provided (for example, an attacker can Overload their messages which will result in the web server crashing).
The second objective is that attackers try to hide their identity. The reasons vary, depending on what type of attack, but usually it is to cover their crime or to bypass a known defense that is in place to prevent it. It is with this second objective that SOTA attempts to cover, a other traceback methods, like Probability Packet Marking (PPM) [3] and DPM [16] .

4. Comparison measure

In the comparison part mostly techniques on the different part of the system, attackers is at the one end and service provider at the one end . In between these two there is firewall like service hub and the SOTA framework and X-Detector and Strategies which are responsible for the curbing the DOS and XDOS attack . The following comparison table shows that each methods using its own strategy and technique to minimize DOS attack And detect it .

Functions Methods	Technique use	Work as	Authenticity Checking techniques	limitation
Scheme	Normal mode & Attacking mode	It act as a mediator between client and service provider	X.509 certificate And symmetric key algorithm	N.M. does not work in the attack and In A.M. service may crash
Serialization and deserialsation	Encryption and decryption	Operational response	-	It time consuming technique
SOTA framework	DPM and SOTM	firewall	SOTM tag	Tag have to set on SOAP message
Grid web service architecture	X-Detector	Detection of the attacker IP address	-	-

5. Conclusion and future work

By adopting the existing technique which help in the detection and the curbing the DOS or the XDOS attack, any network becomes robust against the DOS attack. So we can protect the web application from the XDOS attacks.

In Future work all the techniques are simultaneous implemented the certain system then system become invulnerable to the any such attack. We can see following framework diagram which shows all techniques are implemented in this framework. So that system become robust.

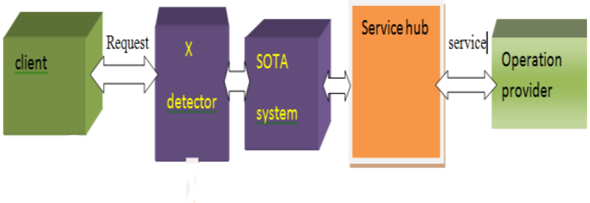

Fig:5 Future framework

5.1 Sequence Diagram

The following sequence diagram showing the exact work flow of the system which is in the future frame work .

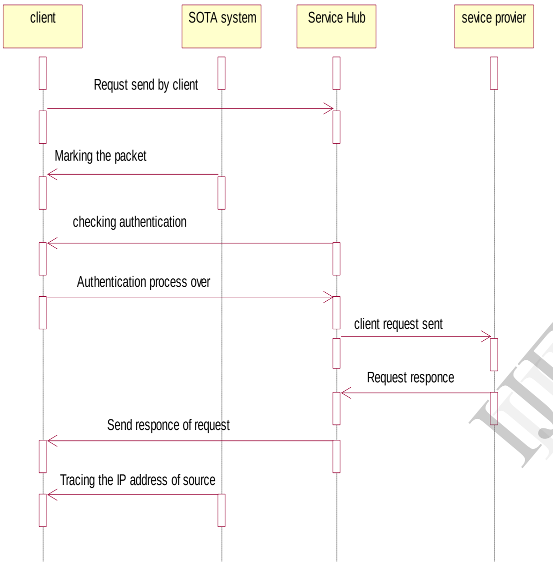

Fig:6 Sequence diagram

6. References

[1]Xinfeng “Countering DDoS and XDoS Attacks against Web Services”, Department of Computer Science, Auckland University, New Zealand

[2] “Ashley Chonka, Wanlei Zhou, Yang Xiang “,Protecting Web Services with Service Oriented Traceback Architecture” Proceedings of IEEE 8th International Conference on Computer and Information Technology, IEEE, Piscataway, N.J., pp. 706-711.!

[3] Ashley Chonka, Wanlei Zhou, Yang Xiang ” Defending Grid Web Services from XDoS Attacks by SOTA”, Seventh Annual IEEE International Conference on Pervasive Computing and Communications, IEEE Computer Society 2009

[4] A. Karthigeyan, C. Andavar, A.Jaya Ramya, June-2012., ” Adaptable Practices for Curbing XDoS Attacks”, International Journal of Scientific & Engineering Research Volume 3, Issue 6,

[5] S.Igni Sabasti Prabu , Dr. V.Jawahar Senthil Kumar, Apr-May 2013 ”Countering the DDoS Attacks for a Secured Web Service ”, Indian Journal of Computer Science and Engineering (IJCSE) l. 4 No.2.

[6] Monika Sachdeva, GurvinderSingh, Kuldip Singh,” A Distributed Approach to Defend Web Service from DDoS Attacks”, International Journal of Computer Science and Security (IJCSS), Volume (5) : Issue (3) : 2011

[7] A.madhuri, A.ramana lakshmi,” Attack patterns for detecting and preventing ddos and replay attacks”, international journal of engineering and technology
vol. 2(9), 2010

[8] Trostle, J, (2006), ‘Protecting Against Distributed Denial of Service (DDoS) Attacks Using Distributed Filtering’, Securecomm and Workshops, 2006 Aug. 28 2006-Sept. 1 2006

[9] Chonka,A., Zhou, W., and Xiang, Y., (2008), "Protecting Web Services with Service Oriented Traceback Architecture", IEEE 8th International Conference on Computer and Information Technology, IEEE, 2008

[10] Padmanabhuni, S.; Singh, V.; Senthil kumar, K.M.; Chatterjee,A.Web Services, 2006, “Preventing Service Oriented Denial of Service (PreSODoS): A Proposed Approach”, ICWS apos;06. International Conference on Volume , Issue , Sept. 2006

[11] Aleksandar Lazarević ,Jaideep Srivastava, Vipin Kumar “DATA MINING FOR INTRUSION DETECTION” Pacific-Asia Conference on Knowledge Discovery in Databases 2003

[12] Y. Huang, J.M. Pullen, “Countering Denial of Service attacks using congestion triggered packet sampling and filtering”, in: Proceedings of the 10th International Conference on Computer Communiations and Networks, 2001.

[13] Nisha H. Bhandari “ Survey on DDoS Attacks and its Detection & Defence Approaches” International Journal of Science and Modern Engineering (IJISME) ISSN: 2319-6386, Volume-1, Issue-3, February 2013

[14] Christos Douligeris , Aikaterini Mitrokotsa “DDoS attacks and defense mechanisms: classificationand state-of-the-art” Department of Informatics, University of Piraeus, 80 Karaoli and Dimitriou Str, Piraeus 18534, Greece Received 9 October 2003; accepted 13 October 2003 Responsible Editor: I.F. Akyildiz

[15] Padmanabhuni, S.; Singh, V.; Senthil kumar, K.M.; Chatterjee,A.Web Services, 2006, “*Preventing Service Oriented Denial of Service (PreSODoS): A Proposed Approach***”,** ICWS apos;06. International Conference on Volume , Issue , Sept. 2006 Page(s):577 – 584

[16] Belenky, A.,and Ansari, N., ‘Tracing Multiple Attackers with Deterministic Packet Marking (DPM)’, Proc. of IEEE Pacific RimConference on Communications, Computers and Signal Processing