[5A-38]

An Efficient Approach of Marking Packet at Source Side for IP Traceback

Yu Xiang, Choong Seon Hong
School of Electronics & Information, Kyung Hee University
yuxiang@networking.khu.ac.kr, cshong@khu.ac.kr

Abstract

With the help of real source identity in packets, intrusion detect system can efficiently defense and counteract the attacks. Unfortunately there are some issues on it, named IP Traceback problem. This paper focuses on this side, and proposes a simple and efficient method to mark an exclusive identity in every packet belonging to upstream traffic. According to our approach, just only need low overhead on the edge routers as well as a little extra network traffic to settle it. Furthermore, ISP will not reveal its internal network topology and other details while use this method.

Keywords – IP Packet, DoS Attack, Packet Marking, IP Traceback

1. Motivation

In the last several years Internet attacks have revealed in frequent, furious and sophistical posture. Attack tools are publicly released vulnerability assessment software, to degrade the performance or even disable vital network servers. In fact, there are a number of widely deployed operation systems and routers that can be disabled by single well-targeted packet. Such as DoS attacks are difficult to prevent and to trace. Most of DoS attack aimed to these servers that are playing an important role in all network service providing. It already has become one of the major threats to network security. To litigate for these attacks, the source of individual packets must be identified. However, determining the source generating attack traffic is surprisingly difficult due to the stateless nature of Internet routing. Attackers routinely disguised their location using incorrectly, or spoofed IP source address.

A great amount of effort has been done to the network security issues. We can divide them into two types: Traceback across stepping-stones and IP traceback. The first one is based on connection and IP traceback focuses on packet trace: Logging, ICMP Trace [2], probabilistic packet marking (PPM), Source Path Isolation Engine (SPIE), Algebraic approach, Tunnel technologies, etc. There are some limitations of above approaches: a large amount of packets, analysis time slow convergence and complicated computation are needed. Background noise and Spoofed marking packets also affect its performance. Based on the above review of traceback approaches, we make the following brief summary: Ideally stopping an attacker is at the source. Even we cannot get the exact origin address, we still hope to gain the approximate source traffic identity. More closed to source side lead to the more efficiency. Using part traffic marking will bring out robust issue. Victim side has to make a complex decision before doing counterattack. Hash-based measures are adopted for lack mark space.

According to the analysis of [1] every packet may be carried in a different path to the destination (load balancing or unwanted isolation of the network routing), only the ingress interface on the router closest the source must be the same. Meanwhile ISPs may only use public addresses for the interfaces to customers and other networks, and use private addressing plans within their own networks. In this case full-path traceback will have low usefulness. Even if ISP's use public addresses, ISPs generally desired to disclose their topologies. Either of the two cases will greatly limit the effect of full-path traceback.

2. Related Work

Deterministic Packet Marking (DPM) [1] is a novel

This work was supported by University ITRC Project of MIC.