ISSUES AND THREATSIN CLOUD NETWORK SECURITY

ANISHA TANDON[1], MAMTA MADAN[2] and MEENU DAVE[3]

[1]Research Scholar, [3]Professor
JaganNath University
Jaipur, India
E-mail: 184.anisha@gmail.com
          meenu.s.dave@gmail.com

[2]Professor
VIPS, GGSIPU
Pitampura, India
E-mail: mamta.vips@gmail.com

Abstract

Being connected to people has become an indispensable part of our day-to-day lives. We stay constantly connected with the people around us. In simple words, Network security can be defined as a connection of multiple devices. With increasing connectivity of devices, it is essential that data shared among a group of devices stays private as intended by the participants of the group. Today's networking structure is intricate and is faced by constant threat from hackers. Loopholes in network security may lead to serious threats such as Data Modification, DOS attack, Eavesdropping, Botnet, Identity Spoofing, MITM attack, Password – Based attacks etc. This paper briefly introduces the concepts related to Network Security and the threats to which a network may be exposed. It also focuses on resolving various threats faced by networks such as Cryptography, Hashing, Firewalls, VPN, Proxy Servers, Anti-virus soft wares and SSL/TLS. This paper gives in depth consideration to wireless network security and a prospective solution to increase wireless network security.

1. Introduction

A network is a set of multiple devices (or nodes) that are connected to each other. These devices can deliver and/or accept information or resources to/from other devices [1]. Network security is the art of preventing misuse, unauthorized access, modification of data, or denial of a computer network

and its resources. Network can be secured by software methods or hardware methods [2]. Attacks on the network can be classified broadly in three ways [3].

Passive Attack. In a passive attack, the perpetrator only tries to read data or capture the information.

The aim of the attacker is not to influence the information across the network.

Active Attack. In an active attack, the perpetrator may attempt to influence the data and resources travelling across the network.

Insider Attack. An insider attack is usually related to a certain organisation. A person such as a discontented member [4] usually carries this out.

This research focuses on the security issues and threats of data over a cloud.

2. Related Work

Shailja Pandey [1] gives an in depth explanation of the concepts of network and the various threats to security of networks. Major importance has been given to the security of networks of an organisation rather than networks of individuals.

Figure 1. Networking.

Sankardas Roy et al. [5] have discussed about:

- Network Security
- Game Theory

- Taxonomy (General)

- Computer Security

Sumit Ahlawat and Anshul Anand have given the history of computers and networking along with characteristics of networks, networking protocols and threats to network security. The authors have also mentioned about the application of wireless technology [14].

Figure 2. Wireless Networking.

Monali S. Gaigole and M. A. Kalyankar highlighted the threats to network security and methods to increase network security [3].

Figure 3. Wireless Network Security.

Comparatively, networking in cloud provides more security than conventional networking [8] [9].

3. Network Security Issues in Cloud Computing

Network security [4] issues are the problems that are faced related to the security of a network. Loopholes in the security of a network may lead to compromising of important data. The data or resources may be subjected to snooping or in some cases manipulation or even permanent deletion/loss. Network security is the security provided to the network to prevent un authorised access to data and resources [5].

Based on the study, we found that there are several issues in cloud but security is the important concern, which is associated with cloud computing [10]. The issues in cloud computing environment are:

- Insecure API

- Insiders and Outsider Attacks

- Data Loss

- Data Crash

- loss of encryption keys

4. Network Security Threats

- Eavesdropping: Eavesdropping in general means listening to conversation, which is not intended for a particular person. Similarly, in case of network, eavesdropping can be defined as the unauthorised interception of data on a network. This data may include phone calls, messages, photos, videos or any other piece of information travelling through a network [6].

- Data Modification: The data being sent is intercepted by an unauthorised person and is changed or manipulated and then sent to the receiver. This leads to loss of confidentiality, authenticity and integrity of the data [7].

- Identity Spoofing: Identity spoofing is taking over the identity of a computer and then using that identity to achieve a certain objective. An attacker may use IP spoofing to assume the identity of another computer thereby hiding the real identity of the attacker.

- Password-Based-attacks: One of the most basic password-based-attacks

is Brute Force attack. In a bruteforce attack, an attacker runs a script for a set of passwords against a username. This is a kind of hit and trial method. For Example, if the attacker has the list of usernames of an organisation, he/she can run a script for some common passwords and one of it might be a match. Another type of password-based-attack is Key Logger attack. Key logger software can be installed on the target computer, which would record every keystroke and send it to the attacker. The most common tool used in password-based-attacks is BurpSuite. A popular Key logger tool is BeeLogger.

• Denial-Of-Service Attack: Denial of Service attack is carried out to deny real users to access a network. It is carried out by sending fake traffic to the host until it becomes unresponsive to real users. The tools used for DOS attacks are Hping, Nmap, Metasploit and Aircrack-ng (Used for wireless access points) [11].

• Man-In-The-Middle Attack: As the name suggests, this attack means that an attacker between the sender and the receiver intercepts the data sent over a network.
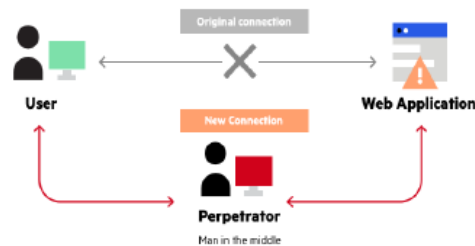

Figure 4. Man inthe Middle Attack.

• Botnets: Botnets can be defined as a network of compromised machines that can be remotely controlled to launch a large-scale attack. Botnets act like slaves that perform any type of attack intended by the attacker [12] [13].

5. Threats Challenges in Cloud Network Security

Security: Security is a major challenge of cloud. Cloud is actually based on the internet. Therefore, there can be a situation when the internet is suspended, personal information leakage and sometimes service provider can report the delay of service due to the maintenance issue, attack of viruses and low internet speed [15].

Usage: Due to Inappropriate, usage of cloud-computing test environments can increase the price [16].

Planning: The testing teams must plan testing environments. Expenses must be estimated such as encrypted data costing, costing for the testing cloud environment, CPU costing for extra memory etc [17].

Test Data: Test data management is a challenging task. To effectively perform testing, few of the testing tasks must be dependent upon the actual user or production data. Supplying production data to the third party is forbidden to the users in some cases [18] [19].

On-demand testing: Because of the on-demand requests, the services of testing must be controlled, managed and supervised. Many challenges and issues might increase due to this kind of testing services [20].

References

[1]   Shailja Pandey, Modern network security: Issues and Challenges 3(5) (2011).

[2]   Behrouz A. Forouzan, Data Communication and Networking.

[3]   Monali S. Gaigole and M. A. Kalyankar, The Study of Network Security with Its Penetrating Attacks and Possible Security Mechanisms; IJCSMC 4(5) (2015), 728-735.

[4]   D. Acharjee and B. S. Panada, Enhancing Social Security through Network of Intelligent Human Nodes Trained by Comuter Algorithms.

[5]   Sankardas Roy, Charles Ellis, Sajjan Shiva, Dipankar Dasgupta, Vivek Shandilya and Qishi Wu, A Survey of Game Theory as Applied to Network Security.

[6]   M. Benaiah Deva Kumar and B. Deepa, Computer Networking: A Survey.

[7]   Mrs. Amandeep Kaur, An overview of quality of service computer network.

[8]   Mamta Madan and Anisha Tandon, Cloud Computing Security and its Challenges, International Journal of Electrical electronics and Computer Science Engineering (2015), 68-71.

[9]   Mamta Madan, Meenu Dave and Anisha Tandon, Challenges in Testing of Cloud Based Application, International Journal of Electrical electronics and Computer Science Engineering, 2016.

[10]   Vinton G. Cerf, Computer Networking: Global Infrastructure for the 21st Century.

[11]   Olivier Bonaventure; Computer Networking: Principles, Protocols and Practice.

[12]   Raj Jain, Computer Networking: Recent Advances, Trends, and Issues.

[13]   Raj Jain, Introduction to Computer Introduction to Computer Networking: Trends and Issues.

[14] Sumit Ahlawat and Anshul Anand, An Introduction To Computer Networking.

[15] Varsha and Amit Wadhwa, Study of Security Issues in Cloud Computing, International Journal of Computer Science and Mobile Computing 4(6) (2015), 230-234.

[16] Anisha Tandon, Implementing and Developing Cloud Computing on Web Application, International Journal of Computer Science and Mobile Computing, 2014.

[17] Anisha Tandon and Mamta Madan, Challenges in Testing of Web Applications, International Journal of Engineering and Computer Science 3(5) (2014) 5980-5984.

[18] Mamta Madan and Anisha Tandon, Testing Application on the web, International Journal of Advanced Research in Computer Science and Software Engineering (2013), 855-858.

[19] Mamta Madan, Meenu Dave and Anisha Tandon, Need and Usage of Traceability Matrix for Managing Requirements, International Journal of Engineering Research 5(8) (2016).

[20] Mamta Madan, Meenu Dave and Anisha Tandon, RTM and Testing Challenges in Cloud Based Application, in International Conference on Computers and Management (ICCM), Delhi, 2018.