Abstract

On the IPv6 over IPv4 tunnel can still occur spoofing. An attacker sends a packet to an address with a forged address that pass through system or one of all nodes of system is a victim. IPv4 address of tunnel endpoint is used by attacker into spoofing packet. IPv6 over IPv4 tunnel uses two types of IP, that's IPv4 and IPv6. IPv6 header and its payload will be encapsulated with IPv4 header so that it can pass through IPv4 infrastructure. IP Security (IPSec) is recommended to reduce spoofing attack that operate in IP layer. There are two security protocols that can be used. That protocols are Authentication Header (AH) and Encapsulating Security Payload (ESP). Each protocol can use transport mode or tunne model. According RFC4891, transport mode will protect the packet defined by (source IPv4 address, destination IPv4 address, protocol=41), while mode tunnel will protect the packet defined by (source IPv6 address, destination IPv6 address). Using mode transport is recommended because protocol 41 is still exist. That protocol is identity of IPv6 packet that brought by IPv4 packet.

It uses host-to-host scenario. There are two main system that is built, tunnel without IPsec and tunnel with IPsec. Each system will be sent a number of spoofing packets and then packet processed will be observed by the victim and other affected node (the suspect). In addition, utility of CPU that caused by spoofing packets will be observed on both host. On system with IPSec will be tested about the influence of IPSec lifetime to spoofing packets that processed by both host and its utility.

After that, result of system without IPSec will be compared with system that used IPSec. The packet that processed by system with IPSec is less than system without IPSec. Before applying IPSec, victim processes packet three times the amount of spoofing packets that sent by attacker (packet with SYN, SYN/ACK, and RST flag), while suspect processes packet twice (packet with SYN/ACK and RST flag). After implementing IPSec, only victim who receives packet with SYN flag from attacker and then that packet will not be processesd again by sending SYN/ACK to suspect. This is due to the incoming spoofing packet rejected at the IPSec level. Utility that caused by spoofing packet is also decreased because there is no packet processed. IPSec lifetime is not influential to packet processed and utility caused spoofing packet. It is also caused by spoofing packet that dropped in the IPSec level so that there is no packet processed.

***Keywords**: IPv6-over-IPv4, tunnel, spoofing, IPv4, IPv6, IP layer, IPSec, AH, ESP, transport mode, tunnel mode, packet, utility, IPSec lifetime*