SECURITY ISSUES IN CLOUD COMPUTING AND COUNTERMEASURES

DANISH JAMIL

Department of Computer Engineering, Sir Syed University of Engineering & Technology, Main University Road, Karachi, Sindh-75300, Pakistan

HASSAN ZAKI

Department of Computer Engineering, Sir Syed University of Engineering & Technology, Main University Road, Karachi, Sindh-75300, Pakistan

Abstract:

Cloud computing technology is a new concept of providing dramatically scalable and virtualised resources, bandwidth, software and hardware on demand to consumers. Consumers can typically requests cloud services via a web browser or web service. Using cloud computing, consumers can safe cost of hardware deployment, software licenses and system maintenance. On the other hand, it also has a few security issues. This paper introduces four cloud security problems, which are XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks, and also gives the possible countermeasures.

Keywords: ***Cloud Computing, Security and Countermeasures, Consumers, XML Signature Element Wrapping, Browser Security.***

1. INTRODUCTION

Cloud computing is a new concept of computing technology that uses the internet and remote servers in order to maintain data and applications. It provides dramatically scalable and virtualised resources, bandwidth, software and hardware on demand to consumers. This allows the consumers to safe cost of hardware deployment, software licenses and system maintenance. The consumers are able to use applications or services on the clouds using the internet. Users can typically connect to clouds via web browsers or web services. Although cloud computing offers many advantages to the consumers, it also has several security issues. This paper illustrates the issues in cloud computing concept. The paper is organised as follow: In the next section, related technologies to cloud computing and technical concept of cloud computing are described. The third section shows the security issues in cloud computing and potential attacking techniques used to break into the cloud systems. Then, the conclusion is given in the last section of the paper.

2. BACKGROUND AND RELATE TECHNOLOGIES

A. Web Service

A Web service is a software system designed to support interoperable machine-to-machine interaction over a network [4]. It can be a user request a service from a web service or another web service request a service from the web service. Web service can be interacted using SOAP messages. The SOAP messages are generally transmitted through HTTP protocol with an XML format.

In general usage, a web service provides services to clients. On the other end, a client requests a service via a particular application communicating directly to the web service or a web browser connecting to the web service via AJAX (Asynchronous JavaScript and XML). In order to protect SOAP messages from unauthorised parties to view or alter the messages, OASIS (Advancing open

Standards for the information society) released a standard for web service called Web Services Security (WS-Security) [9]. WS-Security is the security mechanism for web service working in message level. It relies on digital signature and encryption techniques to ensure that messages are secured during in transit. Digital signature provides data integrity or to proof authenticity to the communications by using hash algorithm whereas encryption process offers data confidentiality to the messages. In WS-Security case, encryption method can be implemented by either symmetric or asymmetric method.

B. Cloud Computing

Cloud computing is a model for enabling on-demand network access in order to share computing resources such as network bandwidth, storage, applications, etc , that is able to be rapidly scalable with minimal service provider management [2]. National Institute of Standard and Technology (NIST) describes cloud computing with five characteristics, three service models and four deployment models.

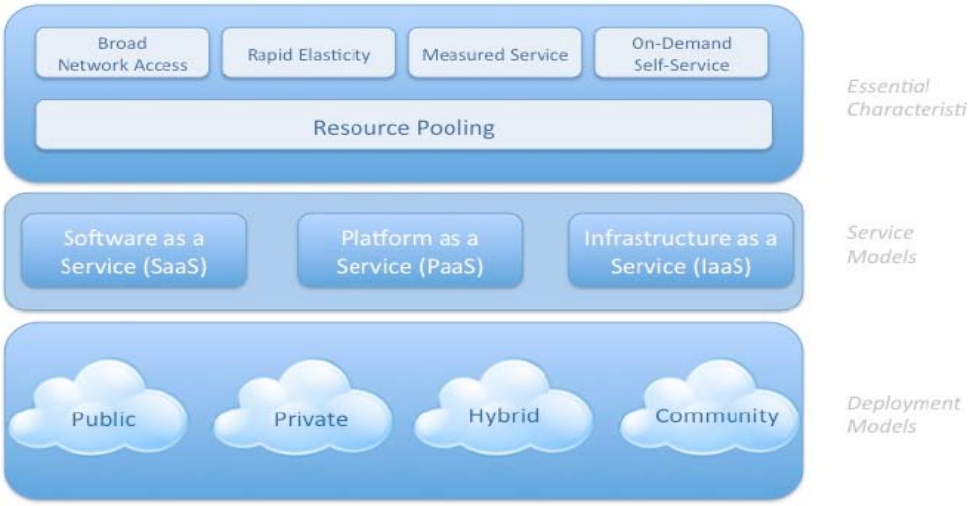

Fig. 1 NIST visual model of cloud computing definition [3].

Five characteristics of cloud computing consist of on demand self service, broad network access, resource pooling, rapid elasticity and measured service. On-demand self service provides automatic computing capability management to systems, without requiring human interaction. Broad network access allows heterogeneous clients, such as mobile phones, laptops, to connect to cloud systems over the network. Resource pooling in cloud systems is available as pooling resources for multiple consumers which is able to dynamically assign and reassign according to consumer demand. Rapid elasticity offers rapidly and elastically provision of capabilities. It can quickly scale out and dramatically release to quickly scale in automatically in order to support consumer's systems. Measure service provides monitoring, controlling and reporting of resource usage. Three cloud service models refer to software, platform and infrastructure models. Cloud Software as a Service (SaaS) is the model of providing the capability for consumers in order to use the provider's application running on a cloud infrastructure.

The applications can be accessed from a client interface such as a web browser or web service. An example of this model is "Google Apps". Cloud Platform as a Service (PaaS) allows consumers to deploy their own infrastructures or applications using programming languages and tools supported by the provider. Cloud Infrastructure as a Service (IaaS) provides processing, storage network bandwidth and other fundamental computing resources which allow customers to deploy and run operating systems or applications. Four cloud deployment models, public, private community and hybrid, are divides by considering by requirements. Public cloud is operated for the general public. The cloud system owner sells cloud services to consumers. Private cloud is made to a single organization. It can be managed by either the organization or a third party. Community cloud is the cloud infrastructure that is shared by several organizations and supports a specific community. Hybrid cloud is the composition of two or more cloud infrastructures that are bound together.

C. Denial of Service (DoS) Attack

DoS attack is the form of attack that an attacker aims to prevent legitimate users from accessing information or services. The common type of DoS attack occurs when an attacker floods a network with excessive requests to

the target server until the server is unable to provide services to normal users [10]. There are many methods to perform a DoS attack such as SYN flood. A SYN flood exploits the TCP 3-way handshake by initialling request connections to the target server and ignoring the acknowledge (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.

3. THE CLOUD COMPUTING SECURITY ISSUES

A. 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 WS-Security uses XML signature in order to protect an element's name, attributes and value from unauthorised parties, it is unable to protect the positions in the document [7]. 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 2 and 3 illustrate an example of an XML signature element wrapping attack.

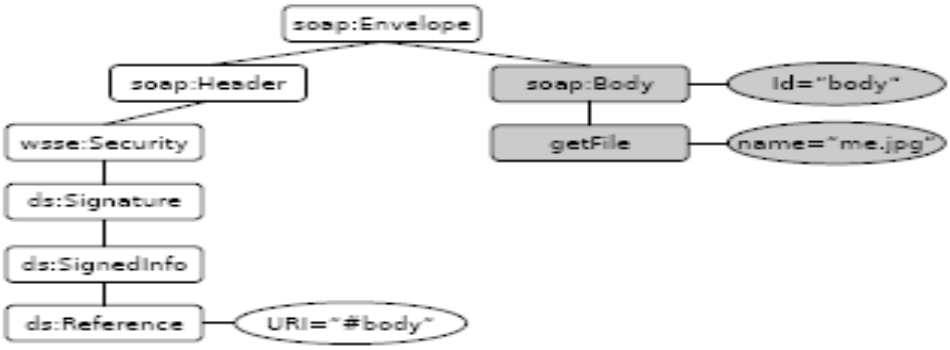

Fig. 2 SOAP message with signed SOAP body.

According to the figure 2, 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 3. 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, Amzon's EC2, which is the public cloud computing system of Amazon, was discovered that it was vulnerable to XML signature element wrapping attack [8].The possible countermeasure would be using a combination of WS-

Security 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.

B. Browser Security

In a cloud computing system, the computational processes are completed in the cloud server whereas the client side just send a request and wait 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 [6]. Marlinspike used the technique called "Null Prefix Attack" in order to perform undetected man-in-themiddle- 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.

C. 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 had 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 theclient'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.

D. Flooding Attacks

Although data transmission between a client and the server may secure, attackers might choose to attack the cloud environment directly. One of the common characteristics of the cloud system is to provide dynamically scalable resources. It offers a benefit for variability in usage. Once there are more requests from clients, cloud system automatically scale up by starting up new service instances in order to support the clients' requirements. On the other hand, this also can be a severe vulnerability of flooding attack such as DoS, which, basically, is an action of sending a large number of nonsense requests to a certain service. When an attacker performs a DoS attack to a particular service in a cloud system, cloud computing operating system realises the extra requests. It

begins to provide more service instances in order to deal with the workload. If the attacker sends more requests, the cloud system will try to work against the requests by providing more computational resources. Eventually, the system might consume all of the resources on the cloud system and be not able to provide services to normal requests from users.

Indirectly, the other service instances running on the same cloud hardware server of the target service instance may also suffer from the workload caused by the DoS attack. Once the resources of the server are almost or completely depleted, there are no resources available for other services on the same server. As a consequence, the other services also might not be able to provide their services to normal users. In terms of accounting point of view, DoS attack costs extra fees to the consumers. For instance, Amazon Elastic Compute Cloud (Amazon EC2) charges money to customers from the actual data transfer and resources usage [1]. Once a service instance running on Amazon EC2 has been attacked by DoS, the extra computational resources have been used and also there are a lot of additional data transfer between the attacker and the service instance. The service instance owner has to pay extra money to Amazon for the unexpected situation. Even though it is difficult to completely prevent DoS attacks, installing a firewall or intrusion detection system (IDS) is able to filter malicious requests from attacking the server. Nonetheless, sometimes, an IDS can mislead the administrator because it gives false alerts. It may consider normal requests as intrusive requests.

4. CONCLUSIONS

In this paper, a selection of issues of cloud computing security, XML Signature Element Wrapping, Browser Security, Cloud Malware Injection Attack and Flooding Attacks, and its potential countermeasures are introduced. It appears that the security systems of cloud computing requires an in-depth analysis because attackers may choose to exploit cloud systems via various vulnerabilities. An attacker may choose to manipulate a client's request during data transit from the client to the cloud system. This leads the attacker to gain unauthorised access to the cloud system. The attacker might try to add malicious service to the cloud system for a particular purpose which costs damage to other clients or even the could system itself. On the other hand, the attacker could attempt to stop the services on the cloud system; leading clients are unable to request services from the cloud system and the service owner has to pay extra fees to the cloud system provider for the extra requests from the attack.

5. ACKNOWLEDGMENT

I convey my honest thanks to Dr. Syed Faisal Ahmed Bukhari Chairman of Computer Engineering Department in the Sir Syed University of Engineering and Technology for providing me the leadership and conveniences for this paper. I expand my truthful gratitude to Mr. Muhammad Numan Ali Khan for his cooperation for presenting this paper. I also extend my sincere thanks to all other faculty members of Sir Syed University of Engineering and Technology and my friends for their support and encouragement.

6. REFERENCES

[1] Amazon Web Services. (2009) Amazon Elastic Compute Cloud (Amazon EC2). [Online]. Available: http://aws.amazon.com/ec2
[2] A. Mell and T. Grance. (2009) The NIST definition of cloud computing. [Online]. Available: csrc.nist.gov/groups/SNS/cloudcomputing/ cloud-def-v15.doc
[3] Cloud Security Alliance. (2009) Security guidance for critical areas of focus in cloud computing V2.1. [Online]. Available:
[4] http://www.cloudsecurityalliance.org/guidance/csaguide.v2.1.pdf
[5] D. Booth, et. al. (2004) Web service architecture. [Online]. Available:http://www.w3.org/TR/ws-arch/
[6] M. Jensen. et. al. (2009) "On Technical Security Issues in Cloud Computing" IEEE International Conference in Cloud Conouting,pp.109-116, Sep 2009.
[7] M. Marlinspike. (2009) Null Prefix Attacks Against SSL/TLS Certificates. [Online]. Available:
[8] http://www.thoughtcrime.org/papers/null-prefix-attacks.pdf
[9] M. McIntosh and P. Austel. "XML Signature Element Wrapping Attack and CounterMeasures" Workshop on Secure Web Service, pp.20-27, 2005.
[10] N. Gruschka and L. L. Iacono. "Vulnerable Cloud: SOAP Meaage Security Validation Revisited" IEEE International Conference on Web Service, pp.635-631, Jul 2009.
[11] OASIS. (2004) Web services security: SOAP message security 1.1. [Online]. Available: http://www.oasisopen.
[12] org/committees/download.php/16790/wss-v1.1-spec-os- SOAPMessageSecurity.pdf
[13] US-CERT. (2004) Understanding Denial-of-Service Attacks. [Online]. Available: http://www.us-cert.gov/cas/tips/ST04-015.html