ISSN:0975-9646

The Countering the XDoS Attack for Securing the Web Services

Amit Vinayakrao Angaitkar
Computer Department
MPSTME, NMIMS University
Ville Parle, Mumbai, India

Narendra Shekokar
Computer *Department DJSCOE,*
Mumbai University
Ville Parle, Mumbai, India

Mahesh Maurya
Computer Department
MPSTME, NMIMS University
Ville Parle, Mumbai, India

Abstract-In this decade the use of web services consist of different interacting technologies and application in all field like defense, banking, transportation, marketing, finance. In such a case web technology play a important role in every field, it becomes very 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 attack, there are some techniques that are newly introducing like traceback architecture, framework, grid, authentication and the validation. In addition to this existing system mediator between client and service provider, which prevent direct communication between them. Result of this tracing the exact location of the service provider is not possible. The proposed system suggest simultaneous verification /validation and traceback architecture.

Keywords – xdos, soap , sota , x-detector , dpm.

1. INTRODUCTION

Nowadays Internet has been a part of life for day to day activities, because it provides many important services in business, finance, commercial ,educational, hospitality, retail , entertainment and telecommunication . 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 which provided by service provider, it causes inconvience to users. These interruption activities are due to Denial of service (DoS) \ XML denial of service (XDoS) attacks which done by the attacker for the material gain access or popularity or personal reasons .

XDoS attacks can be done from either a single source or multiple sources. XDoS attacks commonly overwhelm their victims by sending a vast amount of request 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].Web 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.

The researcher finding that XDoS attack in the following pattern

- 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.
- Thirdly, attackers manipulate the message content, so that the result web server gets crash.

An XDOS attack mainly uses three strategies

During review it has been observed that the client communicating with the service provider via mediator.This mediator is hiding the server details from outside world. review paper is write and give comparison measure of the techniques . This paper divide in the section first discus introductory part andthen second section in that strategies to overcome the attack . Third section discus the methods for detecting the XDos attack fourth section gives the comparison measure which based on the analysis of existing defense techniques. Fifth section is discus the proposed technique which overcome anomaly of existing system. Last section for the conclusion and the future work

2. STRATEGIES

To overcome the problem of the dos attack, there are some strategies which are taken from the reference papers all are discus in this section.

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.

3.METHODS FOR DETECTION OF DOS ATTACK

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 by sending large amount of request towards service provider. For this purpose operation provider subscribe service hub. The service-hub act as a mediator between client and the service provider. There are two modes which are as follows.

3.1.1 Normal mode

In the normal mode firstly client send request to the service hub, then this request send to the operation provider. Request which are coming from the service hub get process by the service provider. After giving the response to the request, it sends back to service hub. The service hub sends response of request to the client .The architectural diagram 2 shows service hub act as mediator between the service provider and the client .

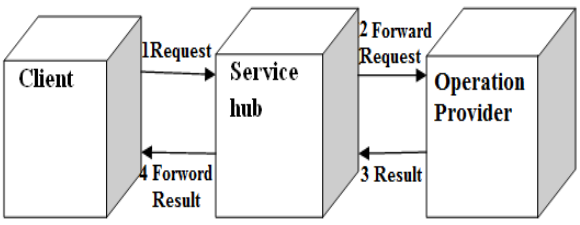

Fig 1: Normal mode

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 .

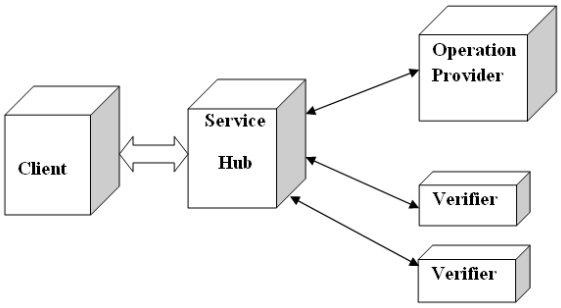

Fig 2: Attack mode

By using the verifier authenticity of the client can be check so that legitimacy of the client is checking in this process. Here verifier plays the vital role to avoid the XDOS attack. It checks every request authenticity by symmetric key algorithm and X.509 certificate

In 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. 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]. For the purpose of authentication and validation mechanism also require system resources. To avoiding such attacks service provider subscribe new system resources for authentication and validating called as verifier . Verifier checks the every request which are coming towards the service provider, that are all authentication and validation done by subscribing new service by service hub . So that verifiers do the authentication of request and result attacker can't able to exhaust operation provider system by sending large amount xml message. Operation provider and verifier provide service through the service hub which acts 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

The author of paper [4] proposed architecture, describe process on SOAP message. When sends a request to the web service then request is serialized into a SOAP message at client side and sent over the network. On reaching the server side, this SOAP message is deserialized and the web service reads the request which are coming 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.

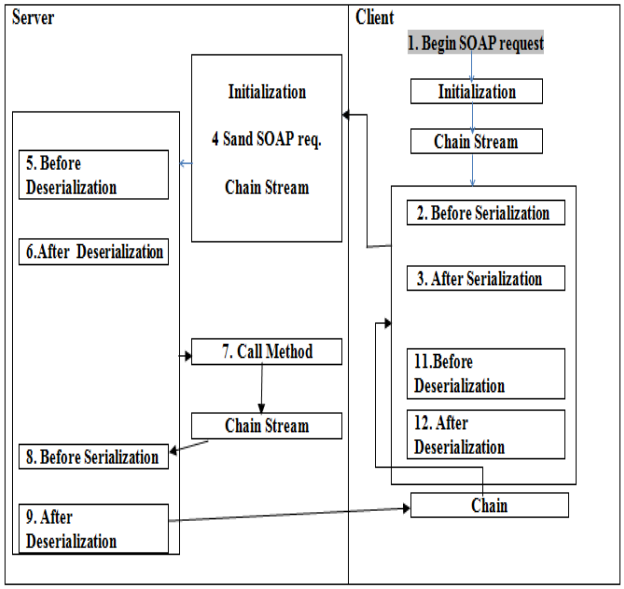

Fig 3 :SOAP serialization and Deserialization

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 following architecture flow diagram , we can understand actual sequence of the serialization and the deserializaion of the SOAP message .When the SOAP request come from the client then operation provider or server deserialize it , and give the response in the SOAP message so the result is avoiding the XDOS attack. In this way the web services attack can be curb.

3.3. SOTA Framework

The another one technique of author of paper [9] for securing the web services name SOTA Service oriented traceback architecture. Main objective of SOTA Architecture is to apply a SOA approach to traceback methodology, so that the true source of a 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 technique 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 which contains the exact source identification, which is then placed inside the SOAP message, after entering message in 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 .

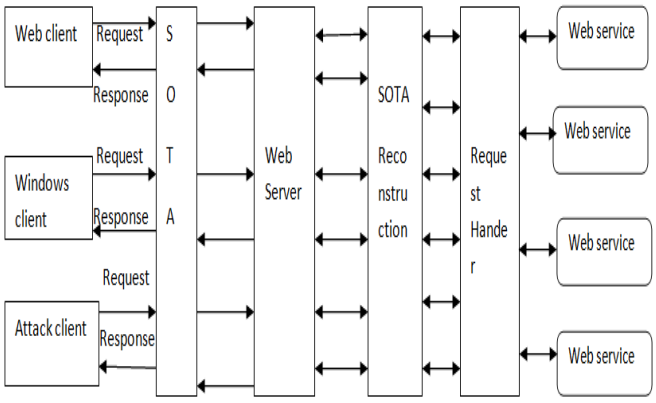

Fig 4: SOTA Framework

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 [9].In the above framework depict the how SOTA is work . When attack is going on , then attack client will request a web service from SOTA, which in turn will pass the request to the web server as shown above framework . The attack client will then formulate a SOAP request message based on the service description formulated by WSDL [9].

Upon receipt of SOAP request message, SOTA will place a SOTM within the header .When the SOTM tag has been placed, then SOAP message will be sent to the Web Server. To discovery of an attack, the victim will ask SOTA reconstruction to extract the mark and inform them of the message origins and then it begins to filter out the attack traffic.

3.4. Grid web service architecture

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.

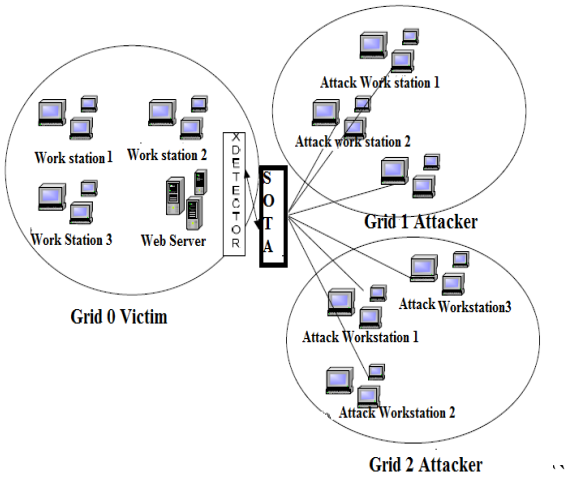

Fig 5: Grid web service

XDetector is the firewall which filter out the attack which tracing out by SOTA by using PPM method. The exact origin or IP address of the packet from which it is coming with the token system can be find out.

SOTA system has two objective

- Firstly finding a known vulnerability, that are responsible for bring down system. These vulnerabilities could be found in communication channels like flooding , or 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 may be different. But it depending on what type of attack is going on ,
  By using a other traceback methods, like Probability Packet Marking (PPM) [3] and Deterministic packet marketing (DPM) [16] .find out the origin of the attack.

4. COMPARISON MEASURE

By analyzing the various architecture of technique to secure web services , we compare this techniques . 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 .

Table1.Comparison of techniques

Function / Methods	Technique used	Work as	Authenticity Checking techniques	Limitation
Scheme	Normal mode And Attacking mode	It act as a mediator between the client and the service provider	X-509 certificate and symmetric key algorithm	N.M. does not Work in the attack and In A.M. service hub may crash
Serialization and Deserialization	Encryption and Decryption	Operational Response	-	It time consuming Technique
SOTA Framework	DPM and SOTM tagging	firewall	SOTM tag	Tag have to set on SOAP message
Grid web service Architecture	X-Detector	Detection of attacker's IP Address	-	-

5. PROPOSED ARCHITECTURE

The above discus comparison motivate us, on the basis of existing technique proposed new architecture for securing the web services . If the system have hybrid technique to defend XDoS attack which will become more robust than existing techniques.

In the following proposed diagram in between client and service provider XDetector , SOTA system and service hub is present .In the SOTA system and XDetetor there is no verification and validation done of authenticate client which are genuine user . So in such case proposed framework will become robust for any high XDoS attack.

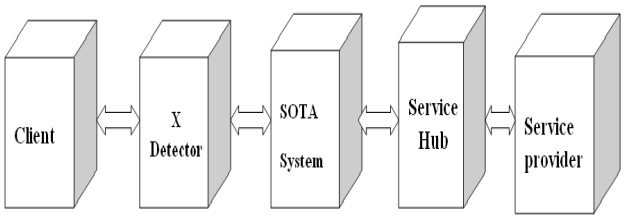

Fig 6: Proposed technique

The proper working of the this framework we can see in the sequence diagram in that it depict that first client sent the request to the service provider

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

- Request send by client to service provider
- Request packet check authenticity and validate at service hub
- That packet get SOTM mark
- If the client get authenticate then request get process by service provider
- Then by PPM back tracking check the exact location of the address client
- Response coming from the service provider sends back to the client through the service provider
- If validation fails then drop the packet from which source it coming

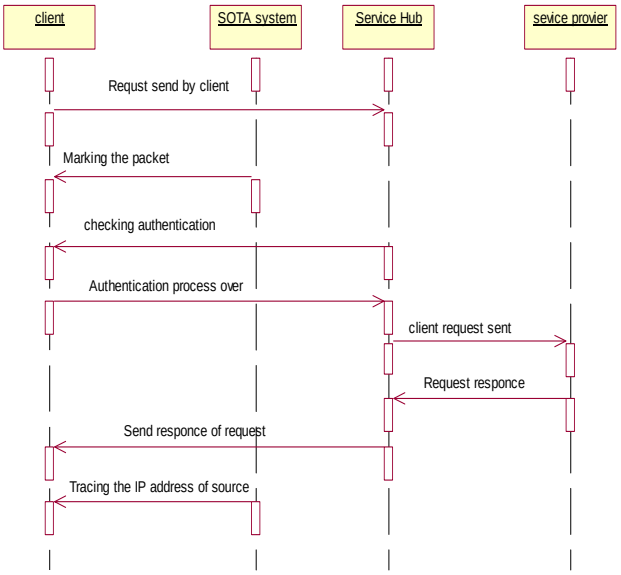

Fig 7: Sequence diagram

CONCLUSION AND FUTURE WORK

During the literature survey it has been observe that that normal mode there is no use of the verifier. In the SOTA system and Xdetector there is no any verification\validation process. To overcome this existing vulnerabilities of the system, proposing a new technique which will take care by verification\validation and backtracking mechanism.

In Future work proposed techniques may extend by examining multiple requests by SOTA and XDetector level before sending it to the service hub for validation .The packet which are coming from the attacker that are blocked at initial Xdetector level by using backtracking and SOTM tag mechanism.

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