Global Scientific JOURNALS

GSJ: Volume 7, Issue 10, October 2019, Online: ISSN 2320-9186

www.globalscientificjournal.com

Network Security, network attacks and Possible Security Mechanisms

---

NYIRIMANA Jean Marie Vianney[1], UMUHIRE Laurence[2], Dr. NIYIGENA Papias[3]

Department of Information Technology

Faculty of computing and information Sciences

University of Lay Adventists of Kigali

Rwanda

[1, 2] students, [3] Lecturer

Abstract

The technology of today is more advanced and computer network is one of the world sector developing rapidly, and the internet technology is developing generally quickly, people are using internet on high level. People are knowing the importance of the network security as it is more useful in different ways of their daily life. The big problem of computing is based on computer network security as there are many types of attacks. The multiple attacks are appearing day to day. To protect computers and network security are the issues to be taken into account seriously. The malicious nodes affect the performance of service in the network usage and deny the service. In this paper we describe the attacks of computer network in world of rapid technology.

Introduction

The first step of network security is authorization. It is commonly composed by a username and a password. The network security is composed by the privileges and policies adopted by a network administrator. Those privileges and policies are helpful to prevent and monitor unauthorized users, changes in system, misuse, and denial of a computer network. The network security is normally based on the authorization of access to resources and data in a network and those things are under network administrator control. It has become more important to personal computer users, and organizations. If this authorized, a firewall has to force the accessibility of policies such as what services are allowed to be accessed for network users and prevent unauthorized access to system, this component may fail to check frequently potential danger content such as computer harmful softwares being transmitted over the network. In other side the anti-virus software or another like intrusion detection system can be helpful to detect the malware attacks. Today hackers may also monitor the network in the different ways for audit purposes and for later on high-level analysis in system. The encryption may be used in communication of two hosts to maintain privacy policy.

The world of today is continuously more interconnected of the internet and new networking technology. There is a big number of personal, companies, and government information on networking infrastructures in the world. Network security is becoming of

great importance because of intellectual property that can be easily acquired through the internet.

The network security is analysed by researching the following:

Classification of attacks

Types of network attacks

Network security for internet access

1. Network security

System and the Network Technology is a key technology for a wide variety of applications. It is a critical requirement in the current situation networks.
There is a significant lack of security methods that can be easily implemented. There exists a "communication gaps" between the developer of the security technology and developers of each networks.

Network design is a developed process that can depend on the Open Systems Interface (OSI) models [1]. The OSI models has several advantages when designing network security. It offers modularity, ease of uses, flexibility, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allows the modular development. In contrast to secure network design is not a well-developed process. There is a methodology to manage the complexity of the security requirements. When considering about the network security, it should be emphasized that the complete network is secured. It does not only concerned with the security in the computers at each end of the communication chains [5]. When transferring from one node to another node the communication channel should be vulnerable to attacker. All the hackers will target the communication channel, get all the data, and decrypts it and insert a duplicate message. Though securing the network is just as important as the securing computers and encrypting the message. When developing the network security, the following needs to be taken into account:

i. Confidentiality

It means that the non-authenticated party does not examine the data.

ii. Integrity

It is a guarantee that the data which is received by the receiver has not been change or modified after the send by the sender.

2. Classification of attacks

Attacks can be classified broadly in following two types:

2.1. Active Attack

In an active attack, the attacker tries to bypass or break into protected systems. This can be done using viruses, Trojan horses, worms, or stealth. Active attack includes attempts to bypass or break features implemented for protection, introducing malicious code, and to modify or

steal information. These attacks are implemented on network backbone, exploit the information in transmission, or attack the authorized remote user while making an attempt to connect to an enclave. Active attacks result in the revealing or dissemination of data files, DoS (Denial of Service), or modification of data.

2.2. Passive Attack

A passive attack monitors unencrypted traffic and looks for clear-text passwords and sensitive information that can be used in attacks of other type. Passive attack includes analysis of network traffic, decrypting weakly encrypted contents in traffic, unprotected communications monitoring, and authentication information capturing such as password.
Intercepting the network traffic passively makes possible for the adversaries to watch or predict upcoming actions. Passive attack results in the revealing of information or data files to an attacker without the consent or knowledge of the user.

3. Types of Attacks

Based on classification of attacks which can be a cause for slow network performance, uncontrolled traffic, and viruses are stated. Attacks to network from malicious nodes. Those attacks are the following:

*3.1.*Active attack

Some active attacks are spoofing attack, Wormhole attack, Modification, Denial of services, Sinkhole, and Sybil attack.

i. Wormhole

This attack is also called the tunnelling attack. In this attack an attacker receives a packet at one point and tunnels it to another malicious node in the network. So that a beginner assumes that he found the shortest path in the network [2].

ii. Fabrication

A malicious node generates the false routing message. This means it generate the incorrect information about the route between devices [3].

iii. Spoofing

In the computer world, spoofing refers to stolen identity, when a person pretence as another individual, organization or business with the purpose of gaining access to sensitive personal information including user names and passwords, bank account information, and credit card numbers. Spoofing is both part of the setup for phishing as well as a technique to gain direct access to an individual or organization's computer or computer network. There are some known spoofing types such as: IP spoofing, URL spoofing, Email spoofing, DNS spoofing, and MAC spoofing [4].

iv. Modification

This attack cause communication delay occurred between sender and receiver when malicious node performs some modification in the routing route, because sender sends the message through the long route.

v. Denial of services

In denial of services attack, malicious node sending the message to the node and consume the bandwidth of the network. The main aim of the malicious node is to be busy the network node. If a message from unauthenticated node will come, then receiver will not receive that message because he is busy and beginner has to wait for the receiver response.

vi. Sinkhole

Sinkhole is a service attack that prevents the base station from obtaining complete and correct information. In this attack, a node tries to attract the data to it from his all neighbouring node. Selective modification, forwarding or dropping of data can be done by using this attack [1].

vii. Sybil

This attack related to the multiple copies of malicious nodes. The Sybil attack can be happen due to malicious node shares its secret key with other malicious nodes. In this way the number of malicious node is increased in the network and the probability of the attack is also increases. If we used the multipath routing, then the possibility of selecting a path malicious node will be increased in the network [2, 3, 5].

***3.2.*Passive attack**

The names of some passive attacks are traffic analysis, Eavesdropping, and Monitoring[2, 3,5].

i. *Traffic analysis*

In the traffic analysis attack, attackers try to sense the communication path between the sender and receiver. Attackers can found the amount of data which is travel from the route of sender and receiver. There is no modification in data by the traffic analysis.

ii. *Eavesdropping*

This attack occurred in the mobile ad-hoc network. The main purpose of this attack is to search some secret or confidential information from communication. This secrete information may be private or public key of sender or receiver or any secret data. It is a passive attack in network.

iii. *Monitoring*

In this attack in which attacker can read the confidential data, but he cannot edit the data or cannot modify the data.

3.3 Advance attacks

i. ***Black hole attack***

Black hole attack is one of the advance attacking which attacker uses the routing protocol to advertise itself as having the best path to the node whose packets it want to intercept. An hacker use the flooding based protocol for listing the request for a route from the initiator,

then hacker create a reply message he has the shortest path to the receiver . As this message from the hacker reached to the initiator before the reply from the actual node, then initiator wills consider that, it is the shortest path to the receiver. That a malicious fake route is created [1].

ii. Rushing attack

In rushing attack, when sender send packet to the receiver, then attacker alter the packet and forward to receiver. Attacker performs duplicate sends the duplicate to the receiver again and again. Receiver assumes that packets come from sender so the receiver becomes busy continuously.

iii. *Replay attack*

It this attack a malicious node may repeat the data or delayed the data. This can be done by originator who intercept the data and retransmit it. At that time, an attacker an intercept the password.

iv. *Byzantine attack*

A set of intermediate node works between the sender and receiver and perform some changes such as creating routing loops, sending packet through non optimal path or selectively dropping packet, which result in disruption or degradation of routing services.

v. *Location disclosure attack*

Malicious node collects the information about the node and about the route by computing and monitoring the traffic. So malicious node may perform more attack on the network.

4. Technologies for providing security to the network

Internet threats will go on being a major issue in the world as long as information is accessible and transferred through internet. Different defence and detection mechanisms were developed to deal with attacks mentioned before. Some of these mechanisms along with advance concepts are mention in this section.

i. Cryptographic systems

Cryptography is a useful and widely used tool in security engineering today. It involved the use of codes and ciphers to transform information into unintelligible data.

ii. Firewall

The firewall is a typical border control mechanism or perimeter defense. The purpose of a firewall is to block traffic from the outside, but it could also be used to block traffic from the inside. A firewall is the front line defense mechanism against intruders to enter in the system. It is a system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both [6]. The most widely sold solution to the problems of Internet security is the *firewall.* This is a machine that stands between a local network and the Internet, and filters out traffic that might be harmful. The idea of a solution in a box‖ has great appeal to many organizations, and is now so widely accepted that it's seen as an essential part of corporate due diligence.

iii. Driving Security to the Hardware Level

To further optimize performance and increase security, Intel develop platforms also include several complementary security technologies built into multiple platform components, including the processor, chipset, and network interface controllers (NICs). These technologies provide low-level building blocks upon which a secure and high performing network infrastructure can be sustained. These technologies include Virtualization Technology, Trusted Execution Technology and Quick Assist Technology.

iv. Intrusion Detection Systems

An Intrusion Detection System (IDS) is an additional protection measure that helps ward off computer intrusions. IDS systems can be software and hardware devices used to detect an attack. Intrusion detection system products are used to monitor connection in determining whether attacks are been launched.

Some IDS systems just monitor and alert of an attack, whereas others try to block the attack. The typical antivirus software product is an example of an intrusion detection system. The systems used to detect bad things happening are referred to generically as intrusion detection systems. Intrusion detection in corporate and government networks is a fast-growing field of security research; this growth has been prompted by the realization that many systems make no effective use of log and audit data.

v. Anti_Malware Software and scanners

Viruses, worms and Trojan horses are all examples of malicious software, or Malware for short. Special so_called anti_Malware tools are used to detect them and cure an infected system.

vi. Secure Socket Layer (SSL)

The Secure Socket Layer (SSL) is a suite of protocols that is a standard way to achieve a good level of security between a web browser and a website. SSL is designed to create a secure channel, or tunnel, between a web browser and the web server, so that any information exchanged is protected within the secured tunnel. SSL provides authentication of clients to server through the use of certificates. Clients present a certificate to the server to prove their identity.

vii. Dynamic Endpoint Modeling

Observable's security solution, represents a profoundly new way to look at information technology security. It models each device on your network, so you can understand normal behaviour and quickly take action when a device starts acting abnormally. There's no need to install agents on the devices, or attempt to use deep-packet inspection, giving you a powerful solution to overcome these new security challenges.

viii. Mobile Biometrics

Biometrics on mobile devices will play a bigger role in authenticating users to network services, one security executive predicted. Biometrics emerging on mobile endpoints, either

as applications that gather users' behaviours or as dedicated features on mobile endpoints that scan personal features.

5. Conclusion

Network security is generally difficult and very important. Depending on how risks are known, people have different ideas regarding policies of security. The best way to secure network is to know what security means according to what you need in function of time and use. Once that has been determined, everything that goes on with the network can be evaluated with respect to that policy. For today there are different kinds of attacks on the security policies. Those attacks are growing with the advancement and the growing use of internet. As the threats are increasing, so for secure use of systems and internet there are various different security policies are also developing. In this paper we have identified some attacks and mention some of the security mechanisms that can be used mostly by number of users of internet.

6. References

1. Mohan V. Pawar and J. Anuradha / Procedia Computer Science 48 (2015)
2. Neha Khandelwal, Prabhakar.M. Kuldeep Sharma, "An Overview Of security Problems in MANET".
3. Anupam Joshi and Wenjia Li. "Security Issues in Mobile Ad Hoc Networks- A Survey"
4. PCEB, "Network security and spoofing attacks."
5. Ali Ghaffari, "Vulnerability and Security of Mobile Ad hoc Networks".
6. Adeyinka, O., "Internet Attack Methods and Internet Security Technology," Modeling & Simulation, 2008. AICMS 08. Second Asia International Conference on, vol., no., pp.77_82, 13_15 May 2008.

Authors:

1. NYIRIMANA Jean Marie Vianney, email: anne4505@hotmail.com

Student in Master of Science in Information Technology, University of Lay Adventists of Kigali

2. UMUHIRE Laurence, email: umuhirelau@gmail.com

Student in Master of Science in Information Technology, University of Lay Adventists of Kigali

Correspondence author:

1. Dr. NIYIGENA Papias, email: papiasni@yahoo.fr

Lecturer in Master of Science in Information Technology, University of Lay Adventists of Kigali