CS 6301.005
DEVELOPING AND SECURING THE CLOUD

TERM PAPER #2
ATTACK VECTORS ON CLOUD

TABLE OF CONTENTS

1. ABSTRACT

Cloud computing improves the efficiency in many individual and business IT operations. It reduces the total computation cost by providing a shared pool of computer resources at any time over the internet. Cloud provides service in different ways as a software, infrastructure or platform.

Although cloud computing models have more advantages and performances than compared to on-site models, the cloud servers are also prone to both inside and outside attacks. Therefore, there is a vital need to take security measures to protect the user sensitive data from cyber-attacks.

In this paper, we discuss various kinds of cloud attacks which is daunting cloud developers and service providers. We'll start with an overview of key vulnerabilities in cloud services and then discuss some of the most common types of attacks in the cloud. Finally, we analyze on how to ensure the security of cloud-based solutions based on industry best practices.

2. INTRODUCTION

Cloud technology is still being actively developed, and thus it has many vulnerabilities that can be exploited by cybercriminals or malicious insiders. Let's look at the key cloud computing vulnerabilities that raise security concerns among cloud users.

Cloud API vulnerabilities: Application programming interfaces (APIs) is a medium through which cloud services allow users to interact them. API vulnerabilities have significant impact on the security of cloud provisioning, monitoring, management and cloud orchestration. Strong control implementations are in great demand over APIs, to improve security features in the cloud.

Malicious insiders: There are many ways to attack or leak data on legitimate users on cloud environments. By implementing identity and access management (IAM) techniques, the threat can be minimized.

Weak cryptography: Data encryption is generally implemented by automatically generating random numbers. In order to protect their data in storage the cloud providers use cryptographic algorithms. But they usually use limited sources of

entropy to generate cryptographic algorithms which weakens the cryptography strength.

Vulnerable cloud services: Cloud platforms are designed as distributed systems of cloud computation services. Yet these systems have little protection against other services which makes other systems vulnerable. If an attacker exploits a vulnerability in one of the cloud services, then they can gain unauthorized access to other legitimate users' data.

Data threats: Various types of data is stored in cloud environments. This data may contain about business activities or some other sensitive information about users. This data is sensitive to various attacks, data loss, breach or damage due to application vulnerabilities or unpredicted emergencies. It may not be possible to prevent all the possible data attacks or threats, but cloud providers should apply modern algorithms like encryption, cryptography while uploading data to cloud to ensure the integrity of user data.

3. APPROACH

The cyber-attacks on cloud computing mainly focus on preventing access to cloud services and data stealing. The hackers, hack into network and block the users or the services by:

- stealing users' credentials somewhere outside the cloud
- cracking user password by cookies left by application on the user browsers
- some unpatched vulnerabilities on cloud service might leave a backdoor for the attackers
- social engineering, i.e. by impersonating like a network admin etc.

3.1. *Malware Injection*

Malware injection attacks are used to take control of users' information from cloud by spreading an infected service into the cloud. Now that the cloud service is hijacked the user's data or requests are out in the open for the attacker, he can now impersonate any user and perform malicious deeds.Some of the most common attacking techniques are Cross-site scripting and SQL injection:

The XSS attack against the Amazon Web services in 2011 is done by injecting malicious scripts into the web vulnerabilities.

The Sony's PlayStation Webpage was attacked using SQL injection in 2008 by exploiting a vulnerable database application.

3.2. Misuse of cloud services

The cloud services can also be used in a malicious ways to perform various attacks.The following are some of the examples.

In DOS attacks, cloud services can be used to block a client or a company it's access rights. For example the attack using Amazon's EC2 in 2010 where the company was blocked of it's access just using 6$.

In Brute force attacks,The cloud servers could be utilized to perform repeated password trails to crack an user account as demonstrated in Black Hat Technical Security Conference, 2011

3.3. *Denial of service*

Denial of service attacks on cloud are done by filling the server space and service requests, which makes the cloud services not accessible to the users. This effect very wide spread since cloud provides services to various users, companies,etc as even if one of the servers is down it will have a huge impact on more than one company or users. Distributed Denial of Service is even more destructive as it might overload the servers causing permanent failures.

3.4. *Side channel*

In this attack malicious virtual host is deployed on the same platform as the target and observers pattern ike power, cryptographic implementations and electromagnetic leaks to gather information to perform attacks.This can be avoided by using a secure system.

3.5. Wrapping

The cloud users must make a connection with the cloud service provider before accessing the data. This is secured by using XML signature for authentication, but it still leaves gap by not securing the credentials position. In this attack the signature is wrapped and modified accordingly to gain access.

In 2009, a vulnerability was found in Amazon(EC2) interface allowing the attacker modify its content as a successful signature wrapping attack.

3.6. Man-In-The-Cloud

Man In The Cloud attack is similar to Man In The Middle attack but the attacks are performed using vulnerabilities in synchronization tokens. This token can be used by the attackers to use it for authentication during next synchronization with the cloud,allowing attackers to gaining access to the cloud. The user won't notice that his account has been compromised.

3.7. Insider Attack

An employee or a client which has access to the company resources making use of access out of the defined security policy is called a Insider attack. The only way to prevent this attack is build secure access control policies and assign different levels of access to the users according to the roles assigned.

3.8. Hijacking Account or Service

Various methods like rootkits,viruses,cookie hijacking, session hijacking are used to get access to an user's account or exploit a service. The attacker can also leverage users sensitive information. In 2007 an employee became a victim of account hijacking through the use of a phishing attack, and later the attacker increased the privileges of the account to steal all the data.

3.9. Advanced Persistent Threats (APTs)

This attacks is used to exploit vulnerabilities to continuously gather sensitive data from cloud. This can be an open attack or can be done without the notice of the users. This allows attacker to exploit and adopt the security measures in place to gain further access into the network.

3.10. Meltdown and Spectre

These attacks utilize vulnerabilities in processors to read encrypted data using javascript. The two threats Meltdown and Spectre utilizing the above mentioned technique it become a big threat to the cloud. These attacks mentioned above

breaks the isolation the applications and platform, allowing attackers to freely retrieve information from the kernel. This has been a problem, as most cloud users neglect the latest security patches.

4. ANALYSIS

By providing a layered security approach, cloud providers can protect the data in a best way. Best industry practices should be implemented to maximum limit possible to increase the security in cloud. Dynamic nature of cloud services always compromises the security provided by the on-site software. Although a cloud provider can't ensure the total security in cloud, they can follow some tips mentioned below to ensure the security of cloud-based solutions.

4.1. Boost up security policies

Software vendors should limit the scope of their responsibility for protecting user data and operations in the cloud in their security policies when providing cloud services. Clients should be informed about how security measures should be taken from their side.

4.2. Strong authentication

Cloud developers should implement strong authentication and identity management as stealing passwords is the most common way to access user data. Establish multi-factor authentication. Static and dynamic passwords are used by various cloud tools. Dynamic passwords are much handy to confirm user's credentials using biometric systems, one time password, cryptographic tokens etc.,

4.3. Access management

Cloud developers should let cloud users assign role-based permissions to different administrators to increase the security of services, so that users only have the capabilities assigned to them. Privileged users can establish scope and permission for other users according to their duties in the company.

4.4. Data Protection

Data Encryption should be done before uploading it to the cloud. The effective defense against account hijacking in modern data is encryption and tokenization technologies. To effectively deflect cyber-attacks, use strong encryption algorithms that contain salt and hashes. Data backup service should be provided for every data that is uploaded to cloud server.

4.5. Intrusion Detection

Fully developed intrusion detection should be deployed on cloud based solution. It can detect and inform if there is any malicious activity by intruders in cloud. The intrusion detector should be able to monitor over the network and notify on unusual activity in cloud.

4.6. APIs Protection

Cloud applications should be accessible to clients through secure APIs. For secure APIs it requires IP address range limitation or providing access through VPNs or corporate networks. This perspective might be difficult for implementation of public facing applications. Thus, secure APIs can be implemented while using specific templates or scripts only. There is a vast scope for developing APIs with security protection.

5. CONCLUSION

Cloud services have become very popular in the recent past because of its many advantages. Nevertheless, the cloud platform also has many vulnerabilities and security issues that can be a host for the cyber-attacks. By thinking in the line of how cyber crimes are committed on cloud services, the cloud developers can better protect their services. As cloud computing is on the rise, and especially due to its enormous attraction to organized criminals, we can expect to see a lot of security incidents and new kinds of vulnerabilities around it within the decades to come. This paper gives a first step towards classifying them, thus making them more concrete and improving their analysis. Using the notion of attack surfaces, we illustrated the developed classification taxonomy by means of four up-to-date attack incidents of cloud computing scenarios. Being a work-in-progress, we will continue with the collection and classification of cloud-based attacks and

vulnerabilities in order to prove or refute our attack taxonomy's applicability and appropriateness.

6. REFERENCES

- https://www.apriorit.com/dev-blog/523-cloud-computing-cyber-attacks
- https://www.globaldots.com/cloud-attack-vectors/
- https://ieeexplore.ieee.org/document/7423296
- https://pdfs.semanticscholar.org/95c0/ae8181bbd949b69d23b5672038fdf4e4a3d7.pdf