DOI: http://dx.doi.org/10.26483/ijarcs.v8i9.4825

ISSN No. 0976-5697

Volume 8, No. 9, November-December 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

CHALLENGES AND DEFENSES FOR NETWORK AND CLOUD SECURITY FROM RISKS, THREATS AND ATTACKS IN CLOUD COMPUTING

Tingilikar Anusha
Assistant Professor
Department of Computer Science and Engineering
Warangal Institute of Technology and Science
Warangal, Telangana State, India.

B. Prathusha
Assistant Professor
Department of Computer Science and Engineering
Warangal Institute of Technology and Science
Warangal, Telangana State, India.

J. Vijaya Chandra
HOD & Assistant Professor
Department of Computer Science and Engineering
Warangal Institute of Technology and Science
Warangal, Telangana State, India.

Abstract: Cloud Computing emerged from the advancements of several technologies where the roots are from the mainframes supported by internet as web services along with the distributed resources. It is an advanced technology from grid computing and utility computing provides services at large scale level using different data centres for large capacity of data storage. The major challenges related to cloud computing is the security such as the network reliability, performance monitoring, scale management, quality of services, interoperability and probability. In this paper, we majorly concentrated on the network security, different procedures and mechanisms involved in defence system from risks, threats and attacks on the cloud computing and we discussed different possible vulnerabilities and malwares. We give the mathematical cryptography procedures and mechanisms for securing the network and cloud. Mathematical methods and procedures are given for Cryptographic defences against the man-in-middle attacks, spoofing attacks and transmission control protocol attacks. Experimental and statistical analysis is done, we evaluate real time challenges by designing -building a private cloud and injecting the transmission control protocol injection attacks, the observations are done along with the defence system where the graphical and statistical analysis is given.

Keywords: Cloud Security, Risks, Threats, Attacks, Defences, network security, transmission control protocol, injection attacks.

I. INTRODUCTION

The most definitive and coherent connections are made using one of the most important transport protocol that is TCP. There is also a probability to attackers through TCP which is vulnerable to Man-in-Middle attacks. Appropriate to avoid the complexity that are occurred by using Man-in-Middle attack and eavesdropping attack, the attacker chooses the off-path attack since the establishment of paths or controlling the routers through the path between legitimate users is unpredictable [1].

Cryptography plays a major role in security, there are two false beliefs or illusions against network-based risks, threats and attacks, the foremost belief is that in reality, attackers can rarely obtain Man-in-the-Middle capabilities, and even when they can, they are opposed to do so since such actions may lead to recognition. We attest that this is incorrect; there are common scenarios where attackers may obtain Man-in-the-Middle capabilities, for example by accessing wireless communication and by manipulations of the largely unsecured routing protocols, procedures and mechanisms, or by controlling some transitional devices. Furthermore, such attacks are often carried out, without detection and effect such as route tracking or hijacking occurs frequently. Now we concentrate on the next false belief, which is based on current, non-cryptographic, Internet protocols that are already provide sufficient protection against most typical and crucial situations by common attackers, and in particular, against off-path attackers. Man-in-the-Middle attacker is quite different from off-path attacker, an off-path attacker cannot monitor or modify legitimate packets sent between other parties, however, he can transmit packets with a spoofed that is with fake source IP address - impersonate it as legitimate party [2].

The internet protocol is designed for the transmission of information through the internet and computer networks. The transmitting IP packet should consist of header, and few other transmitting information of clients. The source IP address is definitely the packet address which was sent from, but the senders address in the IP header can be varied, so the destination assumes that the packet is from another transmitter and the source waits for acknowledgement from the recipient. Here the source does not worry about the response from recipient because the spoofing attack has injected. Internet Protocol spoofing is predominantly used to influence man-in-the-middle attacks against hosts on a computer network [3].

II. RELATED WORK

A. *Spoofing Attack*

The primary goal of spoofing attack is to steal the private data from authorized user acceptable to launch the attacks against network hosts to spread malware or bypass access control to accomplish with the help of malicious parties [4]. The firewalls which are having a capability of deep packet inspection and to identify the authorized users can be reduced by using the TCP/IP suite protocols for spoofing attack. In spoofing attack we have again two different spoofing attacks. They are client-side spoofing and server-side spoofing [5].

In client-side spoofing, the intruder spoof like a authorized client and gets the required private data from a dense server. The reverse way of client -side spoofing is server-side spoofing. In server-side spoofing the intruder acts like a actual service provider and then performs the stealing of private information from clients individually [6].

In order to overcome the network security the intruder need to use the IP spoofing which makes the use of trusted IP address like authorization - related to IP addresses. Here the successful relationship is provided between devices. With the help of spoofing an intruder can attack the authorized devices of the same network which has successful relationship without getting any permission from authorized users [7].

Hiding of internet protocol is possible in spoofing attack which is very frequently used by multiple attackers. For the purpose of protecting authorized data we need to implement few critical techniques against spoofed packets, notably access filtering. The known fact is that the internet protocol spoofing is practicable to many of the internet service providers. Here we mainly concentrate on the off-path attacker which has an incorrect belief in present internet protocols [8].

B. Transmission Control Protocol Attack

In major the TCP is not designed for security purpose. Apart from these there are many security patches have been designed for specification and implementation level. The high-level security has developed for new specifications. Unfortunately, this high level security development leads to create a more serious vulnerability. In the internet protocol suits transmission control protocols is the main protocol. Its implementation has been arisen with starting network which is complemented with internet protocol. That is the main reason we treat the whole suit as the TCP/IP. The applications that are transferring reliable, error-checked data provided by TCP between the devices can be communicated using internet protocol [9].

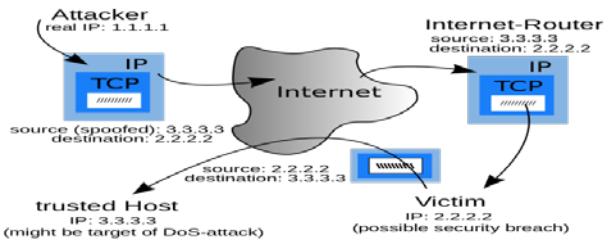

Figure 1: Structure of TCP attack

The TCP connection may be hijacked by an intelligent intruder to eavesdrop a TCP session and redirect packet. For this purpose the intruder need to learn the sequence number for hacking the packet by sending the acknowledgment through the communication channel as if it is send by authorized user and if that receiver sends an acknowledgement for that malicious packet to the intruder then the synchronization is lost. Here Address Resolution Protocol or control over routing attacks of packet flow might be result in hijacking of TCP connection [10].

If the identification of sequence number is easy to guess then spoofing of IP address was not difficult. These results the receiver to believe that the packets had came from different IP address which has been send by intruder without the use of establishment of address resolution protocol or network attackers. This made the initial sequence number is treated to be as random [11].

III. TCP INJECTION ATTACKS

There are two phases to operate off-path TCP injection.

1. Learn Connection Four-Tuple: Appropriate to the maintenance of a TCP connection between client and server, the intruder intended to learn four parameters they include IP addresses and ports.
2. Learn Sequence Number: The only way to send packets between users the intruder must know the current sequence number. Now the attacker able to inject data into TCP connection, by acting as a desired user in between the transmission [12].

A. Learn Connection Four-Tuple: To organize the injection attack, the identification of TCP connection between the victim client and server is necessary for the intruder. The victim's device is verified either remotely or locally. Let us consider a simple method - client uses the puppet to provide a recipient connection with known clients address along with IP address and port. The intruder selects the server IP addresses and port of a particular server as well as the client IP address in order to send a request and detect the client port.

The clients will not use any randomized algorithms and assigning ports sequential connections which may result in hacking the devices that are included in transmission protocol which means off-path attacker of the client port. Before and after opening the recipient server connection the puppet spikes to intruder remote site. Intruder detects client ports p1 and p2 that are used in connection to his/her sites, if the connection is p2=p1+2 then intruder learns to the server connection is via p1+1 if not there is chance to restart the attack by intruder [13].

B. Learn Sequence Number: The second phase of TCP injection after recognizing the recipient connection including client port is to know the one or both connections sequence numbers. Several methods can be used by off-path attackers to infer the sequence numbers as they are unable to see them directly. Here the sequence number provides the permission to attacker to inject the spoofed data into connection by acting like a server [14].

IV. DEFENSE SYSTEM FOR ATTACKS

Defense system used to protect the data is the Défense in depth an onion layered security mechanism. Monitoring network traffic is the major aim where firewalls that can help with comprehensive security system, that is adapted for intrusion prevention. The different layers will have shielded for defending the risks, threats and attacks, majorly focused on transmission control protocol and targeted attacks. Anti - viruses are also used in layers for Défense system, for security authentication and authorization mechanisms are used where digital signatures plays a major role. Auditing and log based forensic investigation is used for the Défense in depth strategy and behavioral analysis. Once an attack is detected or vulnerability is identified, immediate measures will be taken, it is important to shut it down immediately and patch work should be done to defend the attack [15].

V. EXPERIMENTAL ANALYSIS

As mentioned, in this proposal an unauthorized user can attack or steal any type of data with the help of number of

technologies without knowing to the sender as well as the receiver. This attack can be considered as TCP spoofing attack. If the third party wants to attack, then the attacker or intruder can use a tool called **WIRE SHARK** by installing in their devices. Let us consider an attack that is stealing live streaming videos. Assume there is a live conference of a company is leading with authorized clients where they are discussing the most confidential information related to company growth. Here the attacker can also access the live video as an authorized client without making any aware to authorized persons by using this **WIRE SHARK** tool. Here the attacking process includes the capturing network packet details. The identification of current system is possible by using IP address in which data to be steeled. This data can be viewed and saved by an unauthorized person who leads to security breaches .

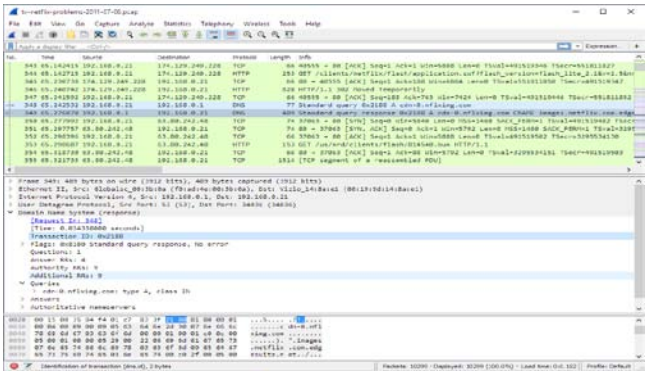

Figure 2: Screen Shot of WIRE SHARK

VI. FUTURE WORK

TCP spoofing attacks, injection attacks are encouraged with the vulnerabilities in the network and security services. When an intruder tries to attack with any type of tool recognizing that attacks and applying any changes which needed to further security are should be more intelligible. As per the new technical issues there is an introduction of a new security tool that is a type of fire wall named SONIC WALL. SONIC WALL is a new security tool which makes complex to perform TCP splitting which does not allows any kind of spoofing attacks. Detection of misleading, security breaches and preventions all so made up of with this tool which works like a defence to a particular type of attack.

VII. CONCLUSION

TCP injection attacks and spoofing attack are mainly performed by approaching some methods by monitoring the protocols and data packets information through the transmission channel. Reducing vulnerabilities leads to major security in network. As technology is improving intrusion techniques also learning more skills. In this paper we mentioned that how spoofing attack is taking with security tool and how that attack can be defense by another security tool.

VIII. REFERENCES

[1] Zhiyun Qian, Z. Morley Mao, "Off-path TCP Sequence Number Inference Attack - How Firewall Middleboxes Reduce Security", IEEE Symposium on Security and Privacy - 2012.

[2] J. Vijaya Chandra, Narasimham Challa and MD. Ali Hussain, "Data and Information Storage Security from Advanced Persistent Attack in Cloud Computing", International Journal of Applied Engineering Research, 2014.

[3] J. Vijaya Chandra, Narasimham Challa, Sai Kiran Pasupuleti, Thirupathi RK, Krishna RV, " Numerical Formulation and Simulation of Social Networks using Graph Theory on Social Cloud Platform", Global Journal of Pure and Applied Mathematics. 2015; 11(2):1253–64.

[4] Jian Liu; Kun Huang; Hong Rong; Huimei Wang; Ming Xian, "Privacy Preserving Public Auditing for Regenerating-Code-Based Cloud Storage, "IEEE Transactions on Information Forensics and Security, vol.10, no.7, pp.1513-1528, July 2015.

[5] J. Gionta, A. Azab, W. Enck, P. Ning, and X. Zhang, "Dacsa: A decoupled architecture for cloud security analysis," in Proceedings of the 7th Workshop on Cyber Security Experimentation and Test, 2014.

[6] S. Ruj, M. Stojmenovic, and A. Nayak, "Decentralized access control with anonymous authentication of data stored in clouds," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 384–394, 2014.

[7] J. Vijaya Chandra, Narasimham Challa, Sai Kiran Pasupuleti, "Intelligence based Defense System to Protect from Advanced Persistent Threat by means of Social Engineering on Social Cloud Platform", Indian Journal of Science and Technology, Volume 8, Issue 28, October 2015.

[8] C.-K. Chu, S. S. Chow, W.-G. Tzeng, J. Zhou, and R. H. Deng, "Key-aggregate cryptosystem for scalable data sharing in cloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 468–477, 2014.

[9] Xun Yi, Russell Paulet and Elisa Bertino, Homomorphic Encryption and Applications, 1st edn. Springer Briefs in Computer Science, Springer International Publishing, 2014.

[10] G Ranjith, J Vijayachandra, B Prathusha, P Sagarika, "Design and implementation of a defense system from TCP injection attacks", Indian Journal of Science and Technology, vol 9, issue 40, 2016.

[11] Z. Qian, Z. M. Mao, and Y. Xie, "Collaborative TCP Sequence Number Inference Attack: How to Crack Sequence Number Under a Second," in Proceedings of the ACM Conference on Computer and Communications Security. New York, NY, USA: ACM, 2012.

[12] Y. Gilad and A. Herzberg, "LOT: A Defense Against IP Spoofing and Flooding Attacks," ACM Transactions on Information and System Security, vol. 15, no. 2, pp. 6:1–6:30, Jul. 2012.

[13] Adebayo O.S and AbdulAziz N, "An intelligence based model for the prevention of advanced cyber-attacks," Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on , vol., no., pp.1,5, 17-18 Nov. 2014.

[14] Vance A, "Flow based analysis of Advanced Persistent Threats detecting targeted attacks in cloud computing," Infocommunications Science and Technology, 2014 First International Scientific-Practical Conference Problems of , vol., no., pp.173,176, 14-17 Oct. 2014.

[15] Liu Shengjian, Yang Haiyan, Wang Fengni, "Design of Network Security Early-Warning System Based on Network Defense in depth Model", 2nd International Conference on Measurement, Information and Control, 2013.