www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume – 4 Issue - 12 December, 2015 Page No. 15358-15363

Dos Resistant Cloud Based Secure Authentication Protocol

Dr. Kalavathi[1], Ms. Y. Haritha[2]
[1]Vasireedy Venkatadri Institute of Technology, Department of Computer Science and Engineering
Guntur, Andhra Pradesh, India
Kalavathi_alla@yahoo.com
&
[2]Vasireedy Venkatadri Institute of Technology, Department of Computer Science and Engineering
Guntur, Andhra Pradesh, India

Abstract: cloud computing has become crucial in todays' technical environment The identity verification s the man functionality in these cloud computing services. But as on today these identity protection gateways are very inclined from attacks by denial of service. Numerous authentication protocols are available that are very strong in protecting identities in traditional networked applications. But these protocols suffer with DOS attacks when we us them in cloud computing applications. This failure is due to the heavy utilization of cloud resource and lot of verification process involved in these services. In this paper authors propose a new authentication protocol which overcomes with internal and external denial service attacks. The proposed solution involves multilevel authentication schemes. The technique finds out the legitimate user's requests and allow them at the front of the processing queue.

Keywords: Cloud Computing, Security, DoS Attacks, Authentication

1. Introduction

There are different types of attacks on cloud by intruders or outsiders. They are classified as Denial of service attacks, Cloud Malware Injection attacks, Side Channel attacks, Authentication attacks, man in the middle attacks. In this paper we focus mainly on Dos attacks. Denial of service attacks mainly focus on web resources, which are provided by cloud service providers. Denial of service (DOS) makes the cloud servers unavailable to the end users. In a cloud environment Dos attacks are great security risks since the resources are shared by multiple users in the cloud [4]. Dos attacks makes the cloud servers un available by sending unnecessary traffic to the servers. Because of this unnecessary traffic server performance will be degraded and sometimes servers will crash. There are numerous Dos attacks on cloud.

A. Specific attacks on cloud

There are different types of attacks on cloud by intruders or outsiders. They are classified as Denial of service attacks, Cloud Malware Injection attacks, Side Channel attacks, Authentication attacks, man in the middle attacks. In this paper we focus mainly on Dos attacks. Denial of service attacks mainly focus on web resources, which are provided by cloud service providers. Denial of service (DOS) makes the cloud servers unavailable to the end users. In a cloud environment Dos attacks are great security risks since the resources are shared by multiple users in the cloud [4]. Dos attacks makes the cloud servers un available by sending unnecessary traffic to the servers. Because of this unnecessary traffic server performance will be degraded and sometimes servers will crash. There are numerous Dos attacks on cloud.

B. Dos Attacks

SYN Flooding attack: this attack exploits the flaws in TCP 3 way handshaking during connection establishment. The attacker sends a series of SYN requests from a spoofed IP address and server allocates all the required resources and waits for ACK from client which will never come. So the server is overwhelmed with huge number of requests and will not be able to respond to a legitimate user's request.

Ping of Death Attack: Attacker sends IP packets more than 65,536 bytes which is the maximum size of IP packet. By using fragmentation, IP divides into several fragments. But from 1996 onwards attackers took advantage of this feature when they found

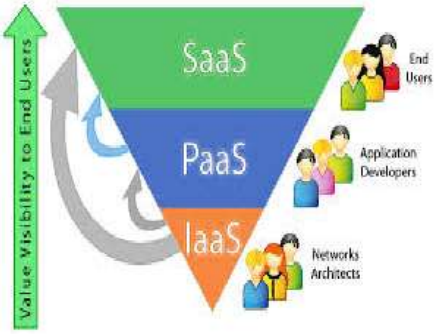
packet broken in a small packet, then they add more than 65,536 bytes in the original data [5]. Many operating systems are not aware of what to do when they receive a packet more than 65536 bytes. Therefore operationg systems simply froze, reboot and/or crashed.

Ping of death attacks are dreadful because the identity of the intruder sending an extra sized packet can spoof the packets. To avoid these attacks, the operating system vendors released some patches, but still some weebsites are under the blocking of ICMP messages. These messages are filtered at firewall to prevent ping of death attacks.

Smurf attacks: It is a type of denial of service attack on IP and ICMP. Intruder uses the features of smurf program to make the network inoperable. ICMP can be used to send error notification messages among the clients to the server [4]. The IP packet contains ICMP ping notifications and the entire network resources address in the given network. The ping messages are sent as echo to reply back to the vulnerable address. These ping and echo messages flood the network traffic.

2. Review of Literature

Generally cloud computing structure relies on 3 service layers such as Infrastructure as a service, Platform as a service and software as a service. The first layer allows users to access physical resources, networks, bandwidth and storage. The second layer PaaS built on IaaS allows users to access operating and system and platform to develop software applications. The last layer SaaS allows end users to access software applications. Dos attacks at all layers of cloud computing is a major challenge due to the difficulty of distinguishing attackers request from legitimate user's request. Therefore detection of dos attacks in the early stage(saas) is more important than in the other layers. However all service requests for Saas must be authenticated to be approved. Many authentication protocols can be used in SAAS layer.

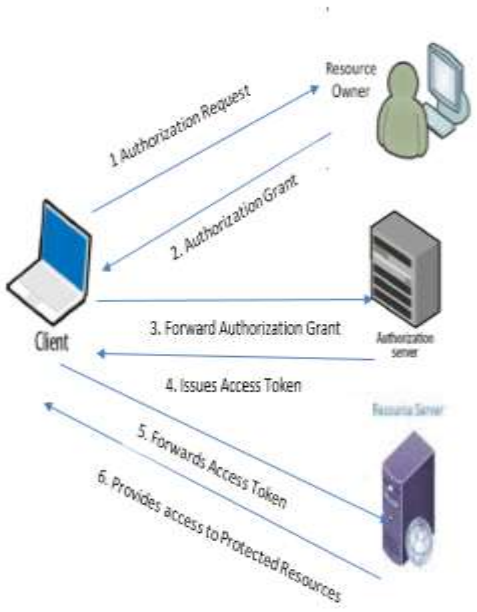


The OAuth (Hardt 2012) protocol is currently a widely used authentication protocol that enables a third party authentication to obtain a limited access to HTTP service. In OAuth, the resource owner can allow a third party client to access the resources through the resource owner. For example a user as a photo owner (resource owner) can grant a permission to a printing service (client) to access the photo. All photos are stored in a photo exchange server (resource server). Rather than sharing the user credentials with the printing service, the user is authenticated to a server that is trusted by the photo exchange server (authorization server) which then issues a session token to access the resources. But there are limitations in sharing credentials such as user name and password with third party client to access the restricted resources. The first limitation is that the access information includes password which is stored by a third party client in a clear text for future reference. The second limitation is server should only use password as an authentication method. The third limitation is resource's owner cannot limit the access of a third party client and cannot control the duration of access. Finally if password is available all the resources are available to third party client. Therefore OAuth allows third party client to access the resources of the server with privileges and rules without using resource owners access information. OAuth Process Flow diagram

1.OAuth process starts from when the resource owner receives authorization request from the client.

2.The resource owner sends back the authorization grant to the client. The client's authorization request determines the type of grant. Authorization are of several types:

a)Authorization Code Grants: These grants are given to the Clients by the resource owners which in turn must be authorized by authorization server. With this type of code client need not require resource owners credentials. So it is a secure grant type.



b)Implicit Grants: These codes depend on browser implementation using a scripting language, so that the access token is directly issued to the client.

c)Resource Owner Password Credentials Grants: Use resource owners user id and password to issue an access token to the client. This type of grant can be used when the client is highly trusted by the resource owner.

d)Client Credentials Grants: Provides limited scope of access to protected resources on the server. This type of grant can be used when the client is resource owner or when the client has previously had privileges to access the resources.

3) Now the client sends authorization grant and authentication to authorization server to get access token

4) The access token will be provided by the authentication server only after the validation of client authentication. The access token can be used in different ways based on security requirements of the server like with different types of cryptography. When the token is expired or becomes invalid it can be refreshed by sending an authorization grant to the authentication server.

5) The client then sends access token to resource server to request restricted resources on the server.

6) The server will respond to the request when validating the access token.

However, any insecure implementation of OAuth, leads to Dos attacks [10]. Many authentication protocols have been proposed for Saas layer, but they are unaware of Dos attacks. Yasin et al (2013) proposed an authentication process based on one time passwords (OTP) with mutual authentication of the cloud user and cloud server. Yasin's authentication procedures defended against the possibility of replay attack but not against a Dos attack. Various cloud based authentication protocols have been proposed by chaudhury et al (2011), Jaidhar et al(2012), Tseur et al(2012), but they use smart card reader for authentication process. In addition Yasin et al protocol also uses another physical device such as finger print scanner. Therefore it is necessary and significant to verify Dos resistance in every process of the authentication protocol.

An example of an authentication protocol that would be aware of Dos attack in the traditional networks is Host Identity Protocol (HIP) which is proposed by moskowitz et al(2008). But this protocol cannot be implemented in the application layer (Saas) because it uses host identity of network layers. Furthermore any authentication protocol that is based on IP address verification such as IPSec makes it difficult to hide the identity of participants.

One approach to investigate the strength of authentication protocol against Dos attacks is the cost based approach. This approach was proposed by Meadows et al(2001) to demonstrate the effectiveness of protocols in preventing Dos attacks [9]. According to Meadows approach, one of the participants will get computationally exhausted first. The computational costs for both the requester and responder need to be determined. The total computational cost of the requester is the total estimated cost of each operation involved in the authentication process during the session life time. The total computation cost of the responder is the total estimated cost of each operation involved in the authentication process until the requester is identified as legitimate user. He further proposed the following categories to classify the computation cost: expensive, medium and inexpensive [8]. The expensive computations include exponential operations and signature operations. The medium computations class includes encryption and decryption operations. The inexpensive computations include all other operations which are not mentioned above.

3. The next section focus on the operational procedure of Dos resistant cloud based authentication protocol (DRCBAP). Section 4

analyzes the proposed algorithm and section 5 provides conclusion remarks on the proposed protocol.

3. Proposed System

The DRCAP is a combination of several protocols. Following are the notations used in DRCAP to establish a secure session.

The first protocol is a registration request protocol (RRP). It establishes an agreement between the client and the cloud server. Thus, the participants can use that information during the operation of DRCAP. The second protocol is an identification protocol that works against Dos attacks. The third protocol is used for authentication process(AP) which includes all operations that occur during registration request. Therefore, cloud server can confirm the identity of the client and then prevent an intruders in Dos attacks.

A. Registration Request Protocol(RRP)

During this phase the client and cloud server share the required identity data to register the client into the cloud server database. The registration process begins when the client submits all required data to the cloud server. This required information includes Client first name, last name, organization name, country name, e-mail-id and phone-number and any other information required by the cloud service provider (CSP). Then the cloud server verify this information and stores in its database and sends a validation message to the client to confirm its request through e-mail. After this validation cloud server will activate the client's account [12]. Furthermore, cloud server generates a hash code on the client's registration data using SHA-1 and then encrypts the hash code using the mater key of cloud server K_m. K_m is only known to the cloud server.

Even if a client is registered with cloud server, the client cannot access the available resources from the cloud server unless the cloud server authenticates the client. DRCAP provides an outer shield to the authentication protocol in identifying the legitimate clients from the Dos attackers. The DRCAP identification protocol is designed to provide this outer shield which is described in the following sub-section.

B.DRCAP Identification Protocol

DRCAP identification protocol was designed on the basis of cost model. According to this approach, before applying the computational power of the authentication protocols on the server side, the clients are asked to give their commitment in receiving the resources from cloud servers [13]. This validation of commitment is to identify the genuinely of client request. DRCAP uses a maximum of 512 items in a set. These items are public integer numbers that both client and cloud server agree during the RRP process itself. The protocol functions as follows:

1.Client sends a request for resource with a Use Id and password to cloud server. At this point, cloud server will block any client who has performed more than 3 consecutive requests within a short time to prevent intruders. The attacker may launch Dos attacks by sending random user id's and passwords.

2.Cloud server sends a nonce(pseudo random number) as a response with valid time stamp. The cloud server requests the client to send its commitment in receiving the services along with h(encrypted hash code on clients data).

3.Client forwards the requested information to the cloud server along with the time stamp which is encrypted with the pre-shared secret key.

4.Cloud server will check the received values and also check the time difference between received and transmitted time stamp

If condition 4 do not satisfy, cloud server will not consider the request and consider the client request as attacker's request. However, once the client satisfy this condition, cloud server will decrypt the received and validates the client ID. Finally to determine whether the client is legitimate or not, DRCAP uses authentication protocol.

DOI: 10.18535/Ijecs/v4i12.43

Operation	Category	Operation	category
Send the initial request	Inexpensive	Reply directly to the request via secure hashing of the related values to obtain h and ask the client for CT	Expensive
Verify the received and transfer It to cloud server	Expensive	Verify the received elements	Medium
Decrypt the session key	Medium	Decrypt the CT. Generate and encrypt the session key	Medium

C. Authentication Protocol

Once the validation is verified at Identification protocol, cloud server will generate the session key ($K_{s)}$, and is encrypted with pre-shared secret key [11]. Furthermore, cloud server adds session and key K_s and Time stamp T to the CT. Authentication protocol functions in the following manner:

1.Cloud server sends the generated session key that is encrypted by pre-shared secret key K_s, along with the modified CT.

2.Client confirms the received information by sending back the modified CT to the cloud server

Later, the two parties can agree regarding the sub session keys by re-applying the processes of the authentication protocol.

The title of the paper is centered 17.8 mm (0.67") below the top of the page in 24 point font. Right below the title (separated by single line spacing) are the names of the authors. The font size for the authors is 11pt. Author affiliations shall be in 9 pt.

4. Analysis of DRCAP

Assessment of the DRCAP entails evaluation of the protocol's efficiency against DoS attacks by applying a cost approach. In addition, the evaluation process measures the computation cost when the client participates in authentication process. The operational cost of DRCAP is categorized as expensive [7]. The other operations of the client are listed within the medium or inexpensive

DRCAP COST Approaches:

5. Conclusion

The use of data in cloud computing environment is increasing day by day. In this work, authors have proposed a new cloud based authentication protocol suite to identify and authenticate cloud users at the SaaS layer and also protects against DoS attacks. By using encrypted hash code CT, one can prevent all the security breaches that led do DoS attacks. In the DRCAP, we have designed an identity protocol such that the computational cost incurred by the cloud resources is minimized and the computation cost incurred by cloud users adjustable based on the service's sensitivity. The proposed DRCAP protocol suite can be implemented in the SaaS layer of cloud computing systems. DRCAP relies on both software and hardware requirements of cloud servers and cloud users. DRCAP protocol does not need any external hardware device for the authentication process.

References

[1] Hassan, Qusay (2011). "Demystifying Cloud Computing"(PDF). The Journal of Defense Software Engineering(CrossTalk) **2011** (Jan/Feb): 16–21. Retrieved 11 December2014.

[2] http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf

[3] M. Haghighat, S. Zonouz, & M. Abdel-Mottaleb (2015).CloudID: Trustworthy Cloud-based and Cross-Enterprise Biometric Identification. Expert Systems with Applications, 42(21), 7905–7916.

[4] "The economy is flat so why are financials Cloud vendors growing at more than 90 percent per annum?". FSN. March 5, 2013.

[5] "Realization of Interoperability & Portability Among Open Clouds by Using Agent's Mobility & Intelligence - TechRepublic". TechRepublic. Retrieved 2015-10-24.

[6] "Interoperability and Portability among Open Clouds Using FIPA Agent / 978-3-659-24863-4 / 9783659248634 / 3659248630". www.lap-publishing.com. Retrieved2015-10-24.

[7] Choudhury AJ, Kumar P, Sain M, Lim H, Jae-Lee H. A strong user authentication framework for cloud computing. In: IEEE Asia-Pacific Services Computing Conference. IEEE; 2011. p. 110e5.

[8] Dierks T. The TLS protocol version 1.0. 1999. http://tools.ietf.org/html/rfc2246.

[9] Diffie W, Hellman M. New directions in cryptography. IEEE Trans Inf Theory 1976;22(6):644e54.

[10] Hardt D. The OAuth 2.0 authorization framework. 2012. http://tools.ietf.org/html/rfc6749.

[11] Hwang MS, Chong SK, Chen TY. DoS-resistant ID-based password authentication scheme using smart cards. J Syst Softw2010;83(1):163e72.

[12] Jaidhar CD. Enhanced mutual authentication scheme for cloud architecture. In: 3rd IEEE International Advance Computing Conference (IACC). IEEE; 2012. p. 70e5.

[13] Juels A, Brainard J. Client puzzles: a cryptographic countermeasure