

NetVis

Network Security Visualisation Tool



James Nicholls, Dominik Peters, Albert Slawinski,
Thomas Spoor, Sergiu Vicol

Project Goals

We declared in our specification that we would implement:

An application to assist an **observer** in the detection and analysis of potential network attacks by visualising network traffic in an intuitive and meaningful way.

The aim was to improve situational awareness of a network in the hope that the user can identify an attack faster than automated analytical techniques (i.e. using an IDS).

To achieve this we needed to build a graphical network analysis program which would receive packets from the IP layer and display the data in a human-friendly format.

Design Choices

The decisions we made in the early stages of the project;

- Java / Swing / OpenGL graphics API
- Main network map for familiarity
- Variety of visual styles
- Overview → zoom and filter → details on demand
[Shneiderman, 1996]

Teamwork

Tools used to encourage Synergy™ between team members

- Version control, code hosting: **GitHub**
- Distribution of tasks: **Google Drive, GitHub**
- Meeting planning: **Facebook, Doodle**
- Shouting at people: **Facebook, GitHub**