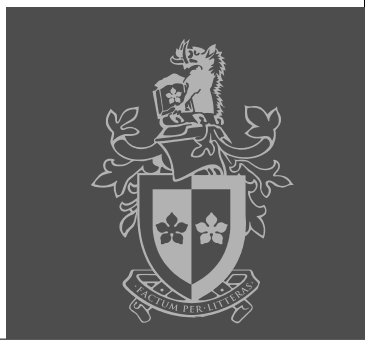
SWINBURNE

CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Visualisation of Darknet Data

Warren Harrop

wazz@swin.edu.au



Outline

- CAIA Darknet
  - What? Why? How?
- Visualisation
  - What? Why? How?
- Future work

CAIA Darknet

- What?
- Subset of IDS (Intrusion detection system(s))
  - "Darknet" has two meanings
    - Ours is Dark == (Dark matter || Black hole)
    - !(Dark == Naughty)
  - Essentially a continuous (but sometimes not) chunk of unused IP address space that we monitor

CAIA Darknet

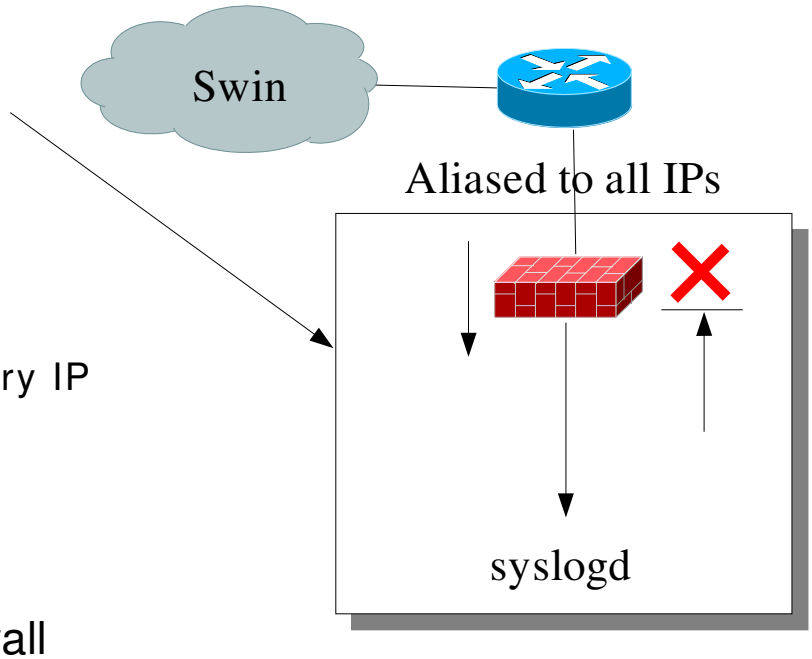
- Why?
  - Packets will still arrive at the Darknet IP range
  - Duh?
    - Packets of 'Dubious' intent
      - Scans
    - Backscatter
      - Results of DOS attacks
  - We can make inferences about what is happening on our network (and other networks) from this info

CAIA Darknet - Example

Aug 25 10:18:41 net /kernel: Connection attempt to TCP xxx.xxx.xxx.73:445 from xxx.xxx.xxx.xxx:3641 flags:0x02
Aug 25 10:18:41 net /kernel: Connection attempt to TCP xxx.xxx.xxx.58:445 from xxx.xxx.xxx.xxx:1128 flags:0x02
Aug 25 10:18:42 net /kernel: Connection attempt to TCP xxx.xxx.xxx.144:445 from xxx.xxx.xxx.xxx:1251 flags:0x02
Aug 25 10:18:45 net /kernel: Connection attempt to TCP xxx.xxx.xxx.144:445 from xxx.xxx.xxx.xxx:1251 flags:0x02
Aug 25 10:18:47 net /kernel: Connection attempt to TCP xxx.xxx.xxx.73:445 from xxx.xxx.xxx.xxx:3641 flags:0x02
Aug 25 10:18:47 net /kernel: Connection attempt to TCP xxx.xxx.xxx.58:445 from xxx.xxx.xxx.xxx:1128 flags:0x02
Aug 25 10:18:51 net /kernel: Connection attempt to TCP xxx.xxx.xxx.144:445 from xxx.xxx.xxx.xxx:1251 flags:0x02
Aug 25 10:19:20 net /kernel: Connection attempt to TCP xxx.xxx.xxx.116:445 from xxx.xxx.xxx.xxx:3358 flags:0x02
Aug 25 10:19:21 net /kernel: Connection attempt to TCP xxx.xxx.xxx.42:445 from xxx.xxx.xxx.xxx:4741 flags:0x02
Aug 25 10:19:23 net /kernel: Connection attempt to TCP xxx.xxx.xxx.116:445 from xxx.xxx.xxx.xxx:3358 flags:0x02
Aug 25 10:19:24 net /kernel: Connection attempt to TCP xxx.xxx.xxx.42:445 from xxx.xxx.xxx.xxx:4741 flags:0x02
Aug 25 10:19:29 net /kernel: Connection attempt to TCP xxx.xxx.xxx.116:445 from xxx.xxx.xxx.xxx:3358 flags:0x02
Aug 25 10:19:30 net /kernel: Connection attempt to TCP xxx.xxx.xxx.42:445 from xxx.xxx.xxx.xxx:4741 flags:0x02
Aug 25 10:19:34 net /kernel: Connection attempt to TCP xxx.xxx.xxx.29:445 from xxx.xxx.xxx.xxx:3627 flags:0x02
Aug 25 10:19:36 net /kernel: Connection attempt to TCP xxx.xxx.xxx.168:445 from xxx.xxx.xxx.xxx:3655 flags:0x02
Aug 25 10:19:37 net /kernel: Connection attempt to TCP xxx.xxx.xxx.29:445 from xxx.xxx.xxx.xxx:3627 flags:0x02
Aug 25 10:19:38 net /kernel: Connection attempt to TCP xxx.xxx.xxx.168:445 from xxx.xxx.xxx.xxx:3655 flags:0x02

CAIA Darknet

- How?
  - VIA motherboard
  - VLAN
  - FreeBSD
    - Aliased to every IP
    - IPFW
    - Syslogd
  - Hole in Swin firewall



Network Visualisation

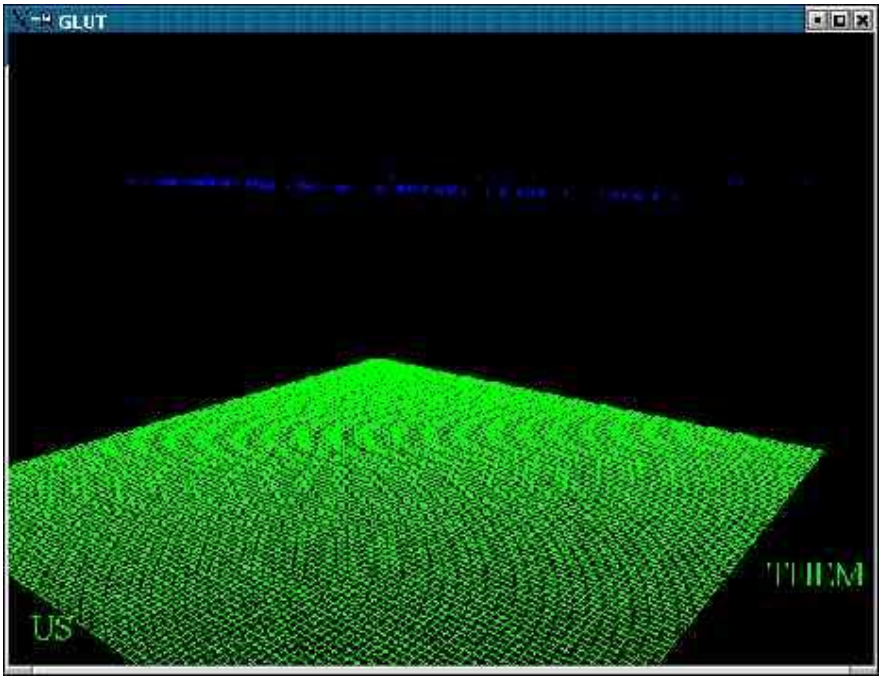
- What?
- Using current tech
  - Hardware 3D acceleration
- Displaying network metrics in an easy to comprehend form

Network Visualization

- Why?
- Long winded anecdote

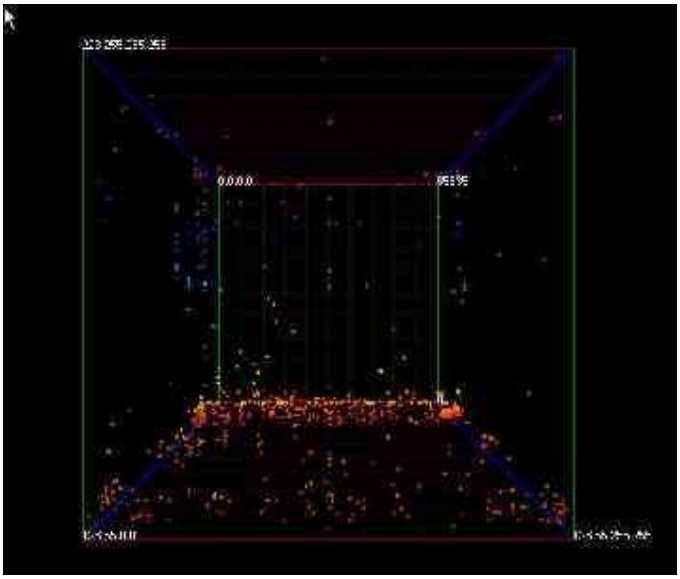
Network Visualisation

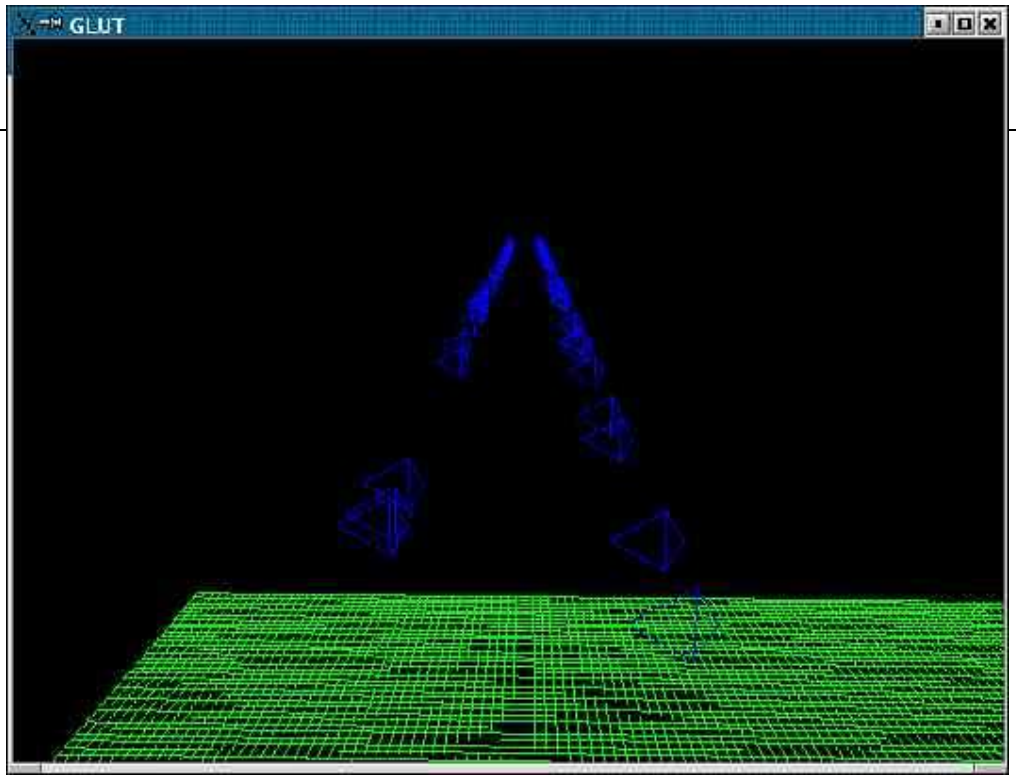
- How?
- OpenGL (GLUT)

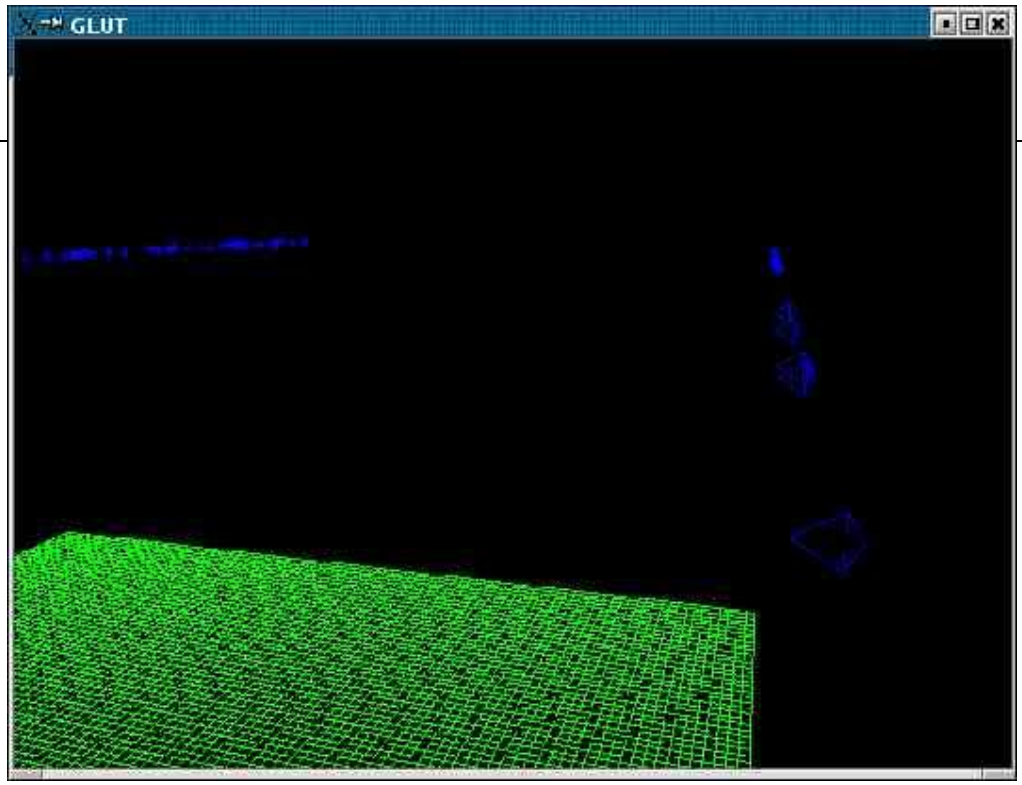


Network Visualisation

- How?
- Close prior work is “Spinning cube of potential doom”




GLUT


GLUT

ATNAC paper

- Current results
- Our views on how things could be done
- Flag in the ground

Future work

- Paper on distributed Darknets
- Finish GLUT version
- Better engine than raw openGL
  - Quake?
  - HL2?
- .....!