Network Security Visualisation Techniques in Early Warning Systems

Marcus Weseloh

Hamburg, 27.01.2010
Motivation
“One picture is worth ten thousand words.”
Words in image:
> 10,000

Words in my head:
3
“That looks pretty!”
Goal:

Find visualisation techniques that provide valuable new insights for analysts working with early warning systems.
Key Questions

- What are the cognitive principles behind effective visualisation?
- Which tasks could benefit from visualisation?
- Which visualisation technique is suitable for which task?
Talk Overview

➔ The CarmentiS Early Warning System
➔ Information Visualisation
➔ Traffic Analysis Tasks
➔ Review of Visualisation Techniques
➔ Implementations
The CarmentiS System
CarmentiS

- Project of CERT-Verbund and BSI.
- Based on netflow toolkit by Peter Haag of SWITCH-CERT (nfdump/nfsen)
- Extends architecture to include other event sources like honeypots, IDS and malware sensors.
CarmentiS uses netflow as base for all other types of events therefore:

Focus on visualisation techniques suitable for traffic analysis!
Information Visualisation

Principles of Visual Perception
Preattentive Processing

- Processing of visual attributes prior to conscious thought.
- Enables us to encode information in such a way that it “pops out” at the viewer.
Some Examples

Find the “odd one out”!
Size
Orientation
Parallelism
Parallelism
Parallelism
Preattentive Attributes

- Size
- Orientation
- Colour
- Shape
- Concavity / Convexity
- Texture

... and more
Gestalt Principles

- Kurt Koffka, German Psychologist (1935)
- Formulated as series of laws
- Explains human pattern perception
- Useful to clarify grouping and ease perception of clusters in visualisations
Proximity
Similarity
Connectedness
Continuity
Use of Colour
Colour for Categorical Data
Colour for Continuous Data

Rainbow Scale?
There is no intrinsic order in the rainbow colour scale!
Colour for Continuous Data
Traffic Analysis Tasks
Information Seeking Mantra:

“Overview first, zoom and filter, details on demand”

Shneiderman (1996)
Four Stages in Traffic Analysis

- Anomaly detection
- Identification of anomaly boundaries
- Anomaly analysis
- Detailed flow information
Anomaly Detection

Goal: Spot significant changes in traffic flows that could indicate an anomaly.
Anomaly Boundaries

Goal: Find the boundaries of the anomaly to reduce amount of processed data.
Anomaly Analysis

Goal: Identify the anomaly as a known type or find attributes that could identify a new anomaly in the future.
Flow Details

View all information for a single flow record.
Four Stages in Traffic Analysis

- Anomaly detection
- Identification of anomaly boundaries
- Anomaly analysis
- Detailed flow information
Review of Visualisation Techniques
Scatter Plots

![Scatter Plot Diagram](image-url)
Enhanced Scatter Plots
Implementations
Web-based Visualisations

- Implemented using plug-in interface
- PortMap – specialised scatter plot
- LinkGraph – directed graphs
- HeatMap – ... an Ipv4 heat map
PortMap

- Specialised scatter plot
- Displays whole TCP & UDP port range (0 – 65,535)
- X-Axis: port number % 256
- Y-Axis: port number / 256
- Colour encodes number of flows / bytes / packets
PortMap

0 255
256 511
512 767
65280 65535
TCP dst flows, 48h
TCP dst flows, 48h, Src Port 80, Syn Ack Flags
TCP dst flows, 48h, Src Port 80, Syn Ack Flags, 48 Bytes
Conficker.C Pattern

Source: www.bamsoftware.com/wiki/Nmap/PortSetGraphics
One million generated port numbers, Fifield

24h darknet UDP dst flows, 17. June 2009
One million generated port numbers, Fifield

48h darknet UDP dst flows, 24.-25. January 2010
TAViS – Traffic Analysis Visualisation System
TAViS Architecture

- Client – Server architecture
- Web-Service provides access to CarmentiS database
- Possibility to aggregate and compress data in Web-Service
- Java client accesses Web-Service
- Modular architecture for easy development of new visualisations
Parallel Coordinate Plot

Src IP  Src Port  Dst Port  Dst IP
Parallel Coordinate Plot

Src IP  Src Port  Dst Port  Dst IP
Evaluation

- First feedback from analysts very positive.
- More evaluation necessary!
- Traffic analysis tasks heavily influenced by current user interface, compare with other early warning systems.
Summary

- Identified traffic analysis tasks
- Reviewed suitable visualisation techniques
- Implemented three web-based visualisations as CarmentiS plug-ins
- Implemented TAViS and a parallel coordinate display.
Thank you for your attention!

E-Mail: weseloh@dfn-cert.de