Asian Journal of Computer Science and Technology
ISSN 2249-0701 Vol. 4 No. 2, 2015, pp.31-34

Proactive Measures on Account Hijacking in Cloud Computing Network

A.Annie Christina
Hindustan University, Chennai, Tamil Nadu, India
E-mail: anniechristinaa@gmail.com

***Abstract* - The development of cloud computing services is speeding up the rate in which the organizations outsource their computational services or sell their idle computational resources. Even though migrating to the cloud remains a tempting trend from a financial perspective, there are several other aspects that must be taken into account by companies before they decide to do so. One of the most important aspect refers to security: amongst these security and trust issues, the user's data has to be released to the cloud and thus leaves the protection sphere of the data owner. This paper focuses on various security issues arising from the usage of cloud services and especially hijacking of account/service the user of cloud computing arena. It also discusses basic proactive measures that can be taken to prevent or in other words minimize to the stealing of the user account details and services.**
Keywords: Cloud computing; cloud security; threats; attacks

I. INTRODUCTION

The "cloud" is a set of different types of hardware and software that work collectively to deliver many aspects of computing to the end-user as an online service. Cloud Computing is the use of hardware and software to deliver a service over a network (typically the Internet) [1] . With cloud computing, users can access files and use applications from any device that can access the Internet. An example of a Cloud Computing provider is Google's Gmail. Gmail users can access files and applications hosted by Google via the internet from any device.

Cloud computing [2] poses privacy concerns because the service provider can access the data that is on the cloud at any time. It could accidentally or deliberately alter or even delete information. Many cloud providers can share information with third parties if necessary for purposes of law and order even without a warrant. That is permitted in their privacy policies which users have to agree to before they start using cloud services. Solutions to privacy include policy and legislation as well as end users' choices for how data is stored. Users can encrypt data that is processed or stored within the cloud to prevent unauthorized access.

According to the Cloud Security Alliance, the top three threats in the cloud are "Insecure Interfaces and API's", "Data Loss & Leakage", and "Hardware Failure" which accounted for 29%, 25% and 10% of all cloud security outages respectively — together these form shared technology vulnerabilities. In a cloud provider platform being shared by different users there may be a possibility that information belonging to different customers resides on same data server.

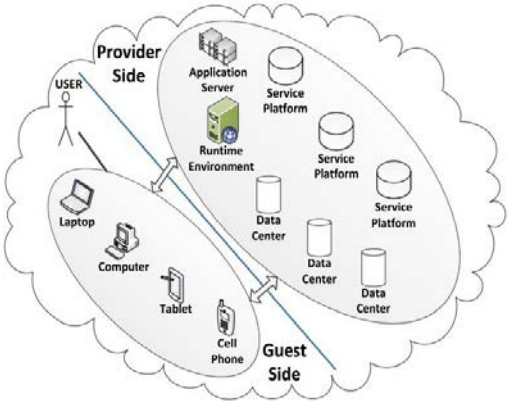

Fig.1 Guest and Provider side of cloud computing

Therefore, Information leakage may arise by mistake when information for one customer is given to other. Because data from hundreds or thousands of companies can be stored on large cloud servers, hackers can theoretically gain control of huge stores of information through a single attack — a process called "hyperjacking".

Physical control of the computer equipment (private cloud) is more secure than having the equipment off site and under someone else's control (public cloud). This delivers great incentive to public cloud computing service providers to prioritize building and maintaining strong management of secure services. Some small businesses that don't have expertise in IT security could find that it's more secure for them to use a public cloud. There is the risk that end users don't understand the issues involved when signing on to a cloud service (persons sometimes don't read the many pages of the terms of service agreement, and just click "Accept" without reading).

This is important now that cloud computing is becoming popular and required for some services to work, for example for an intelligent (Apple's Siri or Google). Fundamentally private cloud is seen as more secure with higher levels of control for the owner, however public cloud is seen to be more flexible and requires less time and money investment from the user.

II. SECURITY THREATS IN CLOUD

A.Data Breaches

A data breach is an incident that involves the unauthorized or illegal viewing, access or retrieval of data by an individual, application or service. It is a type of security breach specifically designed to steal and/or publish data to an unsecured or illegal location. A data breach occurs when an unauthorized hacker or attacker accesses a secure database or repository. Data breaches are typically geared toward logical or digital data and often conducted over the Internet or a network connection.

A data breach may result in data loss, including financial, personal and health information. A hacker also may use stolen data to impersonate himself to gain access to a more secure location. For example, a hacker's data breach of a network administrator's login credentials can result in access of an entire network.

B. Data Loss

A data breach is the result of a malicious and probably intrusive action. Data loss may occur when a disk drive dies without its owner having created a backup. It occurs when the owner of encrypted data loses the key that unlocks it. Small amounts of data were lost for some Amazon Web Service customers as its EC2 cloud suffered "a remirroring storm" due to human operator error on Easter weekend in 2011. And a data loss could occur intentionally in the event of a malicious attack.

C.Account Hijacking

Account hijacking, hackers hijacking your account. This sounds to be a concern in the cloud. Phishing[10], exploitation of software vulnerabilities such as buffer overflow attacks, and loss of passwords and credentials all lead to the loss of control over a user account. An intruder with control over a user account can eavesdrop on transactions, manipulate data, provide false and business-damaging responses to customers, and redirect customers to a competitor's site or inappropriate sites.

D.Insecure API's

The cloud era has brought about the contradiction of trying to make services available to millions while limiting any damage all these largely anonymous users might do to the service. The answer has been a public facing application programming interface, or API, that defines how a third party connects an application to the service and providing verification that the third party producing the application is who he says he is.

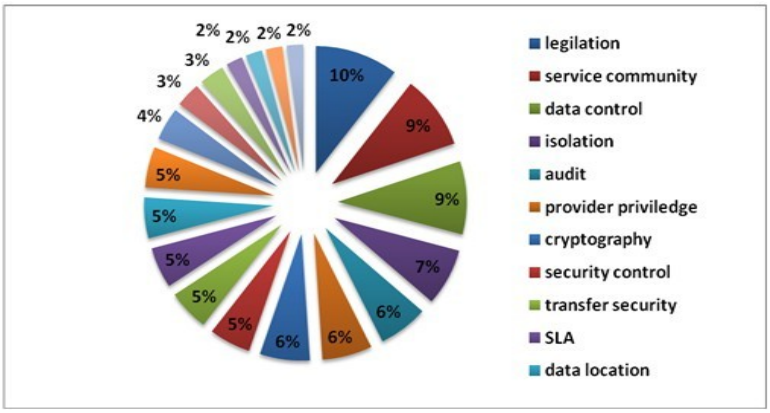

Fig.2 Security problems at different levels

E. Denial of Service

Denial of service attacks are an old disrupter of online operations[3], but they remain a threat nevertheless. The assault by hundreds of thousands or millions of automated requests for service has to be detected and screened out before it ties up operations, but attackers have improvised increasingly sophisticated and distributed ways of conducting the assault, making it harder to detect which parts of the incoming traffic are the bad actors versus legitimate users.

F. Malicious Insider

Malicious insiders might seem to be a common threat. If one exists inside a large cloud organization, the hazards are magnified[12]. One tactic cloud customers should use to protect themselves is to keep their encryption keys on their own premises, not in the cloud. "If the keys are not kept with the customer and are only available at data-usage time, the system is still vulnerable to malicious insider attack. Systems that depend solely on the cloud service provider for security are at great risk from a malicious insider.

G. Abuse of Cloud Services

Cloud computing brings large-scale, elastic services to enterprise users and hackers alike. It might take an attacker years to crack an encryption key using his own limited hardware. But using an array of cloud servers, he might be able to crack it in minutes. Or hackers might use cloud servers to serve malware, launch DDoS attacks, or distribute pirated software.

H. Insufficient Due Diligence

Without an understanding of the service providers' environment and protections, customers don't know what to expect in the way of incident response, encryption use, and security monitoring. Not knowing these factors means organizations are taking on unknown levels of risk in ways they may not even comprehend, but that are a far departure from their current risks.

Enterprises may push applications that have internal on-premises network security controls into the cloud, where those network security controls don't work. If enterprise architects don't understand the cloud environment, their application designs may not function with proper security when they're run in a cloud setting.

I. Shared Technology

In a multi-tenant environment, the compromise of a single component, such as the hypervisor, exposes more than just the compromised customer; rather, it exposes the entire environment to a potential of compromise and breach. The same could be said other shared services, including CPU caches, a shared database service, or shared storage.

The cloud is about shared infrastructure, and a misconfigured operating system or application can lead to compromises beyond their immediate surroundings. In a shared infrastructure, the CSA recommend an in-depth defensive strategy[13]. Defenses should apply to the use of compute, storage, networking, applications, and user access. Monitoring should watch for destructive moves and behaviors.

III. ACCOUNT HIJACKING

In this type of security breach, hackers seek to hijack the account by stealing the security credentials and then eavesdropping on the activities and transactions of users. The hackers can also manipulate the data, insert false information and redirect the clients to illegitimate sites.

This type of vulnerability is particularly scary because hackers are able to use the reputation and the trust users have built up to manipulate the clients. In 2010, Amazon faced an attack[14][15] that allowed hackers to steal the session IDs that grant users access to their accounts after entering their passwords. This left the client's credentials exposed to the hackers. The bug was removed 12 hours after it was discovered, but many Amazon users unknowingly fell for the attack during that time.

A. Ways of hijacking

In account hijacking, a hacker uses a compromised email account to impersonate the account owner. Typically, account hijacking is carried out through phishing[10], sending spoofed emails to the user, password guessing or a number of other hacking tactics. In many cases, an email account is linked to a user's various online services, such associal networks and financial accounts. The hacker can use the account to retrieve the person's personal information, perform financial transactions, create new accounts, and ask the account owner's contacts for money or help with an illegitimate activity.

Cloud account hijacking is a common tactic in identity theft schemes. The attacker uses the stolen account information to conduct malicious or unauthorized activity. When cloud account hijacking occurs, an attacker typically uses a compromised email account or other credentials to impersonate the account owner.

B. Implications on business

Cloud account hijacking at the enterprise level can be particularly devastating, depending on what the attackers do with the information. Company integrity and reputations can be destroyed, and confidential data can be leaked or falsified causing significant cost to businesses

or their customers. Legal implications are also possible for companies and organisations in highly regulated industries, such as healthcare, if clients' or patients' confidential data is exposed during cloud account hijacking incidents.

IV. PROACTIVE MEASURE ON ACCOUNT HIJACKING

Account Hijacking is commonly witnessed by the users of cloud computing network. Even though the cloud providers take at most initiative and attention in this regard[16], yet the hackers find their way in hijacking the user account. Below mentioned are few proactive measures that can be taken in preventing exposure to the security threats caused by hackers/intruders:

a. Setting up protocol that provide sharing account credentials between employees or services.
b. Using a strong two-factor authentication technique and track employee use of the platform for unauthorized activity.
c. Utilizing a secure encryption management system, such as that offered by venfi, should also be prioritized and developed specifically for use with a cloud platform.
d. In high confidential data storage, prohibit the sharing of account credentials between users and services.
e. Leverage strong two-factor authentication techniques are possible.
f. Employ proactive monitoring to detect unauthorized activity.
g. Understanding cloud provider security policies and SLAs, before singing in a cloud network

These measures can reduce the exposure of client account details and data leakage to malicious insiders or external hacker threats. Organizations should be aware of these techniques a s well as common defense in depth protection strategies to contain the damage (and possible litigation) resulting from a breach.

V. CONCLUSION

Cloud computing is now the big wave in computing. It has many benefits, such as better hardware anagement, since all the computers are the same and run the same hardware. It also provides for better and easier management of data security, since all the data is located[9] on a central server, so administrators can control who has and doesn't have access to the files. It is widely accepted today because of its economic benefits.

There are some down sides as well to cloud computing. Out of those down falls one of the major factors is security. User will have to evaluate the security model that is been used by Cloud Provider makes lot of impact on taking the decision of the selecting the cloud provider. Also for Cloud Computing there is more number of threats than compare to security of single PC because clouds have many elements than single PC.

The user of cloud network need to be aware of the security threats as they enjoy the provisions of the network. When the provider and user take measures to prevent these threats, hijacking of account or any threat can thus be minimized considerably.

REFERENCES

[1] http://www.csrc.nist.gov/groups/SNS/cloud- computing /cloud-computing-v26.ppt.
[2] http://arielsilverstone.com/category/cloud- computing-security/
[3] Denail of Service, http://en.wikipedia.org/ wiki/ Denial-of-service_attack.
[4] Muhammad Kazim and Shao Ying Zhu, " A survey on top security threats in cloud computing", IJASCSA, International Journal of Advanced Computer Science and Application, vol 6,N0.3, 2015.
[5] Zeus Botnet, http://en.wikipedia.org/wiki/ Zeus_ (trojan_ horse).
[6] Yexia Cheng, Yuejin Du, JunFeng Xu, Chunyang Yuan, "Cloud Computing and Intelligent Systems (CCIS)", 2012 IEEE 2nd International Conference on (Volume:01) Oct. 30 2012-Nov. 1 2012 Page(s):459- 465.
[7] Ping Wang, Wen-Hui Lin ; Pu-Tsun Kuo ; Hui-Tang Lin, "Computing Technology and Information Management (ICCM)", 2012 8th International conference, IEEE conference, Vol.1, 24-26 April 2012, pp. 106-111.
[8] M. D. Ernst. "Static and Dynamic Analysis: Synergy and Duality", In Proceedings of the Program Analysis for Software Tools and Engineering (PASTE 2004) Workshop, pp. 24–27, June 2004.
[9] Peter Oehlert. "Violating Assumptions with Fuzzing", IEEE Security & Privacy, pp. 58-62, March/April 2005.
[10] T. Moore and R. Clayton, "Examining the impact of website take-down on phishing", In Anti- Phishing Working Group eCrime Researcher's Processes-laws_blog/AWS_Security_Whitepaper Summit (APWG eCrime), pp. 1–13, ACM Press, New York, 2007.
[11] Hypervisor,http://en.wikipedia.org/wiki/Hypervis or.
[12] Meiko Jensen, J¨org Schwenk and Nils Gruschka, Luigi Lo Iacono, "On Technical Security Issues in Cloud Computing", IEEE International Conference on cloud computing,2009.
[13] Securing Microsoft's Cloud Infrastructure - http://www.globalfoundationservices.com/security/ documents/ SecuringtheMSCloudMay09.pdf
[14]Amazon Web Services: Overview of Security Processes-aws_blog/AWS_Security_Whitepaper2008_09.pdf.
[15]Amazon uses HackAlert™ - http://malwareinfocom/ mal_faq_hackalert.html.
[16] "Cloud Computing - Benefits, risks and recommendations for information security", November 09 ByENISA.