ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

Preventing Cloud System from XML and HTTP DDoS Attack by Using Comber Approach via XDetector

Hemalatha G, Sundararajan.M, Arulselvi S

Assistant Professor, Dept. of CSE, Bharath University, Chennai, Tamil Nadu, IndiaDirector, Research Center for Computing and Communication, Bharath University, Chennai, Tamil Nadu, India

Co-Director, Research Center for Computing and Communication, Bharath University, Tamil Nadu, India

ABSTRACT: Cloud Computing is the newly emerged technology of Distributed Computing System. In this environment Distributed Denial of Service attack (DDoS), especially Hypertext Transfer Language(HTTP), Extensible Markup Language (XML) or Representational State Transfer(REST) based DDoS attacks may be very dangerous and may provide very harmful effects for availability of services and all consumers will get affected at the same time. One other reason is that because the cloud computing users make their request in XML then send this request using HTTP protocol and build their system interface with REST protocol such as Amazon EC2 or Microsoft Azure. So the threaten coming from distributed REST attacks are more and easy to implement by the attacker, but to security expert very difficult to resolve. So to resolve these attacks this paper introduces a comber approach for security services called filtering tree. This filtering tree are also called as XDETECTOR.

KEYWORDS: DDoS, REST Protocol, Amazon EC2, XDETECTOR.

1. INTRODUCTION

1.1 CLOUD COMPUTING

Cloud computing is a combination of distribute system, utility computing and grid computing. In cloud computing we use combination of all these three in virtualized manner. Cloud computing converts desktop computing into service based computing using server cluster and huge databases at data center. Cloud computing gives advanced facility like on demand, pay per use, dynamically scalable and efficient provisioning of resources. Cloud computing the new emerged technology of distributed computing systems changed the phase of entire business over internet and set a new trend. The dream of Software as a Service becomes true; Cloud offers Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS). Providing the basics of Cloud Computing is not part of this paper, for basic knowledge go through. Cloud offers these services with the help of Web Services

The main aim of the proposed framework is to create an Open Grid Services Architecture (OGSA) by employing Service Oriented Traceback Architecture (SOTA) in Conjunction with a filter defence system (XDetector) for an effective defence against XDoS and upcoming DXDoS attacks.

Denial of Service Attacks

- Exploitation of a system weakness.
- Computational system overload- Impose a computationally intensive task on a victim.
- Misusing a protocol- Inject packets and disturb protocol handlers.
- Flooding-based attacks- Use up all available bandwidth by fast sending many attack packets

Distributed Denial of Service Attacks

- Attacker logs into Master and signals slaves to launch an attack on a specific target address (victim).
- Slaves then respond by initiating TCP, UDP, ICMP or Smurf attack on victim.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

II. RELATED WORK

A lot of research has been done in the domain of network security but security for cloud computing is still a very new open challenge. Lot of research is going in security aspects in cloud computing. Now a days daily it is going to see that Cloud is facing the problem regarding new vulnerabilities as there are various latest real time examples in which cloud is suffering from new attacks. Among these different cloud vulnerabilities this paper is focusing on cloud API vulnerability mainly HTTP and XML DDoS attacks.

In the next following section paper is discussing about various vulnerability issues (as Shared Technology, Data Leakage and Insecure API)in IaaS layer.

2.1 Deterministic Packet Marking (DPM)

This approach effectively addresses shortcomings of existing techniques. [3]DPM is light, secure, scalable, and suitable for many types of attacks. In addition, it does not reveal the topologies of ISPs, which implement DPM—this is desirable.

2.2 SYN Flooding Attacks Using Fuzzy Logic

This paper introduced the new logic called fuzzy logic[4] to find flooding attack. This solution will give more false positive results.

2.3 Packet Marking for IP Traceback

We also offer a solution to traceback through our Cloud TraceBack (CTB)[5] to find the source of these attacks, and introduce the use of a back propagation neutral network, called Cloud Protector, which was trained to detect and filter such attack traffic. Our results show that we were able to detect and filter most of the attack messages and were able to identify the source of the attack within a short period of time.

2.4 IP Flow

In this paper, we establish IP Flow which is used to select proper features for DDoS detection[8]. The IP flow statistics is used to allocate the weights for traffic routing by routers. Our system protects servers from DDoS attacks without strong client authentication or allowing an attacker with partial connectivity in-formation to repeatedly disrupt communications. The new algorithm is thus proposed to get efficiently maximum throughput by the traffic filtering, and its feasibility and validity have been verified in a real net-work circumstance. The experiment shows that it is with high average detection and with low false alarm and miss alarm. Moreover, it can optimize the network traffic simultaneously with defending against DDoS at-tacks, thus eliminating efficiently the global burst of traffic arising from normal traffic.

2.5 Client Puzzles

DoS attacks using client puzzles[10], a cryptographic countermeasure which provides a form of gradual authentication by requiring the client to solve some computationally difficult problems before access is granted. In particular, we describe a mechanism for integrating a hash-based puzzle into existing web services frameworks and analyze the effectiveness of the countermeasure using a variety of scenarios on a network testbed. Client puzzles are an effective defence against flooding attacks. They can also mitigate certain types of semantic-based attacks, although they may not be the optimal solution.

2.6 SOAP message exchange in a SOA

[9]SOAP message exchange is one of the core services required for system integration in Service Oriented Architecture (SOA) environments. One key concern in a SOA is thus to provide Message Level Security (as opposed to point to point security). We observe that systems are communicating with each other in a SOA over SOAP messages, often without adequate protection against XML rewriting attacks.

III. PROPOSED WORK

In this project Our new approach, service oriented traceback architecture (SOTA), provides a framework to be able to identify the source of an attack. This is accomplished by deploying our defence system at distributed routers, in order to examine the incoming SOAP messages and place our own SOAP header. By this method, we can then use the new

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

SOAP header information, to traceback through the network the source of the attack. According to our experimental performance evaluations, we find that SOTA is quite scaleable, simple and quite effective at identifying the source. Fig 1 shows the overall architecture of the proposed.
we follow Service-Oriented Trace back Architecture (SOTA), by applying our framework to OGSA. We further add to our work by introducing a defense filter called XDetector [XML Detector], in which it is distributed throughout the grid, in order to properly defend it. Our system is one of the first defense systems to attempt to defend against these new attacks.

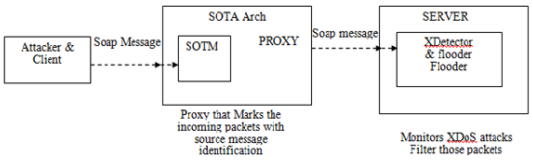

Fig 1 architecture of proposed work

The cloud browser can sent request to the server to access the data. while sending request original message is converted into SOAP message. The XML SOAP message from the client or attackers send to the corresponding server. It is considered to be a Service Oriented Traceback Architecture (SOTA). SOTA is founded upon the Deterministic Packet Marking (DPM) algorithm. DPM marks the ID field and reserved flag within the IP header. As each incoming packet enters into proxy is marked. Fig 2 shows the operation of the XDETECTOR architecture.
The marked packets will remain unchanged as they traverse the network. Outgoing packets are ignored. DPM methodology is applied to our SOTA framework, by placing the Service-Oriented Traceback Mark (SOTM) within web service messages. If any other web security services (WS-Security for example) are already being employed, SOTM would replace the 'token' that contains the client identification. Real source message identification are stored within SOTM, and placed inside the SOAP message. SOTM, as in DPM tag, will not change as it traverses through the network. The composition of SOTM is made up of one XML tag, so not to weigh down the message, and stored within a SOAP header.
SOTA does not directly eliminate an XDoS or DXDoS attack message. This is left for the filter section of a defense system (Firewalls or our new filter XDetector). Instead SOTA's two main goal is to deal with the two main objectives of XDoS, which are: 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, as other trace back methods.

IV. FUNCTIONAL MODULES

The cloud browser can sent request to the server to access the data. while sending request original message is converted into SOAP message. The converted message is send to the proxy server and transfer to the XDETECTOR to filter theattack before to reach the cloud server it filter all the attack in the requested message.

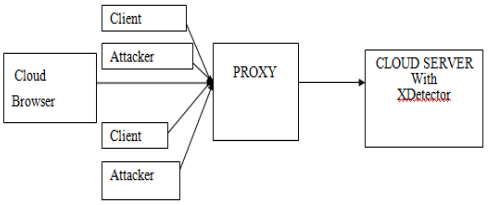

Fig 2 XDECTECTOR architecture

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

4.1 PROXY

This proxy transfers the XML SOAP message from the client or attackers to the corresponding server. It is considered to be a Service Oriented Traceback Architecture (SOTA). SOTA is founded upon the Deterministic Packet Marking (DPM) algorithm. DPM marks the ID field and reserved flag within the IP header. As each incoming packet enters into proxy is marked. The marked packets will remain unchanged as they traverse the network. Outgoing packets are ignored.

It deals with attackers, who are going to attack servers through web services. In this module attacker can hide his real source of identification by servers, they can compose a wrong message and they can change their XML structure and send the message to destination server via proxies.

4.2 XDETECTOR

It identifies the real source of XDoS attack messages, and filters in order to protect Grid Web Services. SOTA is a trace back system that is constructed on the basis of Web Services. XDetector, is a Back Propagation Neural Network, trained to detect and filter XDoS attack message. The empirical data from our experiments shows that SOTA is efficient and effective. The experimental data also shows that SOTA is able to traceback to the source. Once an attack has been discovered and the attacker's identity known, XDetector can filter out these attack messages.

It checks the SOAP message for any of the changes through, True identity hiding, Wrong composition of message, Unformatted message.

4.3 SERVER

Server can validate the user and check the user IP address and response the request to the client. Sometimes proxy can act as server and sent response to the client. Proxy can act as a intermediate node between the client and the server to provide the reliable service to client without any delay attack. It contains the web page to calculate life time for the input (DOB), generally called user interface.

V. CONCLUSION

DDoS attack is a more dangerous in cloud system because the cloud system consists of collection of information in the single place so for the hacker it is easy to send the attack to affect or stop the services in the network. So this paper is used to filter the service request messages at different stages by using the XDectector in the server. By using this application the Xml and HTTP DDoD attack is monitored and to provide the reliable service to client.

REFERENCES

[1] Ashley Chonka,YangXiang n, WanleiZhou, AlessioBonti (2011), "Cloud security defense to protect cloud computing against HTTP-DoS and XML-DoS attacks" Journal of Network and Computer Applications, vol. 34, pp.1097–1107.

[2] Subha Palaneeswari M., Ganesh M., Karthikeyan T., Manjula Devi A.J., Mythili S.V., "Hepcidin-minireview", Journal of Clinical and Diagnostic Research, ISSN : 0973 - 709X, 7(8) (2013) pp.1767-1771.

[3] Bakshi, A.; Yogesh, B (2010), "Securing Cloud from DDOS Attacks Using Intrusion Detection System in Virtual Machine",ICCSN '10.Second International Conference on Communication Software and Networks , pp.260-264.

[4] Laljee R.P., Muddaiah S., Salagundi B., Cariappa P.M., Indra A.S., Sanjay V., Ramanathan A., "Interferon stimulated gene - ISG15 is a potential diagnostic biomarker in oral squamous cell carcinomas", Asian Pacific Journal of Cancer Prevention, ISSN : 1513-7368, 14(2) (2013) pp.1147-1150.

[5] Belenky, A.; Ansari, N (2003), "Tracing multiple attackers with deterministic packet marking (DPM)", IEEE Pacific Rim Conference on Communications,Computers and signal Processing pp. 49- 52.

[6] Kumar S., Das M.P., Jeyanthi Rebecca L., Sharmila S., "Isolation and identification of LDPE degrading fungi from municipal solid waste", Journal of Chemical and Pharmaceutical Research, ISSN : 0975 – 7384 5(3) (2013) pp.78-81.

[7] Chu-Hsing Lin; Chen-Yu Lee; Jung-Chun Liu; Ching-Ru Chen; Shin-Yang Huang (2010), "A detection scheme for flooding attack on application layer based on semantic concept", Computer Symposium (ICS), 2010 International pp.385-389.

[8] Sundar Raj M., Arkin V.H., Adalarasu, Jagannath M., "Nanocomposites based on polymer and hydroxyapatite for drug delivery application", Indian Journal of Science and Technology, ISSN : 0974-6846, 6(S5) (2013) pp.4653-4658.

[9] Gruschka, N, Iacono, L.L (2009), "Vulnerable Cloud: SOAP Message Security Validation Revisited", ICWS 2009. IEEE International Conference on communication system pp.625-631.

[10] Vijayaprakash S., Langeswaran K., Gowtham Kumar S., Revathy R., Balasubramanian M.P., "Nephro-protective significance of kaempferol on mercuric chloride induced toxicity in Wistar albino rats", Biomedicine and Aging Pathology, ISSN : 2210-5220, 3(3) (2013) pp.119-124.

[11] Liming Lu (2008), "A General Model of Probabilistic Packet Marking for IP Traceback," ASIACCS '08, ACM. pp 18-20, pp. 83–97.

[8] Lin Fan (2010),"A Group Tracing and Filtering Tree for REST DDoS in Cloud Computing" International Journal of Digital Content Technology and its Applications. pp. 226–237

[9] M.A. Rahaman, A. Schaad and M.Rits (2006),"Towards secure SOAP message exchange in a SOA", Proceedings of the 3rd ACM workshop on Secure Web Services.ACM Press, pp.77-84.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

[10] Suriadi, S, Stebila D,Clark, A.; Hua Liu(july (2011) , "Defending Web Services against Denial of Service Attacks Using Client Puzzles", 2011 IEEE International Conference on Web Services (ICWS), pp.25-32, 4-9.
[11] Tuncer, T.; Tatar, Y (2008)."Detection SYN Flooding Attacks Using Fuzzy Logic", 2008. ISA 2008. International Conference on Information Security and Assurance, pp.321-325, 24-26.
[12] Jemima Daniel,Language Teaching in the Digital Age,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 11029-11031, Vol. 3, Issue 4, April 2014.
[13] Jemima Daniel,Importance of Group Discussions,International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 9081-9084,Vol. 3, Issue 2, February 2014.
[14] Jemima Daniel,The Playboy of the Western World' As a Tragi-Comedy, International Journal of Innovative Research in Science,Engineering and Technology,ISSN: 2319-8753,pp 10379-10381,Vol. 3, Issue 3, March 2014.
[15] Jemima Daniel,Techniques Used in Teaching English, International Journal of Innovative Research in Science, Engineering and Technology,ISSN: 2319-8753,pp 8791-8793,Vol. 3, Issue 1, January 2014.
[16] M. Santhi & Dr. A. Mukunthan,A Detailed Study of Different Stages of Sleep and Its Disorders – Medical Physics,International Journal of Innovative Research in Science, Engineering and Technology ,ISSN: 2319-8753, pg 5205-5212 , Vol. 2, Issue 10, October 2013.
[17] M.NAGESHWARI, Dr.A.MUKUNTHAN , C.RATHIKA THAYA KUMARI,A Study of Surface Ozone Measurement at Vadasery, Kanyakumari District,International Journal of Computer & Organization Trends (IJCOT),ISSN: 2319-8753, pp 160-165,Vol. 1, Issue 2, December 2012.