Journal of Computations & Modelling, vol.6, no.3, 2016, 87-103
ISSN: 1792-7625 (print), 1792-8850 (online)
Scienpress Ltd, 2016

A review of wireless hacking techniques that affect the security of cloud systems

Basant Kumar[1], Joseph Mani[2] and Prem Chand Akunuru[3]

Abstract

Cloud is one of the promising technologies that has enabled the massive growth of Internet-based services, from search to streaming media to offline storage of individual data as well as the background processing capabilities that enable mobile Internet devices. Security is recognized as a prevalent function but unfortunately, security threats have become a major challenge in cloud. There are several hacking systems used by hackers in order to attack the cloud system. Here, this study reviews about the wireless hacking techniques that affect the security of cloud systems. In particular, this study reviews about four main hacking techniques such as account hijacking attack, denial of service (DoS) attack, wrapping attack and cloud malware injection attack. This study also concludes that, even though, there are numerous solutions available in practice to overcome these attacks, wireless hacking techniques are still upsetting the security of cloud systems at a greater extent.

[1] Modern College of Business & Science. Department of Computer Science, Muscat, Sultanate of Oman. E-mail: basant@mcbs.edu.om
[2] Modern College of Business & Science. Department of Computer Science, Muscat, Sultanate of Oman. E-mail: drjosephmani@mcbs.edu.om
[3] Genpact, Oracle DBA, USA.E-mail: Premc2k@yahoo.com

Article Info: *Received* : May 18, 2016. *Revised* : June 5, 2016.
Published online : October 1, 2016.

Keywords: Cloud systems; account hijacking attack; denial of service attack; wrapping attack; cloud malware injection attack; security

1 Introduction

Cloud acts as one of the significant milestones in the history of computers. Cloud provides several opportunities and potential benefits but unfortunately, it also poses several kinds of risks and issues. Security of cloud becomes one of the challenging issues. Several security mechanisms have been developed in order to prevent and avoid several attacks and also to protect cloud systems. At the same time, hackers are also finding new ways to attack cloud systems. Nowadays, cloud systems are increasingly affected by several types of wireless hacking techniques. It is not possible for hackers to attack the cloud system with one-step procedure and it needs several techniques to be used in combination to attack the system. Attacks can be targeted against both the wireless and wired networks [1]. Here, this study reviews only about the wireless hacking techniques that affect the security of cloud systems.

2 Aim and objectives

2.1 Maintaining the Integrity of the Specifications

The main aim of this research is to review about various wireless hacking techniques that affect the security of cloud systems.

2.2 Objectives

- To identify various types of attacks that affect the cloud

- To analyze the motive behind each of the attack
- To review the solutions available at present to mitigate and overcome such attacks.

3 Literature review

3.1 Types of wireless hacking techniques that affect the cloud

• **Account Hijacking Attack**: Account hijacking is undertaken with stolen credentials [2]. Attackers can attack sensitive information and compromise the integrity, availability and confidentiality of services provided [3]. Such attack instances are eavesdropping on sensitive/transaction activities, manipulation of data redirection to illegitimate sites and returning falsified information [4].

• **Denial of Service Attack**: Denial of service attack the attacker attempts to hinder the legal users to access cloud resources [5]. The bulk messages are sent by attacker in this attack asking the server to check the requests. [6] has mentioned that DOS attacks has been associated with distributed attacks of flooding infrastructure of network layer with huge number of traffic to cause essential components to consume or to fail available resources of hardware. DOS attack is hindered by using prior automatic switch offering the analysis of packet rate [7].

• **Wrapping Attack**: Wrapping attacks use extension markup language signature wrapping to determine the weakness when the servers of web validate signed requests [8]. Extension Markup Language wrapping attacks have been demonstrated against a public infrastructure successfully as a service cloud [9]. Policies of security for fending wrapping attacks. They evolved a formal structure for verification of policy and derived an advisor of policy for testing and producing policies of security [10].

• **Cloud Malware Injection Attack**: The attack of malware injection is one of the web based attacks classification in which hackers use vulnerabilities of web

application and embed hostile codes into it that alters the course of its usual implementation [11]. Hackers work on a malicious program, VM (virtual machine) and program and inject them into target service cloud models namely IaaS (infrastructure as a service), PaaS (platform as a service) and SaaS (software as a service) [12]. An interpolar is obligatory to produce his or her personal application, virtual machine or service request and apply it into the structure of cloud [13].

3.2 Motive behind the wireless hacking techniques that affect the cloud

The different types of attacks in the cloud are: 1) account hijacking attack; 2) cloud malware injection attack; 3) wrapping attack; and 4) denial of service attack. Each of these security problems in cloud systems are explained with their root causes.

- **Account Hijacking Attack**: Stolen evidence acts as the major factor to hijack the account of individuals. Attackers are using many tactics to hijack the account based on these stolen proofs [14]. Hackers are attacking in different area such as the data manipulation, return of false information, redirect the victim's to non-official websites, listening the private conversation of others and exploring the false information. The defect in Google's Gmail password recovery options stand as a big advantage for the hackers to steal the account. The hackers mislead the system by redirecting the victim's account to the fake voice mail box which has the tendency to answer the phone call. Sometimes both the victim and the hacker are operating the same account and the information of the victim is traced by the hackers. He also pointed that most of the victims are using the same passwords to access their different accounts which enhances the account hijacking in cloud systems [15].

Stolen credentials are used by the hackers to attack the cloud system. Authors have analyzed that the passwords and the usernames are stolen by the hackers to access the drop box account [16]. Further the attackers are using the stolen password to access the account of an employee to attain the goal. The voice mail box is also used by the hackers who have the tendency to answer the calls automatically [17].

- **Denial of Service (DOS) Attack**: The hackers are trying to prevent the user from manipulating data in the cloud system. Hackers are sending a lot of messages to verify the request of the server [18]. The hackers return the invalid address on connecting with the server and these return address of the hackers are not found by any network and the server [19]. Hackers are sending many numbers of original messages with the invalid address [20]. This activity causes the major trouble to the network and server which does not allow the user to access the data easily and adds lot of congestion to the data.

The resources of network bandwidth are transferred between the user and the server in the cloud based infrastructure [21]. The increase of delay can be affected the cloud based web applications. SLA services are provided to the consumer through cloud system which often causes violation in the form of payment [22].

- **Wrapping Attack**: XML signature is hacked by using the wrapper through the web server which causes destruction in cloud system [23]. The attacker inserts the prepared malicious code elements into the server and then copies the original SOAP messages for illegal access. The cloud system is attacked by the hackers by using this technique [24].

Client request services communication through web server is done by using the Simple Object Access Protocol (SOAP) messages. These messages are converted in to the format of Extensible Markup Language (XML) through the Hyper Text Transfer Protocol (HTTP) [25]. Web Service security (WS-Security) is act as a security mechanism to transmit the SOAP messages to both the clients and the server. These services are using the digital signature to obtain the signed

messages. The content of the information is encrypted by using the encryption technique. The signed requests are verified by the web servers and hence it is considered as the big advantage for the hackers to rewrite the XML signature [26]. This wrapping attack occurs during the transformation of SOAP messages between the user and the server. The hackers alter the original account of user into the duplicate format and then they steal the original message by using the wrapper. Hackers use malicious code to replace the original content of the message and send the original message to the web-server [27]. The body of original message is still acceptable in the user side but there is some illusion occurred in the server area due to the alteration of the messages. Finally the hacker is able to access the planned operations in unauthorized format. Author also has pointed that the wrapping attacks are harmful to the cloud systems.

- **Cloud Malware Injection Attack**: The injection of evil code through Saas, Iaas and Paas module is used by the hackers to create destruction to the cloud-server system. Many original documents of the user are attacked by the hacker using this malware injection attack [28]. The type of attack occurs in the bank applications of cloud system. This malware injection attack has the tendency to return the original instances in to an adversary code which also causes destruction to the cloud server system [29].

The hackers aim to inject the malicious service or virtual machine in the cloud system. There are two types of modules used in the cloud malware injection [30]. They are malicious implementation service (Saas or Paas) and instance of virtual machine (Iaas) and hence act as an opponent to the web-server. This adversary creates some illusion to the valid evidences programmed in the cloud system. As a result of this act, the cloud system substitutes the original requests of the user into harmful terms and proceeds to execute the malicious code. The main aim of the hackers are to inject their arranged copy of harmful instances in to the victim’s service. Further they gain control over the user’s evidence in the cloud system. The hackers are controlling the cloud to attack the security domains of

service instances [31].

The cloud malware injection attack plays an important role in affecting the cloud server infrastructure than other attacks [32]. Malicious code is injected to the cloud system to destroy the victim's instances. The security of service instances are controlled and attacked by the hackers in cloud system through this attack [33].

3.3 Solutions to overcome wireless hacking techniques

In order to prevent the account hijacking attack drop box has implemented 2 factor authentications into the security controls of organization. Two factor authentication also referred as strong authentication is referred as a user entering in 3 properties to ensure her or his identity something which the user knows, something the user has and/or something the user is.. The account hijacking is also be prevented by restricting the account credentials sharing between services and users, employ proactive supervision to predict unauthorized activity, leverage strong 2 factor techniques of authentication where possible and perceive the security policies of cloud provider and service level agreements. Similarly denial of service attack can be resolve by reducing the user privileges that are linked to a server [34]. This will help decrease the denial of service attack. Specialized hardware such as load balances, intrusion prevention devices and firewalls is in place to handle volume based DOS attacks [35].

The attack of malware injection can be hindered by using the system architecture of FAT (File Allocation Table) [36]. From the file allocation table the code or application which is getting executed by the customer can be traced well in advance. Another way to resolve the attack of malware injection is to store a hash value on actual service file of instance image [37]. By carrying out an integrity check between the new service instance and original images malicious instances can be recognized. For extension markup language signature wrapping attacks on

services of web different techniques have been suggested to fix the vulnerability predicted in extension markup language based techniques [38]. For instance Extension Markup Language scheme hardening technique is used to empower the extension markup language schema declarations. A subset of Extension path known as FastXPath is suggested to resist the elements of malware which attackers insert into the structure of simple object access protocol message [39].

Comparison of Attacks								
Name of the attack	**Account Hijacking Attack**	**Author and year**	**Denial of Service Attack (DOS)**	**Author and year**	**Wrapping Attack**	**Author and year**	**Cloud Malware Injection Attack**	**Author and year**
Process	Account of user is hacked from cloud for unauthorized access Stolen credentials are used by the attackers for illegal process	Raghavendra, Lakshmi and Venkateswarlu; (2015) Barron, Yu and Zhan; (2013)	Prevention of accessing the data in cloud Creating the collision of signal to attack the cloud system	Kumar and Nithya; (2014) Booth, Soknacki and Somayaji; (2013)	Hacking of original message from cloud system using wrapper Hiding of data from the server in cloud system	Chou ; 2013 Priyanka and Kaswan; (2014)	Adversary data is injected to attack the cloud system Injecting some malicious code to attack the original data in cloud Created copy of the hacker destructs the function of cloud system	Siva and Krishna; (2013) Singh and Shrivastava; (2012) Gruschka and Jensen; (2010)

Comparison of Attacks								
Name of the attack	**Account Hijacking Attack**	**Author and year**	**Denial of Service Attack (DOS)**	**Author and year**	**Wrapping Attack**	**Author and year**	**Cloud Malware Injection Attack**	**Author and year**
Motive behind the attack	Theft of data is the main source for hacking.	Raghavendra , Lakshmi and Venkateswarlu; (2015)	Hackers are using many invalid addresses to make the server in traffic. Increasing the access time to the cloud server	Kumar and Nithya; (2014)	Stealing of data from an authorization which also causes trouble to the cloud system. Tracking the XML signature from cloud system	Chou ; 2013	Destruction of valid requests in cloud system	Siva and Krishna; (2013)
	Returning the invalid information to cloud server	Barron, Yu and Zhan; (2013)		Booth, Soknacki and Somayaji; (2013)		Priyanka and Kaswan; (2014)	Destruction of Security domain service in cloud	Singh and Shrivastava; (2012)
							Attacking the Evident service security in cloud	Gruschka and Jensen; (2010)

Comparison of Attacks								
Name of the attack	**Account Hijacking Attack**	**Author and year**	**Denial of Service Attack (DOS)**	**Author and year**	**Wrapping Attack**	**Author and year**	**Cloud Malware Injection Attack**	**Author and year**
Solution For Attack	Alteration of passwords and administrative accounts in cloud system.	Raghavendra, Lakshmi and Venkateswarlu; (2015)	Packet rate analysis is done by using the prior automatic switches.	Kumar and Nithya; (2014)	Digitally signed alteration can be done in SOAP messages.	Chou ; 2013	Breaking privacy is used to prevent attack from the hackers	Siva and Krishna; (2013)
	Use of strong authentication scheme like biometric activities prevents from attacking	Barron, Yu and Zhan; (2013)	Merging strategy in clouding prevents the attack	Booth, Soknacki and Somayaji; (2013)	Certificate of self-signed and public certificate registration are used to protect the documents from the hackers	Priyanka and Kaswan; (2014)	Original service instances can be stored by using the hash value.	Singh and Shrivastava; (2012)
							Reinitializing of protocol prevents attack from hackers	Gruschka and Jensen; (2010)

4 Discussion

This study discusses about the different techniques of wireless hacking that affect the security of cloud systems. Cloud computing is a next big wave in computing. Most of the cloud vendors claim falsely to offer secure computation environments and data for users of cloud. Nevertheless, emphatic and effective steps needs to be inducted at greater extents instead of leaving it to individual firms. The hijacking of account and service with stolen credentials is considered as a major threat. The attackers can always use deployed services critical areas of cloud computing permitting them to compromise integrity, availability and confidentiality of those services (Moore and Clayton, 2007). Cloud is vulnerable to denial of service attacks because of its sharing of resources among their clients. The denial of service attack assures much damage to compromised resources in cloud surroundings [40] wrapping attack uses a method referred as wrapping of XML signature and reveals vulnerabilities while executing the web service request. The wrapping attack is hindered by developing the security while sending message from a web server to web browser using simple object access protocol messages. An attacker tries to insert mischievous service or code which develops existing services executing in the cloud in malware injection attack [41]. The massive sql injection intrusions or injection attacks triggered by the malware is prohibited by permitting cloud users to create a cloud account and the provider creates the users of cloud virtual machine image copy in the cloud based image storing structure. In this study different solutions for security problems and security attacks in cloud are discussed. In future the concept of security matrix is used based on multidimensional process to examine threats in cloud further and that assure cloud much secure.

5 Conclusion and scope of future research

Cloud computing is revolutionizing how the IT services and resources are managed and used but the growth often exists with new issues. This study has described some crucial security attacks and has suggested some essential solutions for resolving and preventing cloud based technology from being attacked through wireless hacking techniques. In future this study could be extended by implementing and simulating the attacks in a real-time scenario with the help of cloud simulators and testing the same on how they affect the cloud environment. Further comparative results could also be generated on simulating the attacks in a real-time environment.

References

[1] Cyrus Peikari and Seth Fogi, Wireless Hacking Techniques, retrieved on 28th October 2015, from http://www.computerworld.com/article/2563639/mobile-wireless/wireless-hacking-techniques.html

[2] Cloud Security Alliance, Top threats to cloud computing, *Cloud Security Alliance*, (2010).

[3] Shah, H., and Anandane, S.S., Security Issues on Cloud Computing, arXiv preprint arXiv:1308.5996, (2013).

[4] Khalil, I., Khreishah, A., Bouktif, A., Ahmad, A, Security Concerns in Cloud Computing, *Proceedings of the 10th International Conference on Information Technology: New Generations*, April 15-17, (2013), Las Vegas, USA, 412-416.

[5] Booth, G., Soknacki, A., and Somayaji, A., Cloud Security: Attacks and Current Defenses, *Proceedings of the 8th Annual Symposium on Information Assurance* (ASIA'13) (2013, June), 56.

[6] Sen, J., Sengupta, I., &Chowdhury, P. R. A Mechanism for Detection and Prevention of Distributed Denial of Service Attacks. In Proceedings of the 8th International Conference on Distributed Computing and Networking (ICDCN'06), Springer LNCS, **4308**, Guwahati, India, (December, 2006a), 139-144.

[7] Sattar I., Shahid M and Abbas Y., A Review of Techniques to Detect and Prevent Distributed Denial of Service (DDoS) Attack in Cloud Computing Environment, *International Journal of Computer Applications*, **115**(8), (2015).

[8] McIntosh M. and Austel P., XML Signature Element Wrapping Attacks and Countermeasures, *Workshop on Secure web services*, ACM Press, New York, NY, 20–27, (2005).

[9] Gruschka, N. and Iacono, L.L., Vulnerable Cloud: SOAP Message Security Validation Revisited, *Proceedings of IEEE International Conference on Web Services* (ICWS'09), Los Angeles, California, USA, (July, 2009), 625-631.

[10] Bhargavan K, Fournet C., Gordon A. D. and O'Shea G., An advisor for Web Services Security policies. In SWS '05: *Proceedings of the 2005 workshop on Secure Web Services*, ACM Press, New York, NY, USA, (2005), 1–9.

[11] Ramgonda P Pand Mudholkar R.R., Cloud Market Cogitation and Techniques to Averting SQL Injection for University Cloud, *International Journal of Computer Technology and Applications*, **3**(3), (2012), 1217-1224.

[12] Chawla I, Luthra P and Kaur D., DDoS Attacks in Cloud and Mitigation Techniques, International Journal of Innovative Science, *Engineering & Technology*, **2**(7), (2015).

[13] Booth, D., Web service architecture Available at http://www.w3.org: http://www.w3.org/TR/ws- arch/wsa.pdf, accessed on 28th October 2015, (2004).

[14] Raghavendra G.S., Lakshmi R.N.S and Venkateshwariu S., Security Issues and Trends in Cloud Computing, *International Journal of Computer Science and Information Technologie*s, **6**(2), (2015), 1156-1159.

[15] Gajek S, Jensen M, Lioa L and Schneck J., Analysis of signature wrapping attacks and countermeasures, *IEEE International Conference on Web Services*, **2**, (2009).

[16] Barron, C., Yu, H., and Zhan, J., Cloud computing security case studies and research, *Proceedings of the World Congress on Engineering*, **2**, (July, 2013), 3-5.

[17] Kerr D., Dropbox confirms it was hackers, offers users help, Available: http://news.cnet.com/8301-1009_3-57483998-83/dropbox-confirms-itwas-hacked-offers-users-help, accessed on 28th October 2015.

[18] Kumar, V.V., and Nithya, M., Improving security issues and security attacks in cloud computing, *International Journal of Advanced Research IN Computer and Communication Engineering*, **3**(10), (2014).

[19] Shitoot A., Sahu S. and Chawda R., Security Aspects in Cloud Computing, IJETT, 6(3), (2013).

[20] Angadi A.B., Angadi A.B. and Gull K.C., Security Issues with Possible Solutions in Cloud Computing-A Survey, IJARCET, **2**(2), (2013).

[21] Booth, G., Soknacki, A., and Somayaji, A., Cloud Security: Attacks and Current Defenses, *Proceedings of the 8th Annual Symposium on Information Assurance* (ASIA'13), (June, 2013), 56.

[22] Bhati A.S. and Piquero A.R., Estimating the Impact of Incarceration on Subsequent Offending Trajectories: Deterrent, Criminogenic, or Null Effect?, *The Journal of Criminal Law and Criminology*, **98**, (2007), 207- 253.

[23] Priyanka and Kaswan K.K., Security Issue in Cloud Computing, *International Journal of Computer Science and Information technology research*, **2**(2), (2014), 123-126.

[24] Payne B.D, Carbone M, Sharif M, and Lee W., Lares: An architecture for secure active monitoring using virtualization., IEEE *Symposium on Security and Privacy*, (2008), 233-242.

[25] Chou, T.S. Security threats on cloud computing vulnerabilities, *International Journal of Computer Science & Information Technology*, **5**(3), (2013), 79-88.

[26] Jensen M, Meyer C, Somorovsky J and Schwenk J., On the Effectiveness of XML Schema Validation for Countering XML Signature Wrapping Attacks, *First International Workshop on Securing Services on the Cloud*, Milan, Italy, (2011).

[27] Li H.C., Liang P.H., Yang J.M. and Chen S.J., Analysis on Cloud-Based Security Vulnerability Assessment, IEEE *International Conference on E-Business Engineering*, (2013), 490-494.

[28] Siva, T., and Krishna, E. P., Controlling various network based ADoS Attacks in cloud computing environment: By Using Port Hopping Technique, *International Journal of Engineering Trends and Technology* (IJETT), **4**, (2013).

[29] Fletcher O., Malware Attack Uses China World Expo Guise Available at http://www.computerworld.com/article/2516814/government-it/malware-attack-uses-china-world-expo-guise.html, accessed on 28th October 2015, (2010).

[30] Singh, A., and Shrivastava, M., Overview of attacks on cloud computing, *International Journal of Engineering and Innovative Technology* (IJEIT), **1**(4), (2012).

[31] Sqalli M.H., Al-Haidari F. and Salah K., EDoS-Shield- A Two- Steps Mitigation Technique against EDoS Attacks in Cloud Computing, 4th IEEE *International Conference on Utility and Cloud Computing*, (2011).

[32] Jensen, M., and Gruschka, N., Flooding Attack Issues of Web Services and Service-Oriented Architectures, GI *Jahrestagung*, **1**, (2008), 117-122.

[33] Fletcher K,K., *Cloud Security requirements analysis and security policy development using a highorder object-oriented modeling*, Master of science, Computer Science, Missouri University of Science and Technology, 2010.

[34] Scarfone K.S.A., Guide to Secure Web Services, Available at http://csrc.nist.gov/publications/nistpubs/800-95/SP800-95.pdf, accessed on 28th October 2015, (2007).

[35] Cloud Security Alliance, Securing Microsoft's Cloud infrastructure, Available at https://cloudsecurityalliance.org/securing-the-MS-Cloud.pdf, accessed on 28th October 2015, (2009).

[36] Zunnurhain K. and Vrbsky S., Security Attacks and Solutions in Clouds, 2nd IEEE *International Conference on Cloud Computing Technology and Science, Indianapolis*, (2010).

[37] Jamil D. and Zaki H., Security Issues in Cloud Computing and Countermeasures, *International Journal of Engineering Science and Technology*, **3**(4), (2011), 2672-2676.

[38] Jensen M., Meyer C., Somorovsky J., and Schwenk J., On the Effectiveness of XML Schema Validation for Countering XML Signature Wrapping Attacks, *First International Workshop on Securing Services on the Cloud*, Milan, Italy, (2011).

[39] Stolfo S.J., Salem M.B., and Keromytis A.D., Fog computing: Mitigating Insider Data Theft Attacks in the Cloud, IEEE *Symposium on Security and Privacy Workshops*, , San Francisco, CA, (2012), 125-128.

[40] Tripathi, A. and Mishra, A., Cloud computing security considerations, *Proceedings of the 2011 IEEE International Conference on Signal Processing, Communications and Computing* (ICSPCC), Xi'an, China, (14–16 September, 2011), 1–5.

[41] Zunnurhain, K., and Vrbsky, S., Security attacks and solutions in clouds, *Proceedings of the 1st international conference on cloud computing*, (December, 2010), 145-156.