Chapter 3

Against Spoofing Attacks in Network Layer

Kavisankar L.
SRM University, India

Chellappan C.
GKM College of Engineering and Technology, India

Poovammal E.
SRM University, India

ABSTRACT

In the context of network security, a spoofing attack is a condition in which one person or a program successfully masquerades as another. This is done by providing counterfeit data with the malicious intention of gaining an illegitimate advantage. Spoofing attack which may be generated in various layer of Open Systems Interconnection model (OSI model) is discussed in this chapter. The chapter ends with discussing about the possible spoofing attacks in network layer and the relevant defense mechanism of the same. The detailed analysis and discussion is made on the spoofing attack over the Network layer because, Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) attacks more devastating while using network protocol like Internet Protocol (IP) which have become more of a threat than ever for the past few years.

INTRODUCTION

It is essential to impose the network security, which can achieve control over access from intruders and malicious users. According to Cisco (2012), network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources.

Security is considered as an integral part of internet browsing. It is one of the most important quality attributes in the field of networking. Due to the gradually increasing number of vulnerabilities, the identification of an attack is essential. Network attacks, must thus be defined in order to measure security.

DOI: 10.4018/978-1-5225-0193-0.ch003
In the context of network security, a spoofing attack is a situation in which one person or a program successfully masquerades as another. This is done by providing counterfeit data with the malicious intention of gaining an illegitimate advantage. Spoofing attack which may be generated in various layer of Open Systems Interconnection model (OSI model) is discussed in this chapter. The chapter ends with discussing about the possible spoofing attacks in network layer and the relevant defense mechanism of the same.

We start our discussion in application layer on the vulnerabilities of application protocols towards spoofing attacks. The application protocols like Simple Mail Transfer Protocol (SMTP), Hypertext Transfer Protocol (HTTP), Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) are vulnerable to spoofing attacks. The very essential application like biometric is also vulnerable to spoofed attacks. The biometric like fingerprint and iris suffers spoofing by the attackers. The concentration is on presentation layer now, where the Multi-Purpose Internet Mail Extensions (MIME) is vulnerable to Spoofing attacks. While in the Session layer we have major vulnerability of session hijacking. The Session hijacking is closely related to the session spoofing attack. The like Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are vulnerable to synchronization (SYN) Spoofing and UDP Spoofing respectively. This is done by exploiting the vulnerabilities of the transport layer protocols.

The Data Link layer uses the protocol like Address Resolution Protocol (ARP). The ARP which is used to translate internet protocol addresses to hardware interface addresses. Because ARP does not provide methods for authenticating ARP replies on a network, ARP replies can be spoofed by hosts on a network other than the one from which a reply was expected. A malicious user may leverage ARP spoofing to perform a man-in-the-middle or denial-of-service attack on other users on the network. Various software exists to both detect and perform ARP spoofing attacks, though ARP itself does not provide any methods of protection from such attacks. We also have attack on the Media Access Control (MAC) address i.e. MAC spoofing is a technique for changing a factory-assigned MAC address of a network interface on a networked device. Finally, the Physical layer the location Spoofing works in two ways impersonation of access points (from one location to another) and elimination of signals sent by legitimate access points.

The detailed analysis and discussion is made on the spoofing attack over the Network layer because, denial-of-service (DoS) and distributed denial-of-service (DDoS) attacks more devastating while using network protocol like Internet Protocol (IP) which have become more of a threat than ever for the past few years.

The Network layer is used to router the packets from source to destination based on the IP address of the destination System. Because the router does not have any knowledge about the source address of the packet the attacker use this vulnerability to attack the destination system by using the forged or spoofed IP address. The spoofed IP address with flooding increases the intensity of the attack denial of service attack.

According to IBM (2014), a DDoS attack is launched from hundreds or even thousands of sources simultaneously. A DDoS attack appears like normal traffic coming from a large number of sources rather than an excess of traffic coming from a single source. The identify and mitigation is difficult even more difficult is to trace back to its original origin. To add to it the address spoofing or IP spoofing is programmed by the attackers which are done by putting the fake source addresses in the packets. In such cases tracing to its origin becomes ever more difficult.

According to Brian (2013), and Ronen (2013) Criminals nowadays increase in the volume of attacks, using multi-vector attacks. According to Incapsula’s report the attackers are more successful by varying the attack methods which creates “A smoke screen effect” which is justified by the report with 81% of