SWINBURNE UNIVERSITY OF TECHNOLOGY

Techniques for immersive and collaborative IP network management

Warren Harrop

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

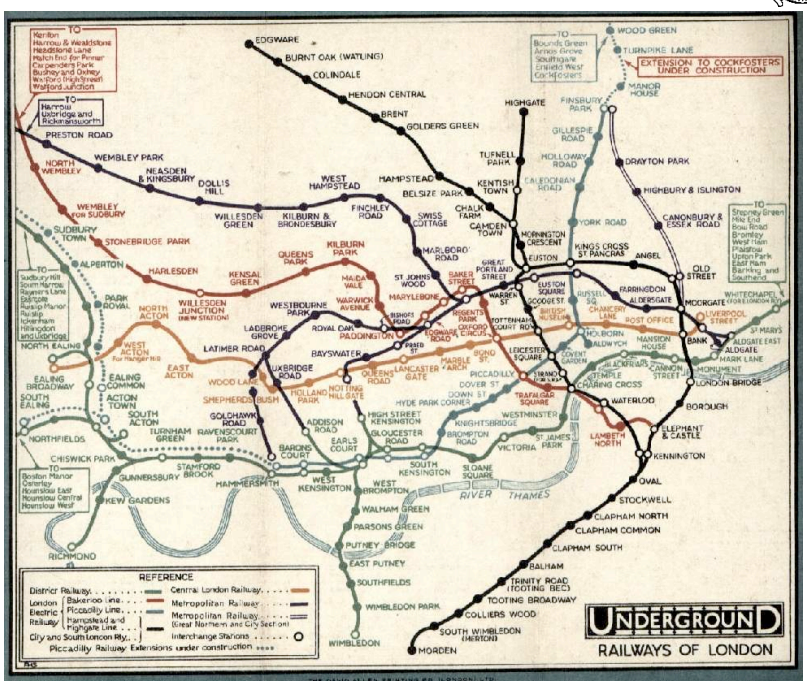
Why turn to visualisation?

- 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]

[1] Spence, R. (2007) Information Visualiszation Design for Interaction (2nd edition), ACM Press
[2] Simon, H. (1996) The sciences of the artificial (3rd edition), MIT Press

Example - “Beck's map”

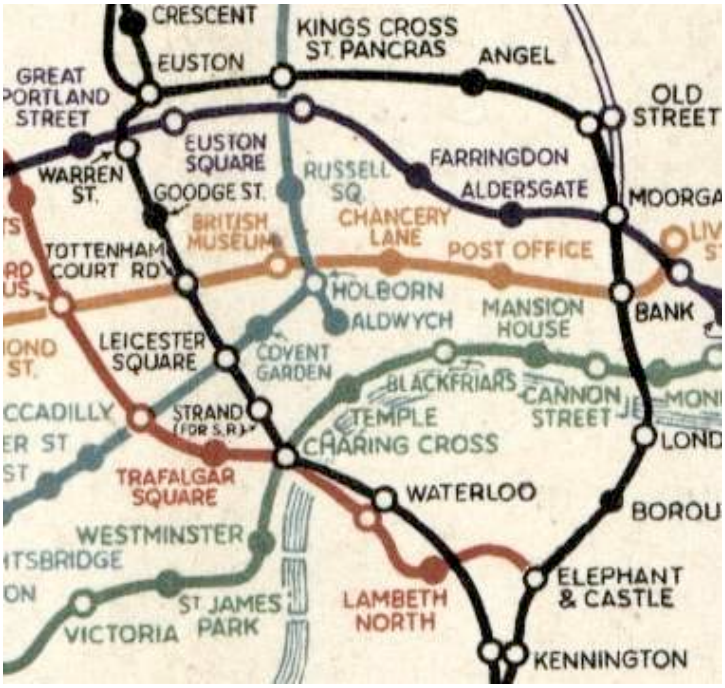
- Pre 1932



http://www.cs.bc.edu/~syu/artvis/course/project/roadmap/index.html

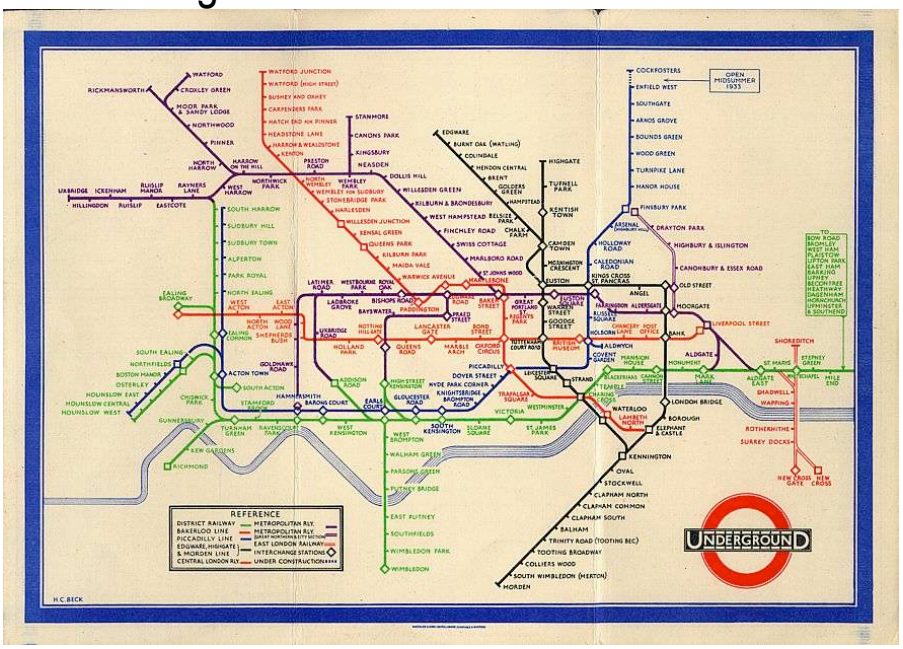
Example - “Beck's map”

- Pre 1932



Example - “Beck's map”

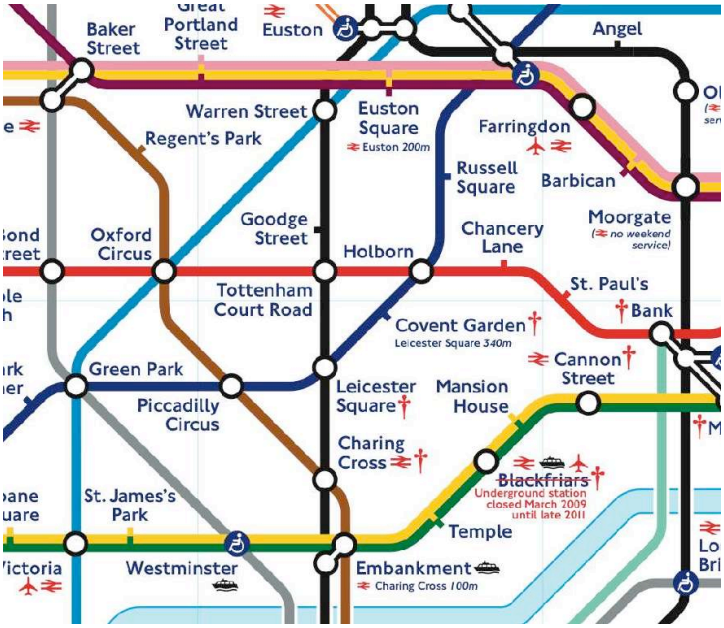
- Abandon scale altogether...



http://www.cs.bc.edu/~syu/artvis/course/project/roadmap/index.html

Example - “Beck's map”

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



http://www.tfl.gov.uk/assets/downloads/Standard-Tube-map.pdf

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

```
xterm
02:21:33.273245 IP 172.16.4.101.51134 > 210.50.193.198.993: . ack 175 win 65535
<nop,nop,timestamp 1446933041 1026637750>
02:21:33.274014 IP 172.16.4.101.51134 > 210.50.193.198.993: P 75:144(69) ack 175
 win 65535 <nop,nop,timestamp 1446933041 1026637750>
02:21:33.302463 IP 210.50.193.198.993 > 172.16.4.101.51134: P 175:276(101) ack 1
44 win 8225 <nop,nop,timestamp 1026637813 1446933041>
02:21:33.303103 IP 172.16.4.101.51134 > 210.50.193.198.993: . ack 276 win 65535
<nop,nop,timestamp 1446933041 1026637813>
02:21:33.306850 IP 172.16.4.101.51134 > 210.50.193.198.993: P 144:181(37) ack 27
6 win 65535 <nop,nop,timestamp 1446933041 1026637813>
02:21:33.335085 IP 210.50.193.198.993 > 172.16.4.101.51134: P 276:329(53) ack 18
1 win 8225 <nop,nop,timestamp 1026637877 1446933041>
02:21:33.335897 IP 172.16.4.101.51134 > 210.50.193.198.993: . ack 329 win 65535
<nop,nop,timestamp 1
02:21:34.209139 IP 1
in 33304 <nop,nop,ti
02:21:34.209149 IP 1
n 33304 <nop,nop,tim
02:21:34.209174 IP 1
 33304 <nop,nop,time
02:21:34.211905 IP 1
,nop,timestamp 14469
02:21:34.212139 IP 1
,nop,timestamp 14469
```

```
xterm
From Address                    To Address                      Prot      Bytes CPS
================================================================================
172.16.4.1..22                  172.16.4.109..55818             tcp      373876 273
172.16.4.109..55818             172.16.4.1..22                  tcp       44500 62
172.16.4.1..139                 172.16.4.15..4646               tcp         137 27
172.16.4.15..4646               172.16.4.1..139                 tcp         133 26
172.16.4.1..53                  172.16.4.18..1118               udp         105 21
172.16.4.18..1118               172.16.4.1..53                  udp          55 11
172.16.4.1..631                 172.16.4.18..1087               tcp          52 10
172.16.4.18..1087               172.16.4.1..631                 tcp          52 10

(fxp1)     11126 kb/total        3 pkts/sec        369 bytes/sec          Page  1/1
```


"Tcpdump/libpcap public repository," http://www.tcpdump.org/, January 2009. [Online].
"trafshow," http://soft.risp.ru/trafshow/, January 2009. [Online].

Text based visualisations

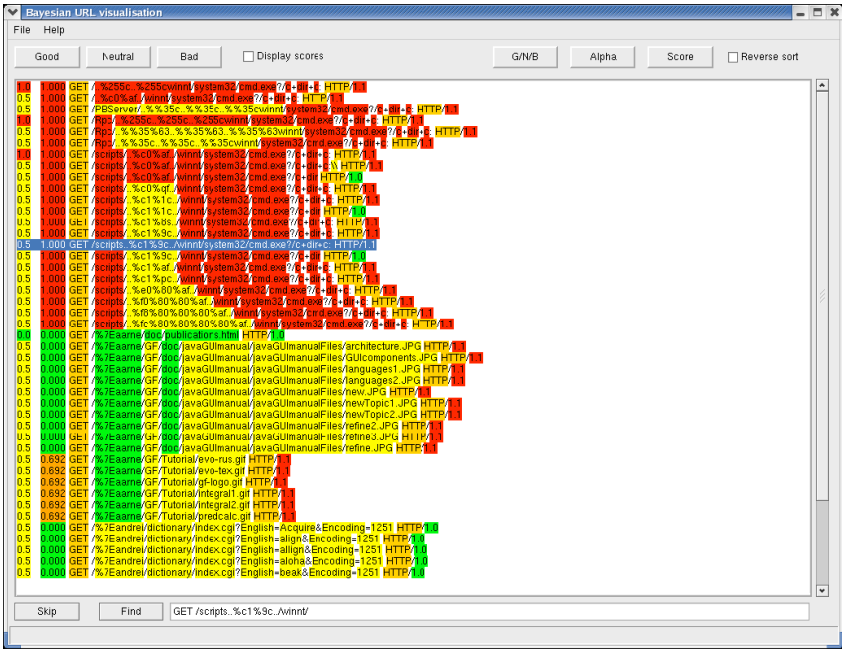
- Wireshark

```
dump.pcap - Wireshark
File  Edit  View  Go  Capture  Analyze  Statistics  Help
Filter:                                  Expression...  Clear

No.  Time        Packet length  Source          Destination     Protocol  Info
60   11.990696   66             172.16.4.101    172.16.4.1      TCP       52610 > ssh [ACK] Seq=1382 Ack=1754
61   14.383573   146            172.16.4.101    172.16.4.1      SSHv2     Encrypted request packet len=80
62   14.386784   114            172.16.4.1      172.16.4.101    SSHv2     Encrypted response packet len=48
63   14.386854   66             172.16.4.101    172.16.4.1      TCP       52610 > ssh [ACK] Seq=1462 Ack=1802
64   14.387153   146            172.16.4.101    172.16.4.1      SSHv2     Encrypted request packet len=80
65   14.389531   98             172.16.4.1      172.16.4.101    SSHv2     Encrypted response packet len=32

▷ Frame 61 (146 bytes on wire, 96 bytes captured)
▷ Ethernet II, Src: Apple_06:18:9e (00:1b:63:06:18:9e), Dst: Intel_46:9e:07 (00:02:b3:46:9e:07)
▷ Internet Protocol, Src: 172.16.4.101 (172.16.4.101), Dst: 172.16.4.1 (172.16.4.1)
▷ Transmission Control Protocol, Src Port: 52610 (52610), Dst Port: ssh (22), Seq: 1382, Ack: 1754, Len: 8
▷ SSH Protocol
  [Packet size limited during capture: SSH truncated]

0000  00 02 b3 46 9e 07 00 1b  63 06 18 9e 08 00 45 00   ...F.... c.....E.
0010  00 84 3c 30 40 00 40 06  9d bd ac 10 04 65 ac 10   ..<0@.@. .....e..
0020  04 01 cd 82 00 16 5d 3c  f4 d7 a4 1b 6e d9 80 18   ......]< ....n...
0030  ff ff 5c 92 00 00 01 01  08 0a 50 c3 8a 87 9f 84   ..\..... ..P.....
0040  c1 a0 96 93 76 34 72 ed  a4 8e 24 b4 6d bd 60 a5   ....v4r. ..$.m.`.
0050  78 f6 f4 ce 4e c4 58 42  79 db 62 73 28 05 46 8e   x...N.XB y.bs(.F.

File: "/Users/warren/dump.pcap" 934...   Packets: 94 Displaye...   Profile: Default
```


"Wireshark: Go deep," http://www.wireshark.org/, January 2009. [Online].

Text based visualisations

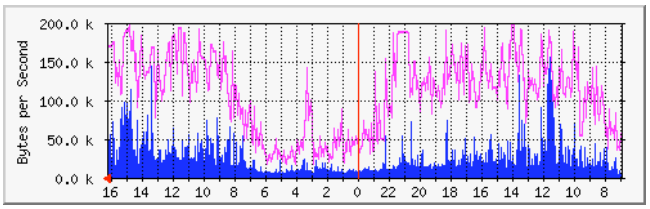
- Bayesviz



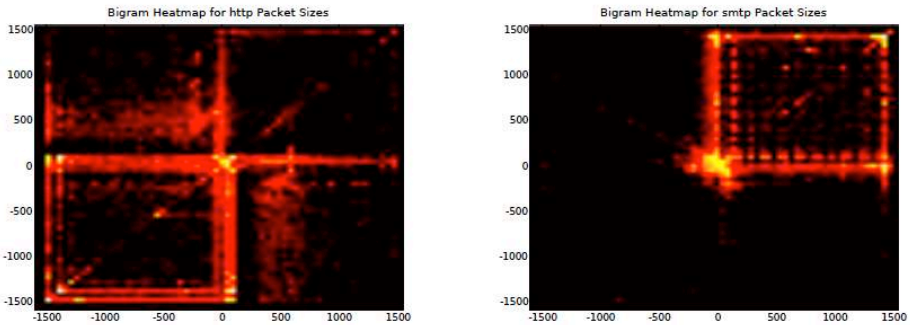
·S. Axelsson, "Combining a bayesian classifier with visualisation: understanding the ids," in VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. New York, NY, USA: ACM, 2004, pp. 99–108.

Static 2D visualisations

- MRTG (RRD)
- Packet heat maps



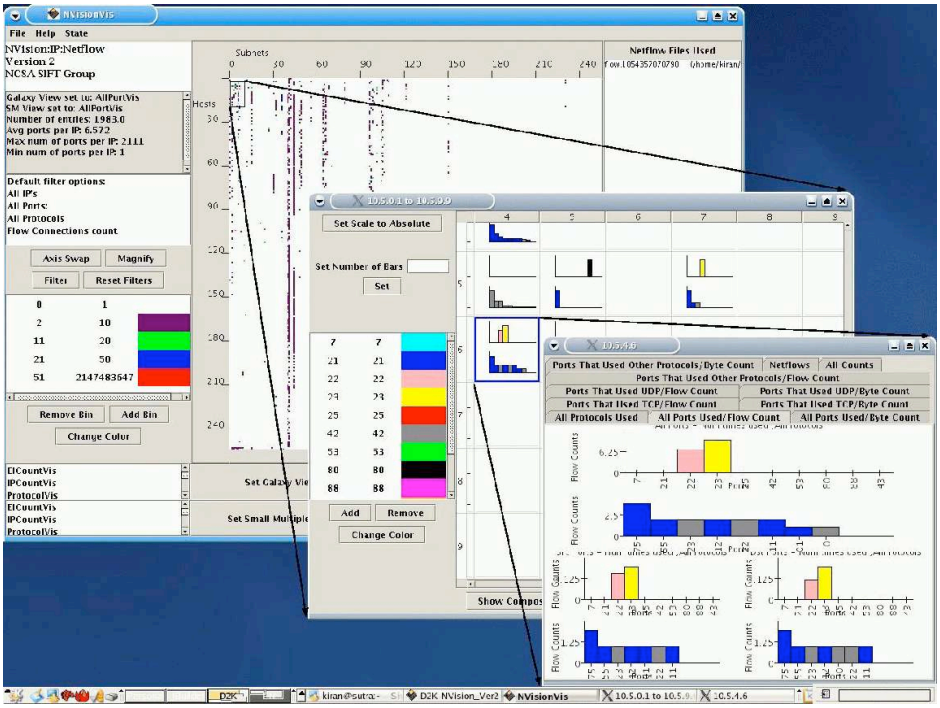
·"MRTG: The multi router traffic grapher," http://oss.oetiker.ch/mrtg/, January 2009. [Online].
·C. V. Wright, F. Monrose, and G. M. Masson, "Using visual motifs to classify encrypted traffic," in *VizSEC '06: Proceedings of the 3rd international workshop on Visualization for computer security*. New York, NY, USA: ACM, 2006, pp. 41–50.



(a) HTTP (b) SMTP

Dynamic 2D visualisations

- NVisionIP

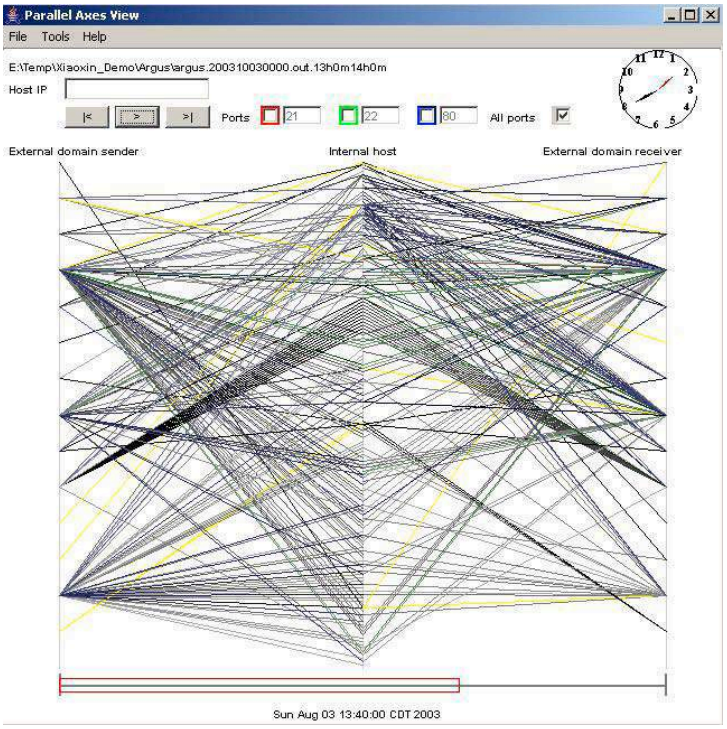


·K. Lakkaraju, W. Yurcik, and A. J. Lee, "Nvisionip: netflow visualizations of system state for security situational awareness," in VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. New York, NY, USA: ACM, 2004, pp. 65–72.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Dynamic 2D visualisations

- VisflowConnect(-IP)

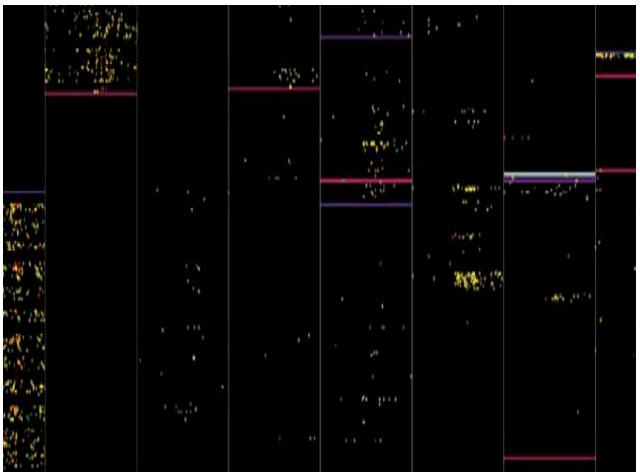


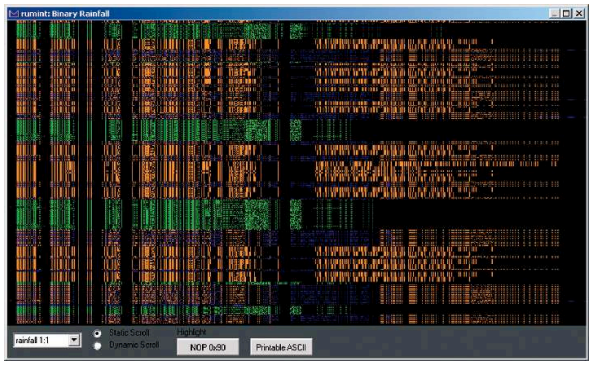
·X. Yin, W. Yurcik, M. Treaster, Y. Li, and K. Lakkaraju, "Visflowconnect: netflow visualizations of link relationships for security situational awareness," in VizSEC/DMSEC '04: Proceedings of the 2004 ACM workshop on Visualization and data mining for computer security. New York, NY, USA: ACM, 2004, pp. 26–34.

SWINBURNE UNIVERSITY OF TECHNOLOGY

Dynamic 2D visualisations

- IDS RainStorm and Rumint

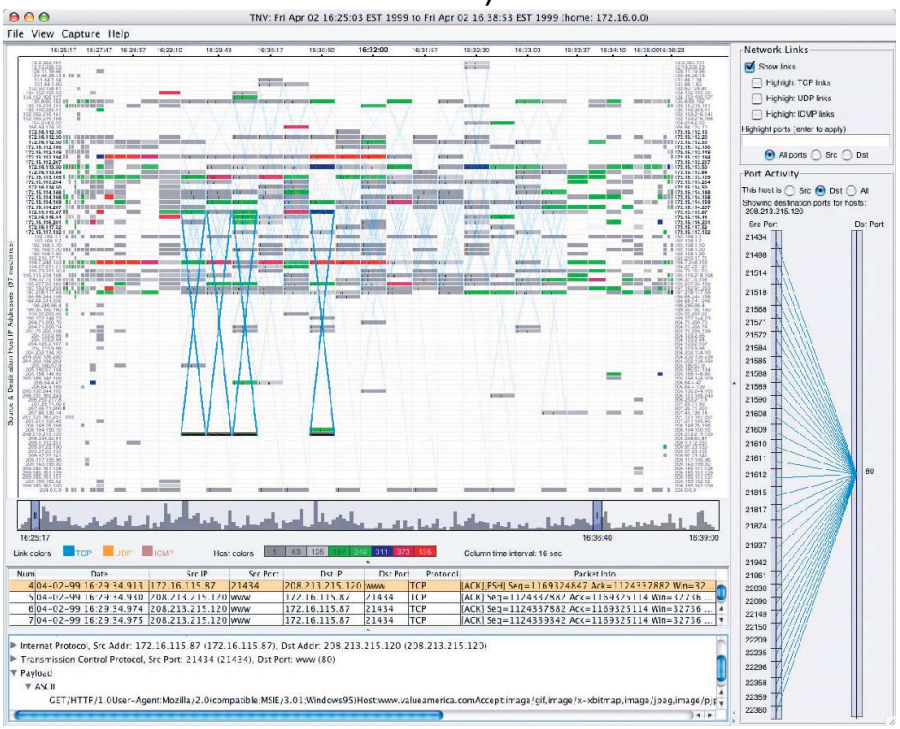




·G. Conti, K. Abdullah, J. Grizzard, J. Stasko, J. A. Copeland, M. Ahamad, H. L. Owen, and C. Lee, "Countering security information overload through alert and packet visualization," IEEE Comput. Graph. Appl., vol. 26, no. 2, pp. 60–70, 2006.

Dynamic 2D visualisations

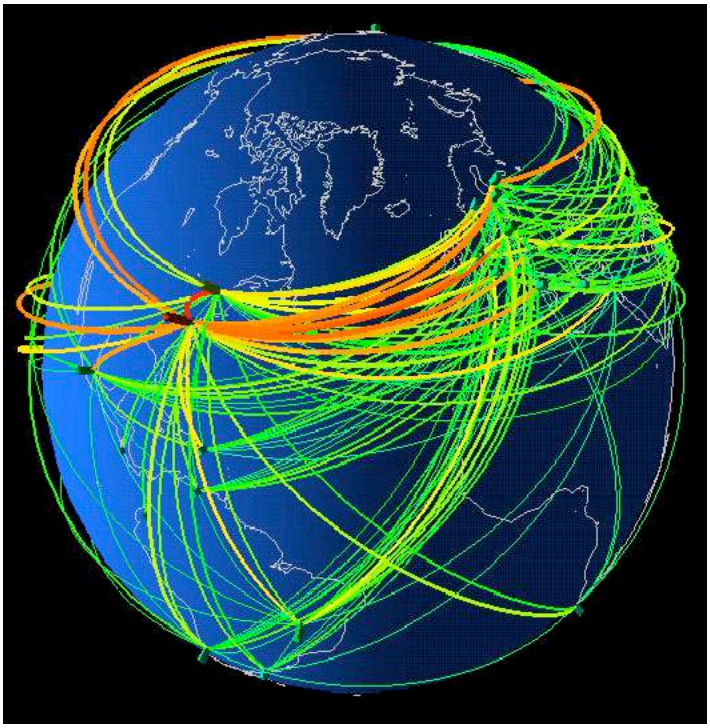
- TNV (Time-based Network traffic Vis)



·J. R. Goodall, W. G. Lutters, P. Rheingans, and A. Komlodi, "Focusing on context in network traffic analysis," IEEE Comput. Graph. Appl., vol. 26, no. 2, pp. 72–80, 2006.

3D visualisations

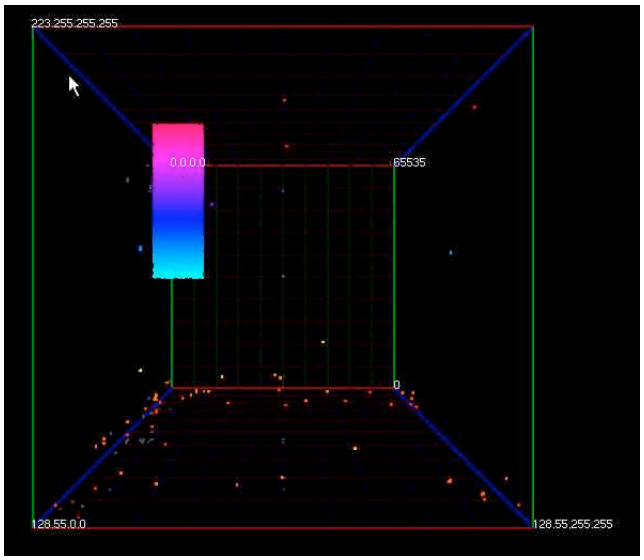
- SeeNet 3D (1995)

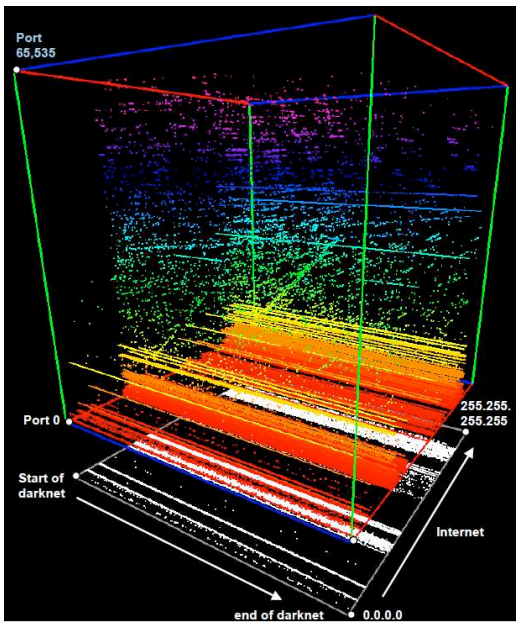


·K. C. Cox and S. G. Eick, "Case study: 3d displays of internet traffic," in INFOVIS '95: Proceedings of the 1995 IEEE Symposium on Information Visualization. Washington, DC, USA: IEEE Computer Society, 1995, p. 129. 61.

3D visualisations

- Spinning Cube of Potential Doom (& Inetvis)





·S. Lau, "The spinning cube of potential doom," Commun. ACM, vol. 47, no. 6, pp. 25–26, 2004.
·J.-P. van Riel and B. Irwin, "Inetvis, a visual tool for network telescope traffic analysis," in Afrigaph '06: Proceedings of the 4th international conference on Computer graphics, virtual reality, visualisation and interaction in Africa. New York, NY, USA: ACM, 2006, pp. 85– 89.

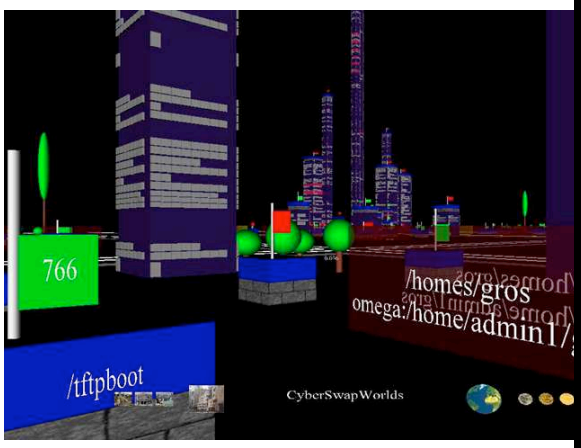
Immersive 3D visualisations

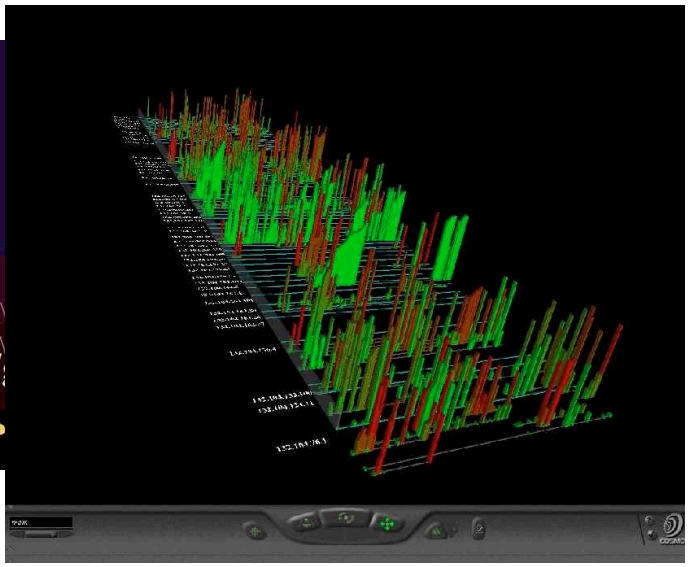
- Untitled – Lazar et al. (1995)
  - Pictures hard to get
- Concept of in-world changes altering the underlying network configuration
  - Context: ATM networks

·L. A. Crutcher, A. A. Lazar, S. K. Feiner, and M. X. Zhou, "Managing networks through a virtual world," IEEE Parallel Distrib. Technol., vol. 3, no. 2, pp. 4–13, 1995.

Immersive 3D visualisations

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





·C. R. D. Santos, P. Gros, P. Abel, D. Loisel, and J.-P. Paris, "Using virtual reality for network management: automated construction of dynamic 3d metaphoric worlds," in VRST '99: Proceedings of the ACM symposium on Virtual reality software and technology. New York, NY, USA: ACM, 1999, pp. 184–185.

Immersive 3D visualisations

- psDoom

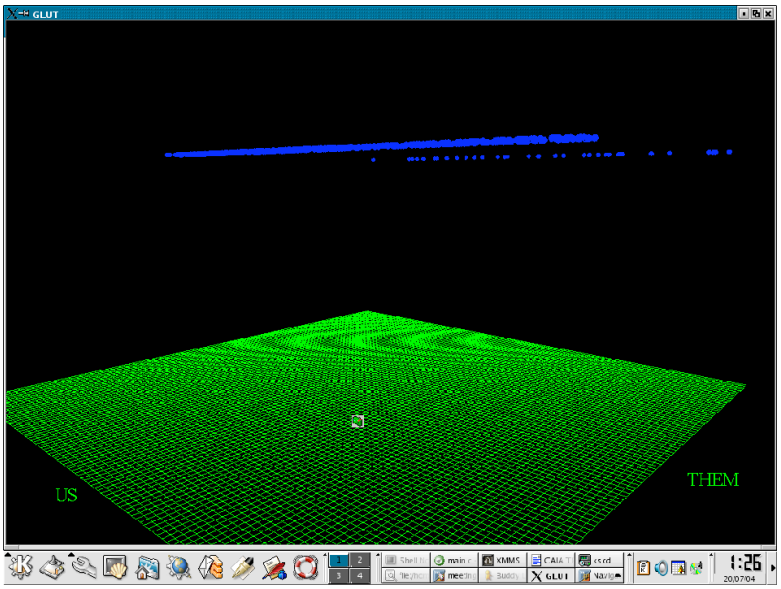
http://psdoom.sourceforge.net/

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”



W. Harrop and G. Armitage, “Intuitive real-time network monitoring using visually orthogonal 3d metaphors,” in *Australian Telecommunications Networks & Applications Conference 2004 (ATNAC2004)*, December 2004.

SWINBURNE UNIVERSITY OF TECHNOLOGY

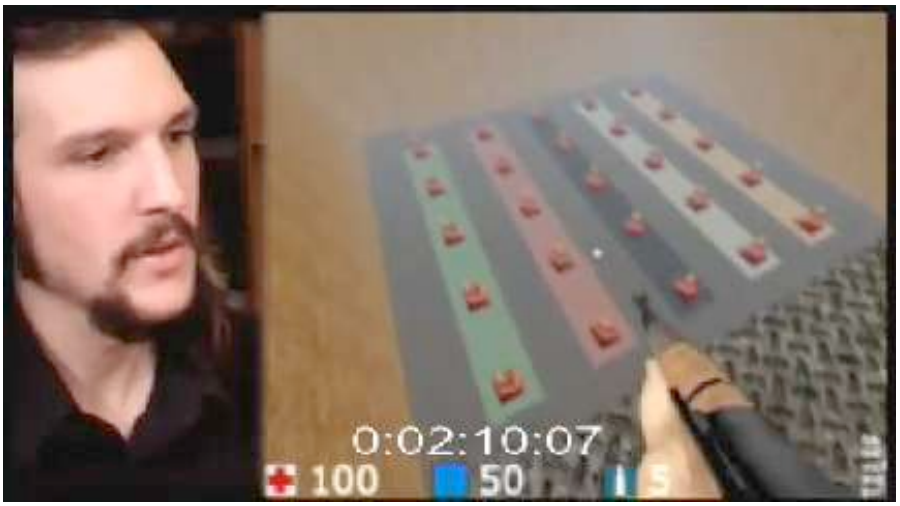
Early work

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

SWINBURNE UNIVERSITY OF TECHNOLOGY

Early work

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



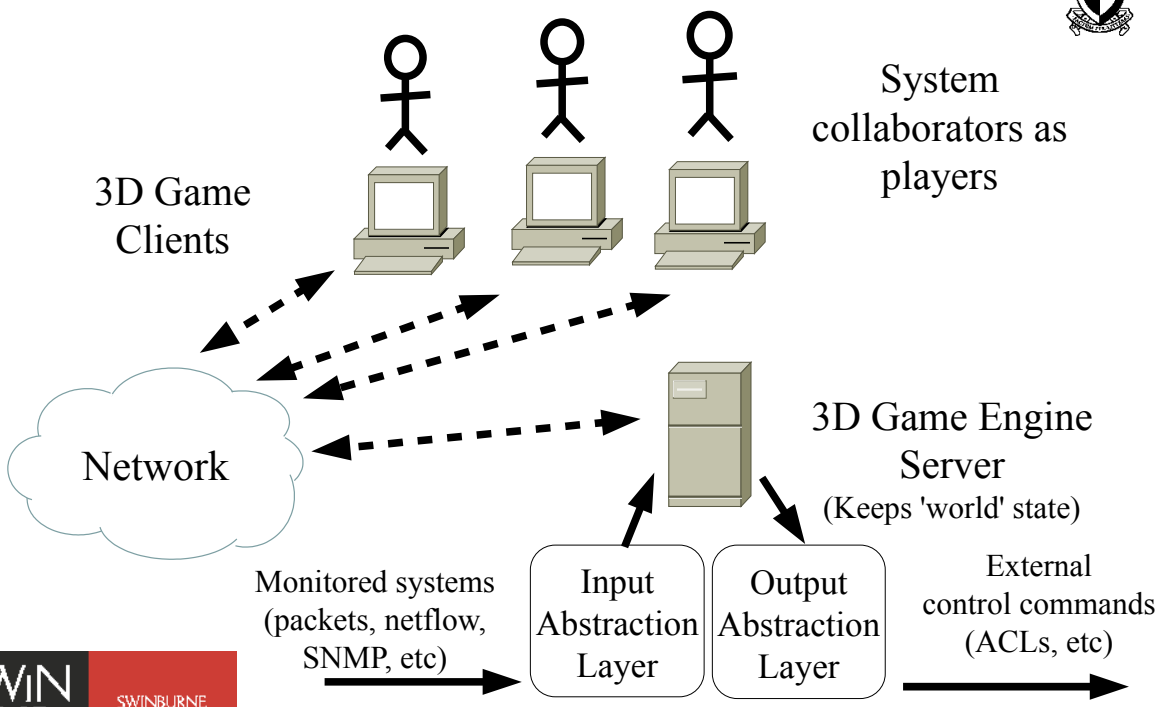
Early work

- "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)

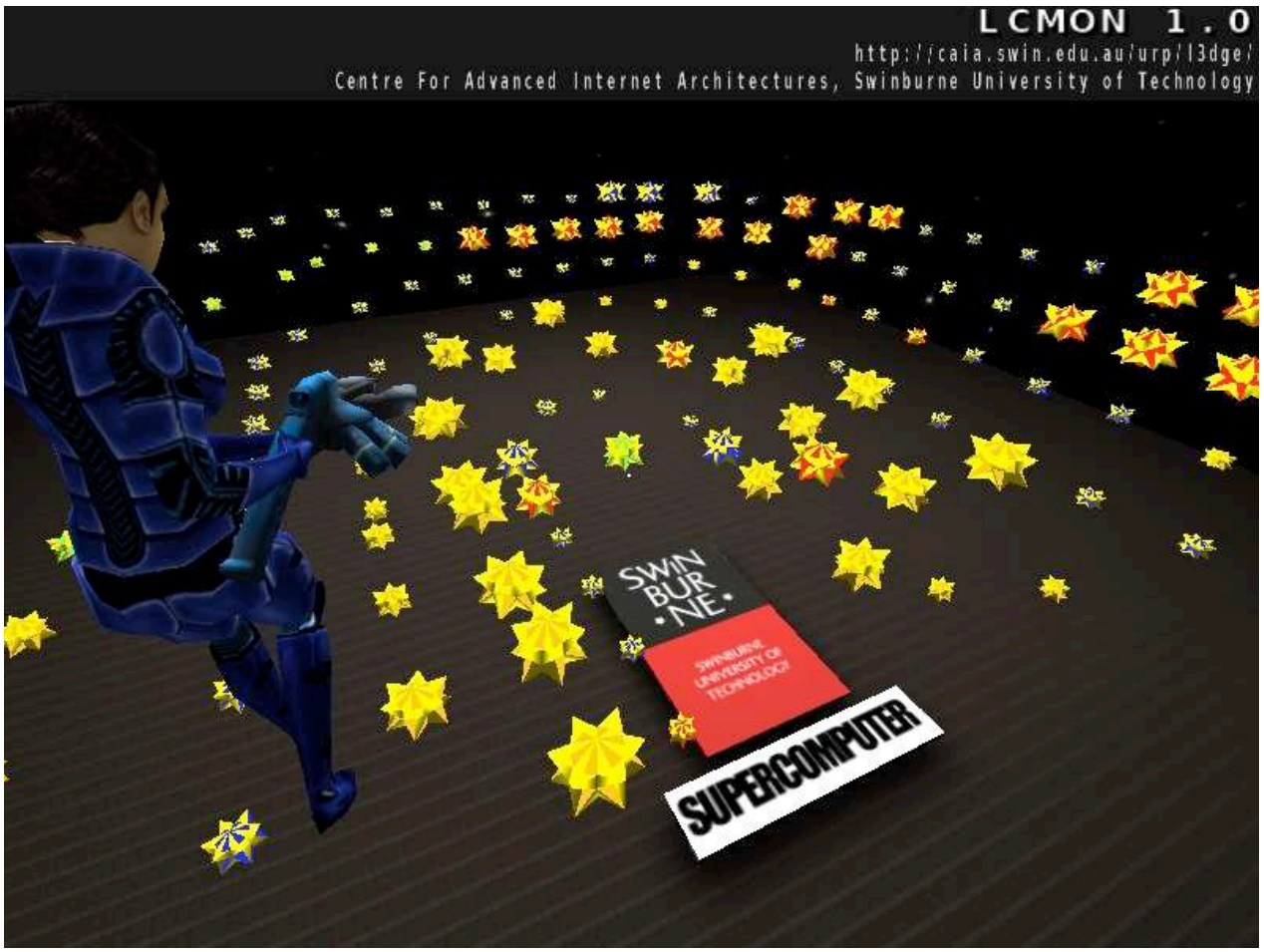
How does it work?

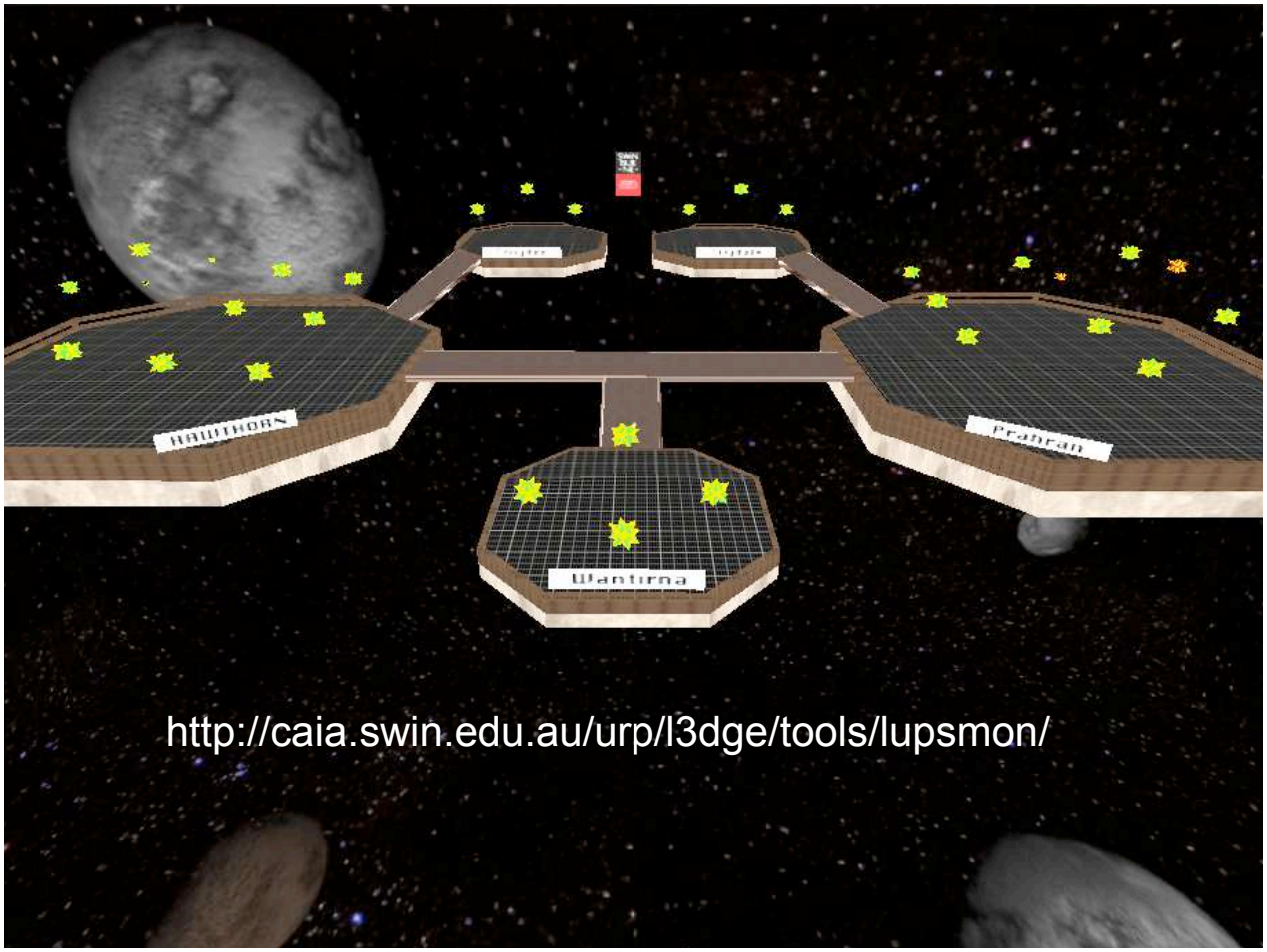


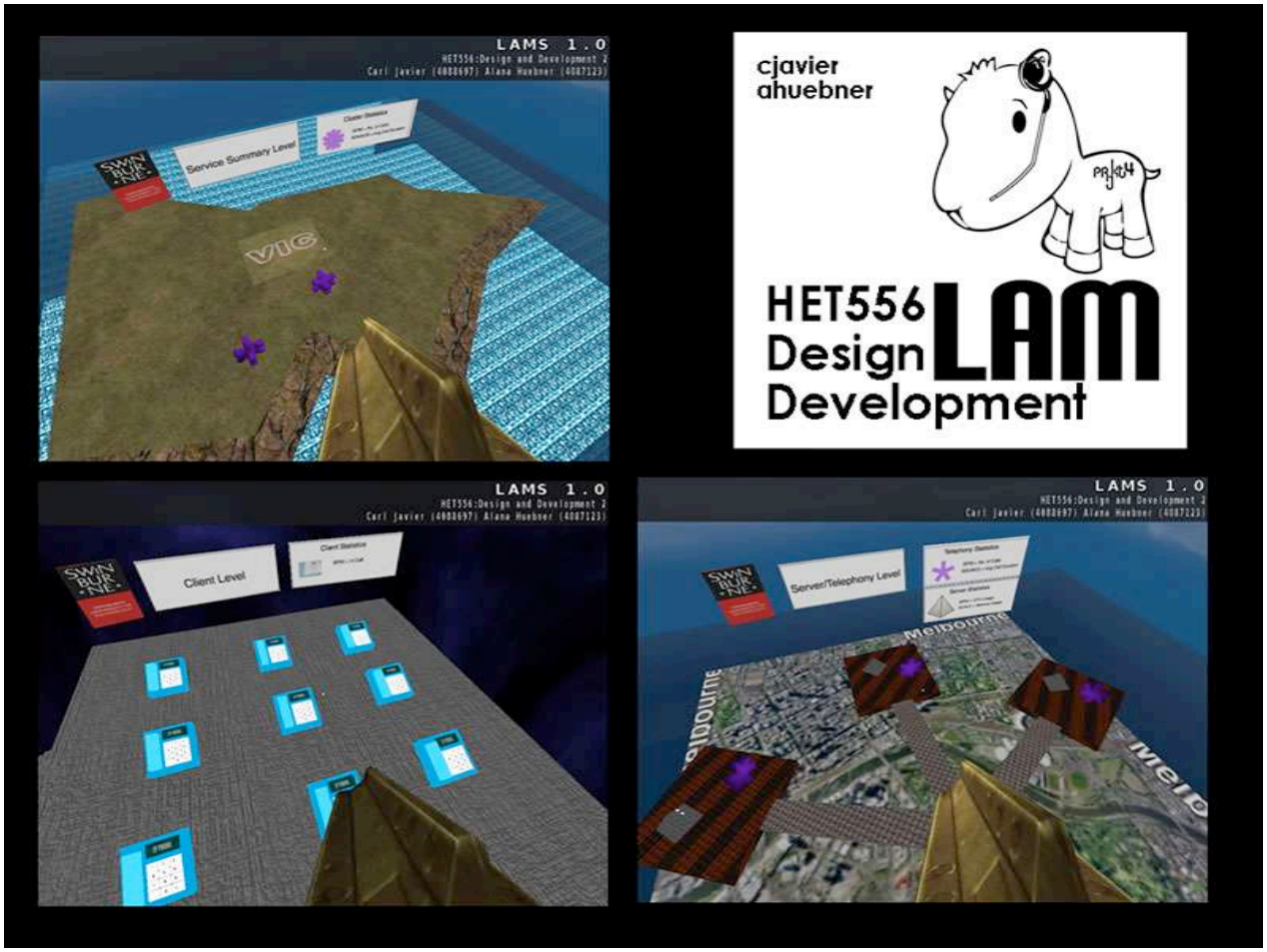
A quick word on "Greynets"

- 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

•F. Baker, W. Harrop, G. Armitage, "IPv4 and IPv6 Greynets," Informational Status Internet-Draft, July 2009 (Expires: January 26, 2010).
•W.Harrop, G.Armitage "Defining and Evaluating Greynets (Sparse Darknets)," IEEE 30th Conference on Local Computer Networks (LCN 2005) Sydney, Australia, 15-17 November, 2005.
•W. Harrop, G. Armitage, "Greynets: A Definition and Evaluation of Sparsely Populated Darknets," (short paper) SIGCOMM 2005 - Workshop on Mining network data (MineNet-05), Philadelphia, Pennsylvania, USA. August, 2005.


LCMON 1.0
http://caia.swin.edu.au/urp/l3dge/
Centre For Advanced Internet Architectures, Swinburne University of Technology
SWIN BUR NE
SUPERCOMPUTER


HAWTHORN
Prahran
Wantirna
http://caia.swin.edu.au/urp/l3dge/tools/lupsmon/



Home networking

- Presented previously...

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?