Visualization of Computer Networks
Bowen Zhang
Introduction


OverFlow: An Overview Visualization for Network Analysis

- **Intention**: Presenting the interactions between and within subnets
- **User**: Network analysts
- **Tasks**: Sifting through large amounts of raw network data and detecting anomalous network events through the simultaneous use of multiple visualizations.
OverFlow: An Overview Visualization for Network Analysis

Hiererarchy

- L1 192.168.0.0/16
- L2 192.168.2.0/24
- L2 192.168.5.0/24
OverFlow: An Overview Visualization for Network Analysis

Adding Hierarchy

Figure 5: The initial set of empty hierarchies (or organizations). The user right-clicks a black circle in order to edit the selected hierarchy.

Figure 6: A dialog that allows the user to specify the name of an organization. The data grid displays information about the network hierarchy with the specified input name, as retrieved from the database.
OverFlow: An Overview Visualization for Network Analysis
OverFlow: An Overview Visualization for Network Analysis

Case Study

(a) The first day.

(b) The second day.

(c) The third day.

(d) The fourth day.
OverFlow: An Overview Visualization for Network Analysis

- Contribution: Quickly determining if there is traffic between organizations that should not exist, or if the characteristics of that traffic (e.g., volume) have changed.

- Critique
  - Why concentric circle?
  - What if handling with large number of hierarchies?
Countering Security Information Overload through Alert and Packet Visualization

Problem
The massive amount of security data that network sensors and host-based applications generate can quickly overwhelm the operators charged with defending the network.

Goals
Providing insightful high-level overviews and detail on demand to support analysis of intrusion alarms and network packets
Countering Security Information Overload through Alert and Packet Visualization

**RainStorm**: Provides high-level overviews of intrusion-detection alerts.

**Rumint**: Detailed insights into packet-level network traffic.
RainStorm-Goal

IDS RainStorm presents alarm data in an overview where system administrators can get a general sense of network activity and easily detect anomalies. Zooming and drilling down for details can be performed at the user’s discretion. After using IDS RainStorm to rapidly identify events of interest, system administrators can then examine the associated network packets using Rumint for more detailed analysis.
RainStorm-High level

y-axis: IP range

x-axis: Time

Pixel color

Glossing- zoom view
RainStorm - Zoom view
Rumint- Goal

The primary design goal of Rumint is letting users view a large number of network packets in a way that supports rapid comparison, deep and broad semantic understanding, and highly efficient analysis. Allowing intuitive interaction to remove noise and highlight packets of interest.

The other goal is to complement higher level systems such as IDS RainStorm. IDS RainStorm excels at identification of events of interest, but lacks comprehensive tools for analyzing the underlying network packets that caused the event. Rumint could fill this gap.
Rumint-Structure

7 visualizations:

- scrolling text display,
- parallel coordinate-plot display,
- glyph-based animation display,
- thumbnail toolbar,
- binary rainfall visualization,
- byte frequency display, and
- detail display.
Rumint-Rainfall Visualization

- Used for plot packet analysis
- One horizontal line per packet
- Packet represent if binary form
- Three bites made up one pixel
- 1000 packet per screen
Rumint-Rainfall Visualization

Benefit for

- Rapidly compare packets contents and lengths
- Identify identical values between packets
Rumint-Byte Frequency Visualization

- One packet per horizontal line.
- There are 256 positions along the horizontal axis which correspond to the presence or absence of byte values (0–255) in the given packet.
- Pixels are colored based on the frequency with which the corresponding byte appears relative to each packet.
Rumint-Byte Frequency Visualization

Benefit for

- Rapid comparison of packet structure and contents
- Detecting the use of encryption, fingerprinting executable files
- Detection of ASCII text, and analysis of polymorphic network worms.
Countering Security Information Overload through Alert and Packet Visualization

Contribution:

IDS RainStorm vs. Rumint = Overview vs. Detail

Complete each other successfully!

Critique?
Comparison

- Communication behavior vs. Overall behavior
- Several days investigation vs. Real time sensitive
- Naive vs. Complex and fantastic
The end - Questions?

Happy end term!