Demo Abstract: PACKTER: implementation of Internet traffic visualizer and extension for network forensics

Daisuke Miyamoto and Takuji Iimura

Received: 30 August 2012 / Accepted: 8 November 2012

Abstract Traffic visualization tools help network operators to maintain awareness of the status of a network, including anomalous activities. Unfortunately, the network operator may look away from the visualizer when beginning network forensics, such as launching a terminal application, logging into a server, and analyzing log files. Thus, the eyesight of the network operator will move from the visual screen even if valuable information is displayed. Our motivation is to develop the ability to use visualization tools as a network operation console. Whereas previous tools focused on outputting packet information, we herein extend the visualizer to accept inputting for operators to start their operations. Since little such software exists for our intent, we develop PACKTER, which is able to visualize traffic based on per-packet information in real time. We also extend PACKTER to have a function of negotiating to a network forensic system, which allows the operator to select an individual packet using a mouse, to start network forensics using a keyboard, and to receive results without looking away from the PACKTER viewer.

Keywords Network Forensic, IP Traceback, Traffic Visualization

1 Introduction

The creation of a new network operation style is beyond the visualization ability of today's networks. Whereas some visualization tools provide novel

D. Miyamoto
Information Technology Center, The University of Tokyo / Project PACKTER
2-11-16, Yayoi, Bunkyo-ku, Tokyo, 113-8658 JAPAN
E-mail: daisu-mi@nc.u-tokyo.ac.jp

T. Iimura
Project PACKTER
E-mail: uirou@packter.net
First IMC Workshop on Internet Visualization (WIV 2012), November 13, 2012, Boston, Massachusetts, USA.

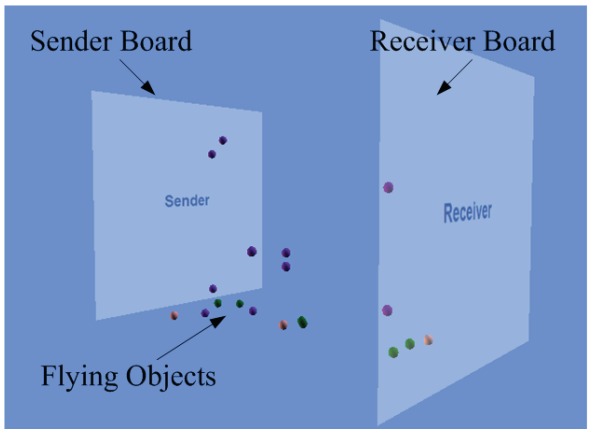

Fig. 1 Overview of PACKTER

graphics representing network activities, such tools are not designed to provide user-interfaces for network operation. While the tools continue to display valuable information, we assume that the visualizer provides a function for supporting network operations whereby the operator can continue to view the visualization screen.

As a preliminary study, we design and implement a traffic visualization tool called PACKTER [Project Packter(2008)], which consists of two programs: the PACKTER agent and the PACKTER viewer. The former collects packet information by primarily monitoring the network interface, and the latter displays the collected information on a three-dimensional screen, as shown in Fig. 1. Each packet appears at the sender board, and flying objects, denoting an individual packet, flow toward the receiver board with animation.

We then extend our developed program to equip a function for network forensics. There are various types of forensics, but we focus on investigating where the packet came from. Thus, the extended program is applicable to IP traceback which locates the sender of the packet even if the packet uses a spoofed source IP address. We refine PACKTER to work in conjunction with InterTrack [InterTrack(2009)], one of the IP traceback systems.

We herein demonstrate that PACKTER enables the network operator to maintain awareness of anomalous network activities, provides user interfaces for network forensics, and displays trace results. We hope that the present study, which involves the integration of the visualizer and the operation interface, will be of use in the development of new operating styles.

References

[InterTrack(2009)] InterTrack (2009) IP Traceback : A mechanism to find attack paths. Available at: `http://intertrack.naist.jp/`

[Project Packter(2008)] Project Packter (2008) PACKTER: A Multi Purpose Traffic Visualizer. Available at: `http://www.packter.net/index_e.html`