Risk Issues at the End of Cloud Service Provider

Adesh kumar
SLBSRSV New Delhi India

Abstract- The Cloud computing has many benefits but along with benefits cloud computing brings many risk issues along with it. The cloud computing add new risk to the already existing risk inherited by traditional system. Virtualization in cloud computing invites new risk in cloud computing. There are many risk in cloud computing but in this paper i will cover only risks which are supposed to be at service provider's end.

Keywords- cloud computing, risk, Virtual Machine

I. INTRODUCTION

Cloud computing is the latest technique which is supposed to be future of computing through internet. In cloud computing various hardware and software resources are provided to the user on rent basis along with uses basis. Beacase computer resources are shared by many users so many risk issues arises with the benefits of cloud computing. Here I discuss the various issues which arise at the end of service provider.

II. RISK ISSUES

1. *Risk due to multi layer design of Virtual Machine*-

   Virtual machine increases the complexity of network by adding more layers. Hence it increases the risk of improper configuration and therefore can be suffer by unseen vulnerabilities.

2. *Risk due to privilege escalation*-

   A hacker can increases its privileges on a system by taking the advantage of virtual machine. The hacker can use hypervisor to take control of higher level from lower level to attack a virtual machine.

3. *Risk due to inactive virtual machine*-

   All virtual machines may not be active all the time and inactive virtual machine contains sensitive data. It is impossible to monitor the access of the sensitive date stored in those inactive virtual machines. The tools which are used for virtual machine systems are not as mature as tools used in tradition system but we expect that tools will be improve quickly.

4. *Risk due to non separation of duties*-

   The virtual machine provides many access and authorization to different types of users. The separation of authorization of all users is very difficult to maintain. There is always risk of improper definition of different user access roles.

5. *Risk due to Poor access control*-

   The hypervisor of virtual machine is responsible for interaction between various hardware and virtual machine. So it creates new single point of vulnerability at its interaction point. Hence the hypervisor can exposed trusted network through improper design of access control.

6. *Back door attack*-

   A back door attack happens when using dial up modem or asynchronous external connection. A hacker can gain access to the network bypassing of control mechanism through a Back Door such as modem

7. *IP spoofing*-

   A hacker can use IP spoofing to gain unauthorized access of the system. IP spoofing convinces the trusted system that hacker is an authorized user of the trusted system. IP spoofing takes place at the TCP level by changing a packet. The intruder sends a packet with an IP address of a known and trusted host instead of IP address of itself.

8. *Man in the middle*-

   Man in the middle is a type of attack in which a hacker secretly read and modifies the messages which are communicating between two parties. The two parties never know that their communication is being read by third person. The two parties always think that they are communicating directly.

9. *Replay attack*-

   A replay attack is the attack in which a attacker steal the messages of some sender and then sends those messages later to receiver repeatedly. Because messages are encrypted so receiver thinks that those messages are intended for it and then reply accordingly.

10. *TCP hijacking attack-*

    TCP hijacking is a process in which a hijacker steals a session which is going on between a network server and a trusted client. The hijacker replaces client IP address by its own IP address and network server think that it is communicating with authorized client.

11. *Social engineering attack*-

    In social engineering a attacker uses social platform to steal password, PIN and other sensitive information from trusted user. The attacker uses telephonic calls, Emails and other social means to interact with trusted user of a network system and convince the user so powerfully that user provide their password and other means of authorization to hacker knowingly or unknowingly.

12. *Dumpster diving attack*-

    Dumpster diving is a technique by which a hacker retrieve sensitive information from deleted data and used that information to take control network server. The hacker search trash for valuable information such as credit card information, password, PIN, technical manuals etc.

13. *Password guessing attack*-

    Password guessing attack is the most common mechanism used for attacking a system. Password guessing can be done by gaining date of birth of the person and gaining other private information by social engineering. Other methods are also used for guessing password such as trying all combination of letters, numbers and symbols. The most common technique used to prevent password guessing is to limit the password input attempts.

14. *Trojan Horses and Malware attack-*

    Trojan horses are the programs which contain malicious code inside them. The pretend to be useful program but when they are run by user the malicious code written inside them get executed and attack system in many ways. Trojan horses are distributed in many ways like website, Email, downloadable applets etc.

III.CONCLUSION

There are lot of risk issues in latest technology of cloud computing. In this paper I tried to identify some important risk issues which should be addressed at service provider's end in the cloud computing. The risks are not limited to mention in this paper. There may be other risk issue related to service provider.

REFERENCES

[1] R. L. Krutz and R. D. Vines, "Cloud Security: A Comprehensive Guide to Secure Cloud Computing", Wiley Publishing, pp.147-149, 2010

[2] Cloud Computing Security. A Trend Micro White Paper, pp.2-10, May 2010

[3] S. O. Kuyoro, F. Ibikunle, and O. Awodele,"Cloud Computing Security Issues and Challenges" International Journal of Computer Networks (IJCN), Volume (3), Issue (5), pp.247-254, 2011

[4] W. Jansen,And T. Grance, DRAFT: Guidelines on Security and Privacy in Public Cloud Computing, NIST, U.S. Department of Commerce, Special Edition 800-144, pp.9-15,January 2011