Flamingo: Visualizing Internet Traffic
J.Oberheide, M.Goff, M.Karir

Siarhei Kuryla

Networks and Distributed Systems seminar

March 9, 2009
Introduction

This paper:

▶ describes a set of visualization techniques to illustrate different aspects of the network traffic data;
▶ provides the details of the Flamingo software tool that implements those visualization techniques;
▶ gives examples how Flamingo can be used to perform network monitoring tasks;
Visualization Methods

- Based on a basic quad-tree algorithm.
- Traffic Volume by src/dst IP Address or Prefix.
- Traffic Volume by src/dst AS.
- Traffic distribution across src/dst ports.
- Traffic flows between Source IP - Destination IP Addresses or Prefixes.
- Traffic flows between src/dst IP/ports.
The Basic Quad-Tree Algorithm
Prefix: 10.0.0.0/3
First IP Address: 
00001010 0..0 0..0 00000000
Last IP Address: 
00001010 0..0 0..0 00000111
Traffic Volume by IP Address or Prefix
Traffic Volume by AS Number
Traffic distribution across src/dst Port
Source IP - Destination IP Traffic Flows
Source IP, Port - Destination IP, Port Traffic Flows
Flamingo Software Tool

- implements those visualization techniques;
- receives traffic data from netflow records;
- provide real-time traffic exploration, as well as playback stored netflow data;
- supports aggregated and non-aggregated modes;
- provides navigation and filtering capabilities that help to easily extract and monitor specific information;
Flamingo Architecture

- Client/Server Architecture
- A single server can act as collector for multiple netflow feeds
- A single server can support multiple clients