

NetVis

Network Security Visualisation Tool



Sponsor: Jassim Happa, University of Oxford

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

Project Goals

Implement an application to assist an **observer** in the detection of potential network attacks.

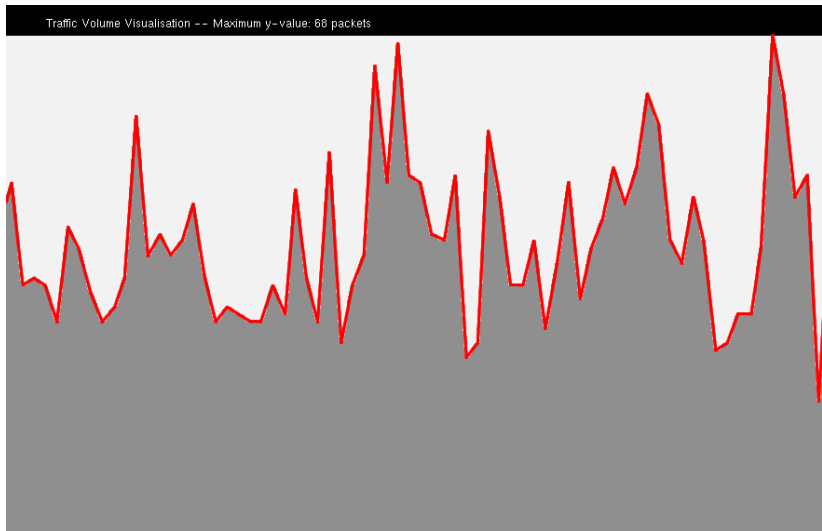
Improve situational awareness of a network faster than automated analytical techniques (i.e. using an IDS).

Design Choices

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

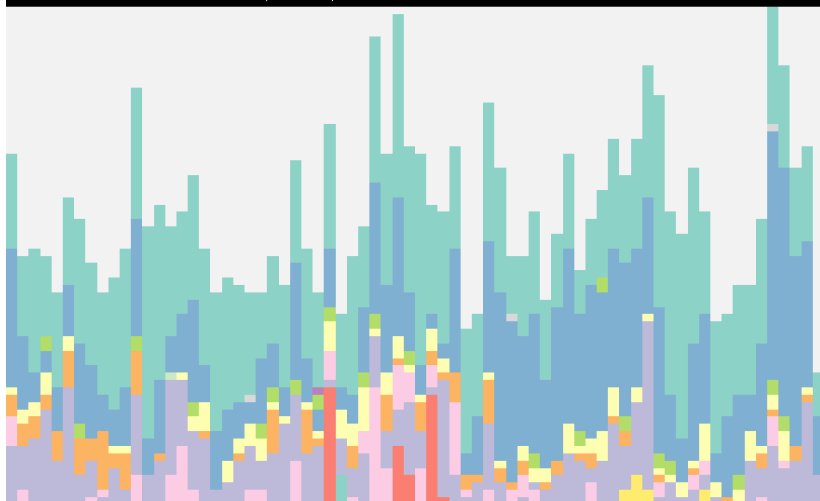
- Java / Swing / OpenGL graphics API
- Network “map” for familiarity
- Overview → zoom and filter → details on demand
[Shneiderman, 1996]
- Variety of visual styles

An unhelpful visualisation



A better visualisation

Traffic Volume Visualisation -- Maximum y-value: 68 packets



Protocol Colour Key

ARP (2083)

ICMPv6 (1436)

MDNS (1029)

SSDP (211)

DHCPv6 (184)

LLMNR (174)

DNS (84)

UDP (72)

NTP (20)

IPv6 (7)

IGMPv2 (6)

EAP (6)

EAPOL (5)

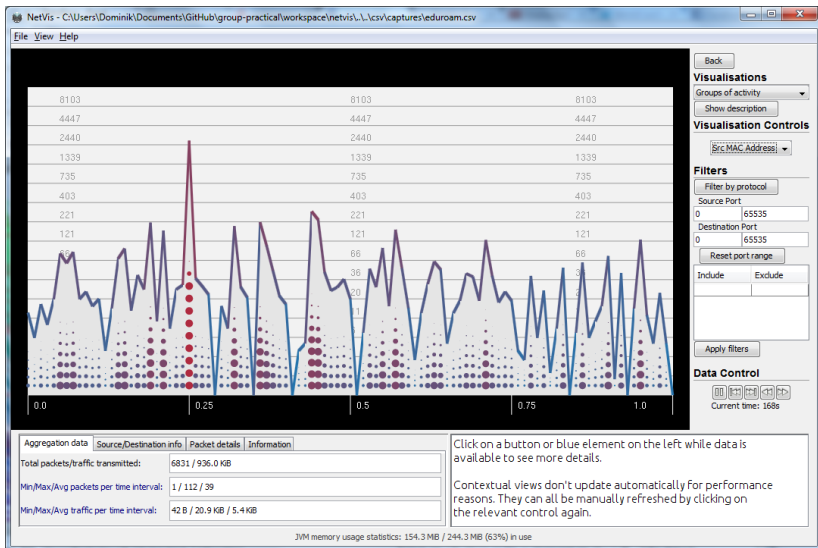
TLSv1 (3)

Teamwork

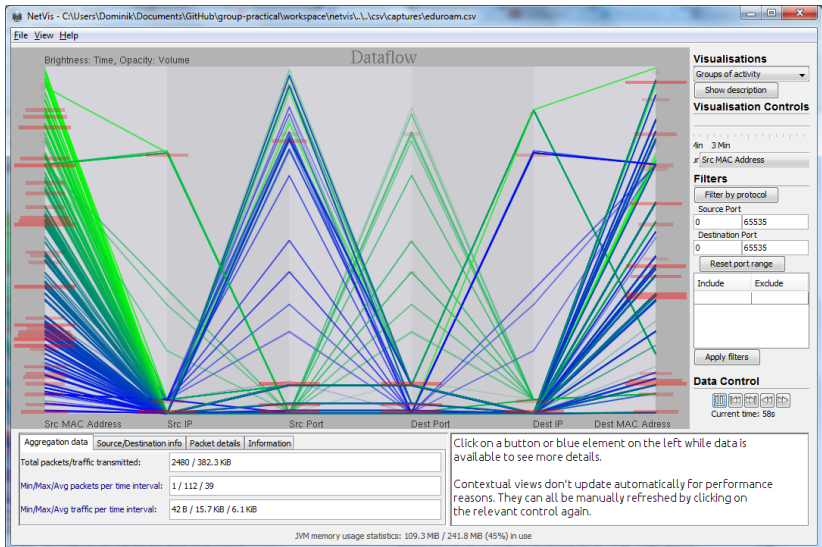
Tools used to promote Synergy™ between team members

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

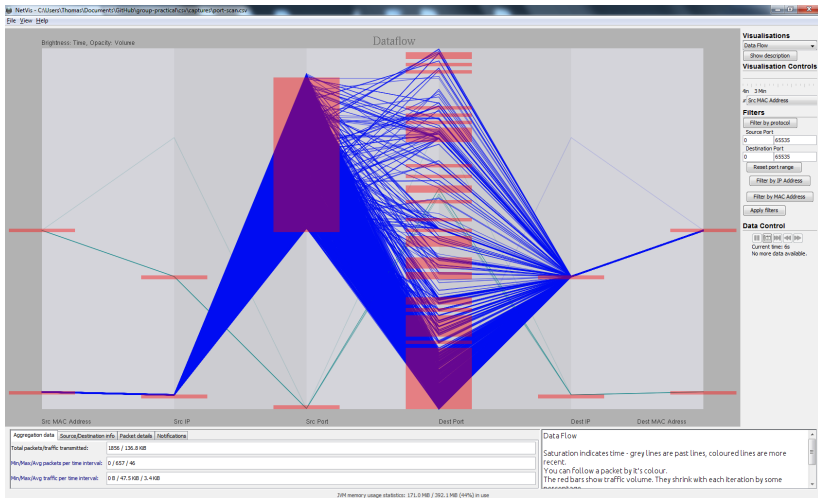
Attributes Visualisation



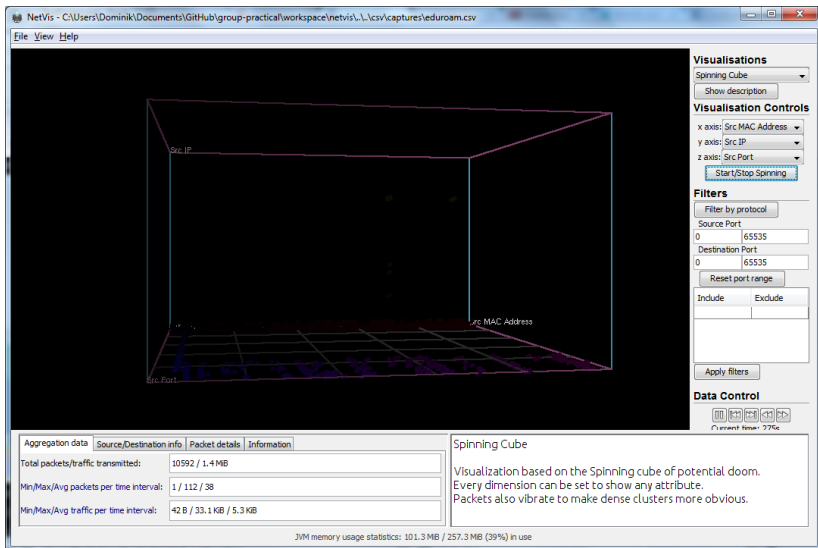
Dataflow Visualisation



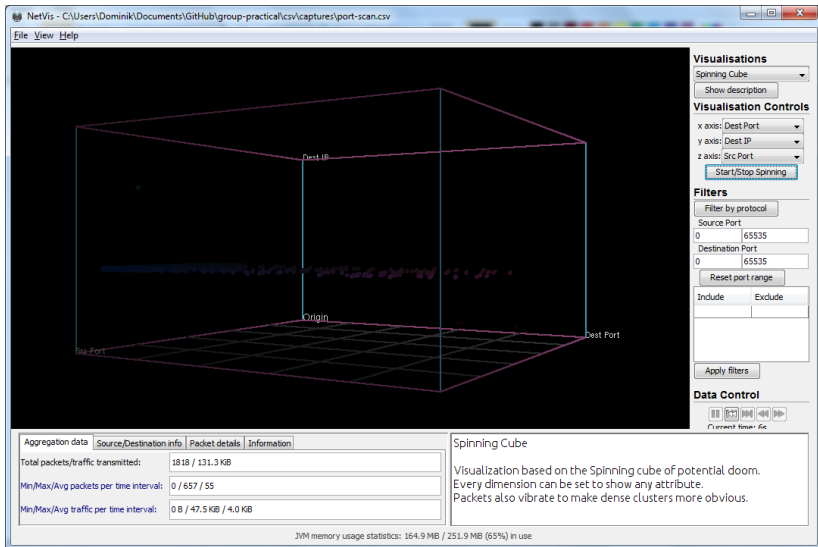
Port Scan Attack



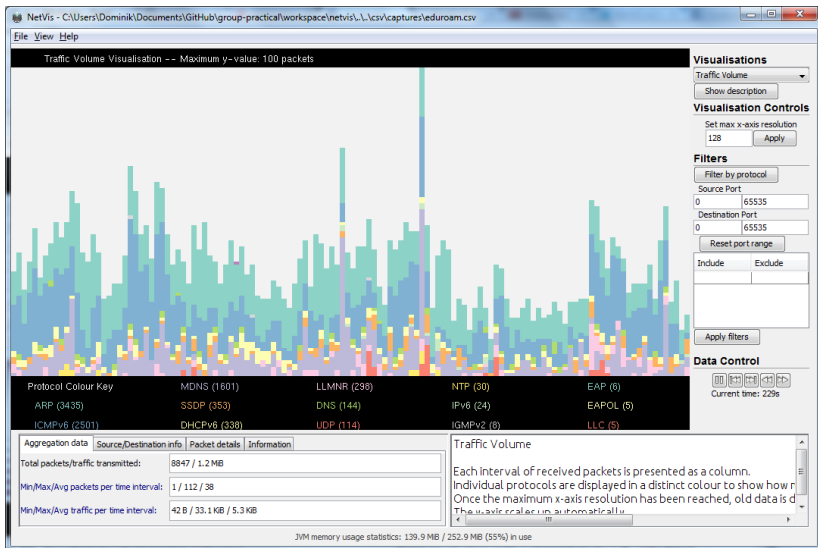
Spinning Cube Visualisation



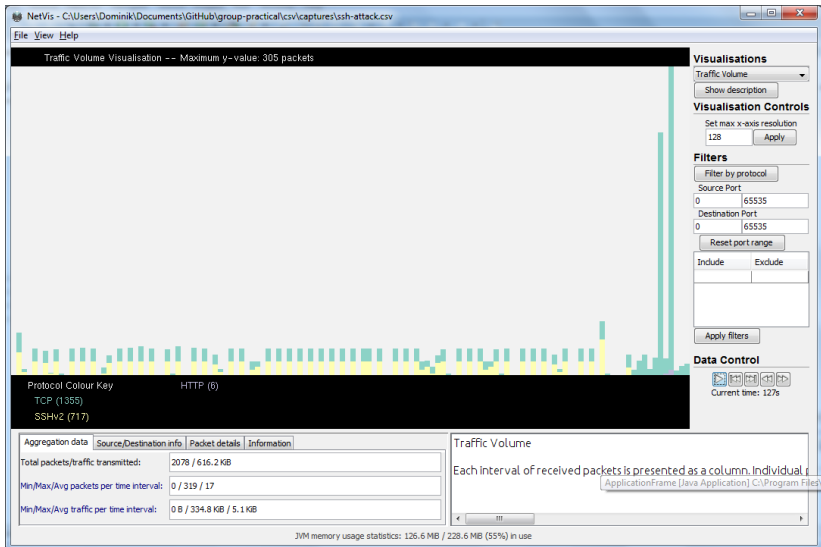
Port Scan Attack



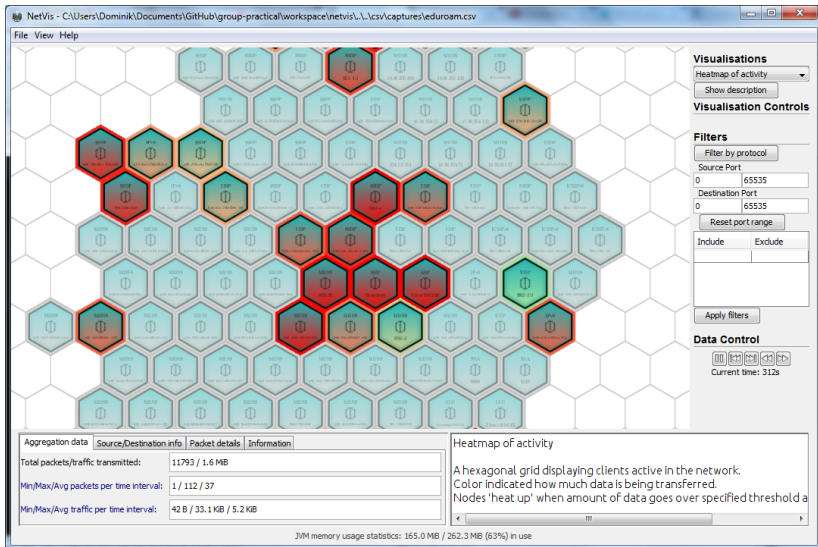
Traffic Volume Visualisation



SSH Brute Force Attack



Heat Map Visualisation



Activity Groups Visualisation

