Security issues in cloud computing and its countermeasures

Pavan Muralidhara

Abstract- Cloud computing is a technology of delivering resources such as hardware, software (virtual too) and bandwidth over the network to the consumers worldwide. All the services are requested and accessed through a web browser or web service. The main advantage that cloud is provided to the nation worldwide is that it is not so easily affordable to one and all. Multi-conglomerate companies invest a lot of money on the cloud and let people access it for a smaller cost and even free at the lowest level of the consumer chain. In this paper we address to the problems that the cloud technology faces and how it can be overcome.

Keywords- Cloud computing, Security issues, Cloud security, Denial of Service, Xml signature element wrapping, Brower security, Cloud malware injection

1 INTRODUCTION

Cloud computing name suggests that it's a cloud of services. It was also named "cloud" because you can view cloud from everywhere be it from India or from Amsterdam. Similarly you can access the cloud from anywhere, from whichever part of the world from an array of devices right from computers, laptops, pda's, mobiles, etc. Companies or even direct consumers can access the services present in cloud through a web server or a web browser. Advantage of cloud is that it reduces the cost of hardware deployment, software license and system maintenance. But as they say, nothing comes without a price to pay. Hence this paper illustrates some of the security issues in cloud technology and how to overcome those.

Figure 1: Real definition of cloud (accessible from anywhere from many devices)

2 CLOUD COMPUTING SECURITY ISSUES AND ITS COUNTERMEASURES

2.1 DoS Attack

Denial of Service is one of the attacks on the cloud that prevents the consumer from receiving the service from the cloud. The attacker usually floods the cloud with excessive requests to the target server and the actual consumer might not be able to receive the service since the server is busy servicing the attacker. There are many methods to perform a DoS attack such as SYN flood. A SYN flood exploits the TCP 3-way handshake by requesting connections to the target server and ignoring the acknowledgement (ACK) from the server. This makes the server to wait for the ACK from the attacker, wasting time and resources. Eventually, the server does not have enough resources to provide services to clients. This attack can be prevented by authorizing strict access to the cloud and using cryptographic protocols to ensure that the right personnel are accessing the cloud.

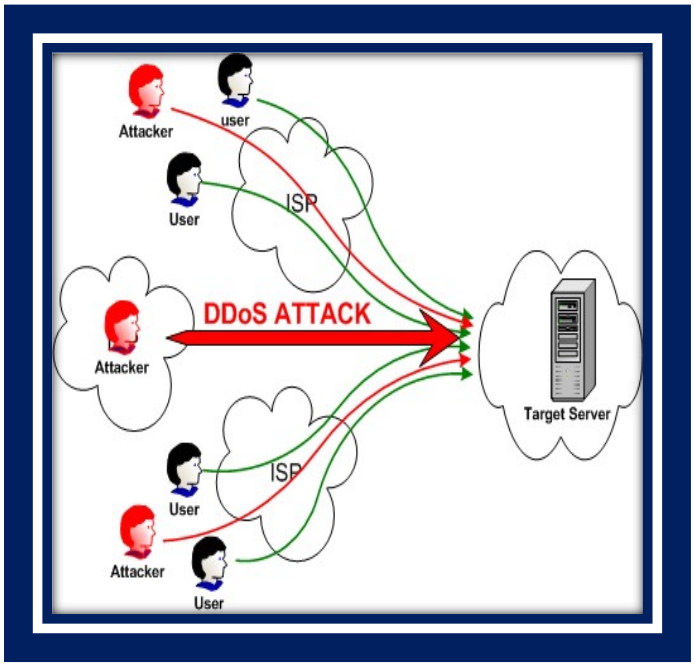

Figure 2: Denial of service to the customer by the attacker

2.2 Xml signature element wrapping

Due to the fact that clients are typically able to connect to cloud computing via a web browser or web service, web service attacks also affect cloud computing. XML signature element wrapping is the well-known attack for web service. Although Cloud security uses XML signature in order to protect an element's name, attributes and value from unauthorized parties, it is unable to protect the particulars in the document. An attacker is able to manipulate a SOAP message by copying the target element and inserting whatever value the attacker would like and moving the original element to somewhere else on the SOAP message. This technique can trick the web service to process the malicious message created by the attack. Figures 3 and 4 illustrate an example of an XML signature element wrapping attack.

According to the figure 3, the client requests a picture called "me.jpg". However, if the attacker intercepts and alters the SOAP message by inserting the same element as the client but the attackers requests a document called "cv.doc" instead of the picture shown as the figure 4. After the web service receives the message, the web service will send the cv document back to the client. Another potential scenario attack may be in the case of the e-mail web service application. If an attacker intercepts the SOAP message and changes the receiver's e-mail address to the attacker's e-mail address, the web service will forward the e-mail to the attacker. In 2008, Amazon's EC2, which is the public cloud computing system of Amazon, was discovered that it was vulnerable to XML signature element wrapping attack .The possible countermeasure would be using a combination of WSSecurity with XML signature to sign particular element and digital certificated such as X.509 issued by trusted Certificate Authorities (CAs). Furthermore, the web service server side should create a list of elements that is used in the system and reject any message which contains unexpected messages from clients.

Figure 3: Soap message before the attack

Figure 4: Soap message after the attack

2.3 Cloud malware injection attack

Cloud malware injection is the attack that attempts to inject a malicious service, application or even virtual machine into the cloud system depending on the cloud service models (SaaS, PaaS and IssA) [5]. In order to perform this attack, an intruder is required to create his own malicious application, service or virtual machine instance and then the intruder has to add it to the cloud system. Once the malicious software has been added to the cloud system, the attacker has to trick the cloud system to treat the malicious software as a valid instance. If it is successful, normal users are able to request the malicious service instance, and then the malicious is executed. Another scenario of this attack might be an attacker try to upload a virus or trojan program to the cloud system. Once the cloud system treats it as a valid service, the virus program is automatically executed

and the cloud system infects the virus which can cause damage to the cloud system. In the case of the virus damages the hardware of the cloud system, other cloud instances running on the same hardware may affect to the virus program because they share the same hardware. In addition, the attacker may aim to use a virus program to attack other users on the cloud system. Once a client requests the malicious program instance, the cloud system sends the virus over to the internet to the client and then executes on the client's machine. The client's computer then is infected by the virus. The possible countermeasure for this type of attack could be performing a service instance integrity check for incoming requests. A hash value can be used to store on the original service instance's image file and compare this value with the hash values of all new service instance images. As a result of using the hash values, an attacker is required to create a valid hash value comparison in order to trick the cloud system and inject a malicious instance into the cloud system.

2.4 Browser security

In a cloud computing system, the computational processes are completed in the cloud server whereas the client side just sends a request and waits for the result. Web browser is a common method to connect to the cloud systems. Before a client can request for services on the cloud system, the client is required to authenticate himself whether he has an authority to use the cloud system or not. In the security point of view, these days, web browsers rely heavily upon SSL/TLS process. They are not able to apply WS-Security concept (XML Signature and XML Encryption) to the authentication process. As a consequence, when a web browser requests a service from the web service in a cloud system, it cannot use XML Signature to sign the client's credentials (e.g. username and password) in order to authenticate the user and XML Encryption to encrypt the SOAP message in order to protect data from unauthorised parties. The web browser has to use SSL/TLS to encrypt the credential and use SSL/TLS 4-way handshake process in order to authenticate the client. Nevertheless, SSL/TLS only supports point-to-point communications, meaning that if there is a middle tier between the client and the cloud server, such as a proxy server or firewall, the data has to be decrypted on the intermediary host. If there is an attacker sniffing packages on that host, the attacker may gain the credentials and use the credentials in order to log in to the cloud system as a valid user. In addition, SSL/TLS has been broken by Marlinspike in July 2009. Marlinspike used the technique called "Null Prefix Attack" in order to perform undetected man-in-the-middle- attack attacks against SSL/TLS implementation. As a result of this, attackers are able to perform this technique in order to requests services from cloud systems without a valid authentication. It seems that SSL/TLS is still limited in its capacities as an authentication for cloud computing. The potential countermeasure for this is that the vendors that create web browsers apply WS-Security concept within their web browsers. The reason why WS-Security appears to be more suitable than SSL/TLS is WS-Security works in message level. As a result of this, web browsers are able to use XML Encryption in order to provide end-to-end encryption in SOAP messages. Unlike point-to-point encryption, end-to-end encryption does not have to be decrypted at intermediary hosts. Consequently, attackers are unable to sniff and gain plain text of SOAP messages at the intermediary hosts illustrated.

3 Conclusions

In this paper, a selection of issues of cloud computing security, DoS attack, XML Signature Element Wrapping, Cloud Malware Injection Attack and Browser Security, and its potential countermeasures are mentioned. Due to Dos attack, the attacker can flood messages to the cloud which results in denying services to the actual customer. The attacker can also alter the soap message to change the requested data by the customer and possibly even change whom the service has to be delivered to which could be ridiculously dangerous. The attacker could also install a malicious software or a program on to the cloud which can cause havoc as the malicious software controlled by the attacker would be servicing the customer and getting a lot of details from the host .Last, but not the least browser security is another issue in cloud security as all services will be requested either through web server or web browser.

4 References

[1]Amazon Web Services. (2009) Amazon Elastic Compute Cloud (Amazon EC2). http://aws.amazon.com/ec2/csrc.nist.gov/groups/SNS/cloudcomputing/ cloud-def-v15.doc

[2]Cloud Security Alliance. (2009) Security guidance for critical areas of focus in cloud computing V2.1. http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf

[3] M. Jensen. et. al. (2009) "On Technical Security Issues in Cloud Computing" IEEE International Conference in Cloud Conouting, pp.109-116, Sep 2009.

[4]M. Marlinspike. (2009) Null Prefix Attacks Against SSL/TLS Certificates. http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf

[5] M. McIntosh and P. Austel. "XML Signature Element Wrapping Attack and CounterMeasures" Workshop on Secure Web Service, pp.20-27, 2005.

[6] N. Gruschka and L. L. Iacono. "Vulnerable Cloud: SOAP Message Security Validation Revisited" IEEE International Conference on Web Service, pp.635-631, Jul 2009.

[7]US-CERT. (2004) Understanding Denial-of-Service Attacks. [Online]. Available: http://www.us-cert.gov/cas/tips/ST04-015.html