60-592 Network Security
Summary Paper1

Pravina Bhatt
104701991

# Summary of “Detecting Spoofed Packets”

According to the portfolio of IP protocol, the packets can be identified on the bases of its source address and redirected to specified destination too, but the authenticity of the source is not possible with this protocol. It means that we cannot check that the packet is evolving from the trustworthy source or it a spoofed attacker. Thus, the main motive of this paper is to encounter all those methods using which it can be detected that either the emerging packets have spoofed source address using various strategies. This paper argues attacks using spoofed packets and a wide variety of methods for detecting spoofed packets. In this paper we will come across an overview of various detection methods followed by various routing approaches including active and passive types and finally ways of detecting the spoofed packets implementing various experiments.

**Packet Spoofing attacks:**

1. SYN-flood: Attack includes the flooding of target network TCP SYN packet.
2. Smurf: Attack includes flooding the target network for receiving ICMP echo packets for the broadcasted ICMP packets within network and spoofing it with source address.
3. TCP Connection Spoofing: This attack is the method of spoofing the target and let attacker to implement DoS attack on host.
4. Bounce Scan: Here the logic of being a part of any network of target and observe the packets that are shared within the network, is being implemented by the attacker.
5. Zombie Control: Here the attacker will control the zombies in the network by spoofing the origin of control messages from the target network.

**Spoofed Packet Detection methods:**

Enlists the automated method of detecting spoofed packets in the network.

1) Routing Methods: Here the role of border router or gateway is to check whether the evolved packets are in same network or not, if they are redirected to external interface it means they are spoofed but if the attacker is in the same network then need to apply following techniques.
2) Non-routing methods: It includes two more branches as active and passive methods.
   a) Active methods: Verifies that the packet was sent from the claimed source or is being spoofed. This includes various methods like TTL methods, Direct TTL probes, IP Identification Number, OS Fingerprinting, TCP Specific Methods, Flow Control, Packet Retransmission and Traceroute.
   b) Passive methods: It is logical extension of reactive method, works on the principle of dealing with TTLs. It follows the strategy of observing the packets, the legitimate packets and trace the irregular or uncommon among the evolving one. This includes Passive TTL and OS Idiosyncrasies methods.

**Use in Intrusion Detection System:**

The logic implemented behind detection of spoofed packets is extended up to firewalls and IDS sensor where if the spoofed packet is detected the sensors will alert IDS and moreover firewalls will either discard these spoofed packets or flag it as a spoofed one to be identified by other IDS.

Experiments for detecting spoofed packets: This includes TTL Predictability in which emerging packet data is collected till specific time period for assessing the predictability of TTLs and evaluate them as a means of detecting spoofed packets. This may also include various limitations relating to Asymmetric routes, redundant routes, DHCP, Network Address Translation, Proxies and Forged TTLs and IP IDs.

**Finally it is concluded that those alternative techniques to automated method can be used individually or as a combination to predict the spoofed packets, as the automated sensors may lack behind in providing all those information for identifying the spoofed packets. As a result all the spoofed packets may not be detected and still can evolve within the network targeted by an attacker, but still they acknowledge that this substitute may also would not guarantee 100% detection but still may overcome the drawbacks of automated sensor methods.**