Overview

- “The problem”
- “The other solutions” - literature review
  - Text based, 2D, 3D, though to “Immersive”
- L3DGE
- Brief “home network” update (time permitting)
“The problem”

- Monitoring of the many distinct, “black boxes that make up a modern IP network –
  - Hard to do.
- The interpretation of the raw data gathered in the previous step –
  - Hard to do.
- Implementing a solution back onto all the, distinct boxes that make up the network –
  - Hard to do.
  - Trained professionals required to perform this work

Can we?

- Lower the skills required to make a positive contribution to the monitoring, diagnosing and controlling of an IP network...
  - Let junior administrators lend a helping hand
  - Train them quicker
- Help you see the things you didn't know you didn't know by...
- Creating suitably high-level, interactive and real-time abstractions and visualisations
Why turn to visualisation?

- To allow a human insight into (large amounts of) data
- In hope of creating that “Ah Ha!” moment:
  - “… quite often, the sight of a graphical encoding of data causes an 'Ah Ha!' reaction in the viewer in the sense that a useful discovery has been made.” [1]
  - “…solving a problem simply means representing it so as to make the solution transparent”. [2]

Example - “Beck's map”

- Pre 1932
Example - “Beck's map”

- Pre 1932

Example - “Beck's map”

- Abandon scale altogether...
Example - “Beck’s map”

- And today...
- Note: Not a replacement for all maps of London, but for it’s purpose - highly effective.

Select Network Data Vis’ Literature

- Text based “visualisations”
- 2D visualisations
  - Static (including “updating graphs”)
  - Dynamic (where the “view” of the data can be changed)
- 3D visualisations
  - Static (Do any exist? - The odd 3D graph maybe...)
  - Dynamic
- Immersive 3D – A presence of users in-world
Text based visualisations

- tcpdump
- trafshow


Text based visualisations

- Wireshark

Text based visualisations

- Bayesviz


Static 2D visualisations

- MRTG (RRD)
- Packet heat maps

“MRTG: The multi router traffic grapher,”
http://oss.oetiker.ch/mrtg/.

Dynamic 2D visualisations

- NVisionIP


Dynamic 2D visualisations

- VisflowConnect(-IP)

Dynamic 2D visualisations

- IDS RainStorm and Rumint


CAIA - Literature Review Series http://caia.swin.edu.au wazz@swin.edu.au 17th Sep '10 2:14 Page 1/

Dynamic 2D visualisations

- TNV (Time-based Network traffic Vis)

3D visualisations

- SeeNet 3D (1995)


3D visualisations

- Spinning Cube of Potential Doom (& Inetvis)

Immersive 3D visualisations

- Untitled – Lazar et al. (1995)
  - Pictures hard to get
- Concept of in-world changes altering the underlying network configuration
  - Context: ATM networks


CAIA - Literature Review Series http://caia.swin.edu.au wazz@swin.edu.au 3rd Sep 2009 Page 21

Immersive 3D visualisations

- Cybernet (2000)
  - Has a network visualisation component, among others

Immersive 3D visualisations

- psDoom

What is the next step?

- What are some the key points from the literature?
  - Extensible / Flexible
  - Interaction with data set
  - Interaction with underlying systems
  - Real-time
  - Scalability
  - Collaborative

- On to our work...
Early work

- Warren writes an OpenGL application (GLUT lib)
  - 3VEN (3D Visualisation Environment for NIDS)
  - or it's working title, “Seg Fault”


Early work

- “Untitled” – First pass at game modification
- Open source “Cube” engine
  - Unique in-world map modification capabilities
- (Now known as “Cube 2: Sauerbraten”)
Early work

- “Untitled” – Second go at game modification
- Open source “Cube” engine
- No more monsters!

Early work

- “LTMON”
  - Open source “Quake III” engine
  - Visualising game server discovery process
Leveraging 3D Game Engines (L3DGE)

- Cisco URP grant
  - http://caia.swin.edu.au/urp/l3dge/
- Hired Lucas Parry for a year of development time
- “OpenArena” engine (a fork of the Quake III engine)

How does it work?

3D Game Clients → Network → 3D Game Engine Server

- System collaborators as players
- 3D Game Engine Server (Keeps ‘world’ state)
  - Input Abstraction Layer
  - Output Abstraction Layer
  - External control commands (ACLs, etc)
  - Monitored systems (packets, netflow, SNMP, etc)
A quick word on “Greynets”

- Greynet host
  - A passive listener on an IP address within an enterprise network
- Detects network scans & other unsolicited traffic
  - Usually bad intent
- Greynet – Many of these passive listeners scattered around your enterprise network on various subnets

http://caia.swin.edu.au/urp/l3dge/tools/lupsmon/
Home networking

- Presented previously...

Create the greatest home network of all time in 3 easy steps (and 472 difficult ones)

Warren Arrop
wazz@swin.edu.au

Lawrence Stewart
lastewart@swin.edu.au
Old things...

- VoIP (Asterisk)
  - Crazy call routing as the norm...
- Tunnels (vtun)
  - File sharing
  - CAIA/Swin access
  - Printing
- RAID/Rolling backups
- WiFi links

New things...

- VoIP - Asterisk
  - Caller ID based routing
    - Callback
  - “Meetme” conferencing
- Encrypted off-site backup
- IPSec
- IPv6
Latex - “Workflow”

- Inkscape for diagrams
  - Win/Mac/UNIX
  - Uses SVG as it's native format
- Makefile for latex build and image conversion from SVG → pdf/eps

Questions?