SWINBURNE

CENTRE FOR ADVANCED INTERNET ARCHITECTURES

Real-Time Collaborative Network Monitoring and Control Using the Open Source “L3DGE” system

Warren Harrop

wazz@swin.edu.au

CISCO

.auDA FOUNDATION

FACTUM PER LITTERAS

FAQ :

- Who are you?
  - How did you get into my house?
- PhD candidate at the Centre for Advanced Internet Architectures, Swinburne University
- Completed an internship with Cisco in 2007
  - Some financial assistance for this research from Cisco

Outline

- Network monitoring
- (Re)Introduce a “greynet”
  - What does it do? How can it help?
  - Introducing “greynetd”
- Network visualisation and control
  - “L3DGE” project
- Quick demos
- Future work

Greynet

- Greynet – term coined in [1]
- Part of an IDS (Intrusion Detection System)
    - **Not** a user installed, unauthorised application on a network host
- We mean “Distributed edge network darknet”
- Ok...
    - What's a darknet?

[1] 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.

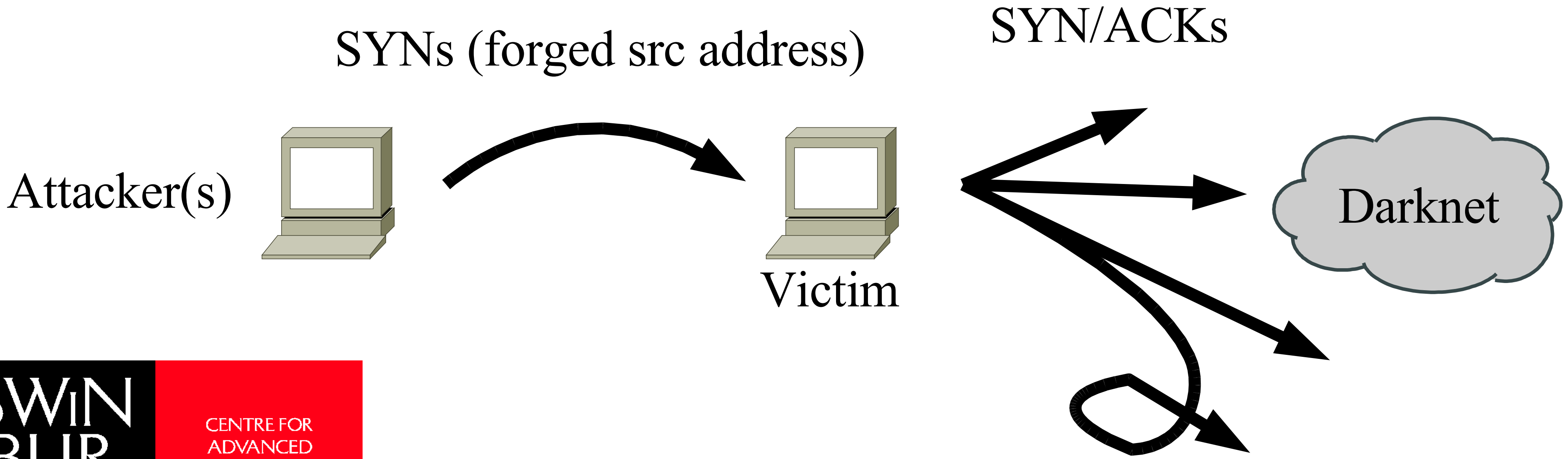
Darknet (Network Telescope or Internet Motion Sensor)

- **Not** a private clandestine content distribution network

- Large contiguous chunk of (spare) IP address space
  - At least a /24 ... but a /8 is better ...
  - Routed but otherwise unused - “Dark”
- No *legitimate* packets should be seen
  - Automated malware (and the people who act like malware) will still send packets into this space in the search for hosts to defile

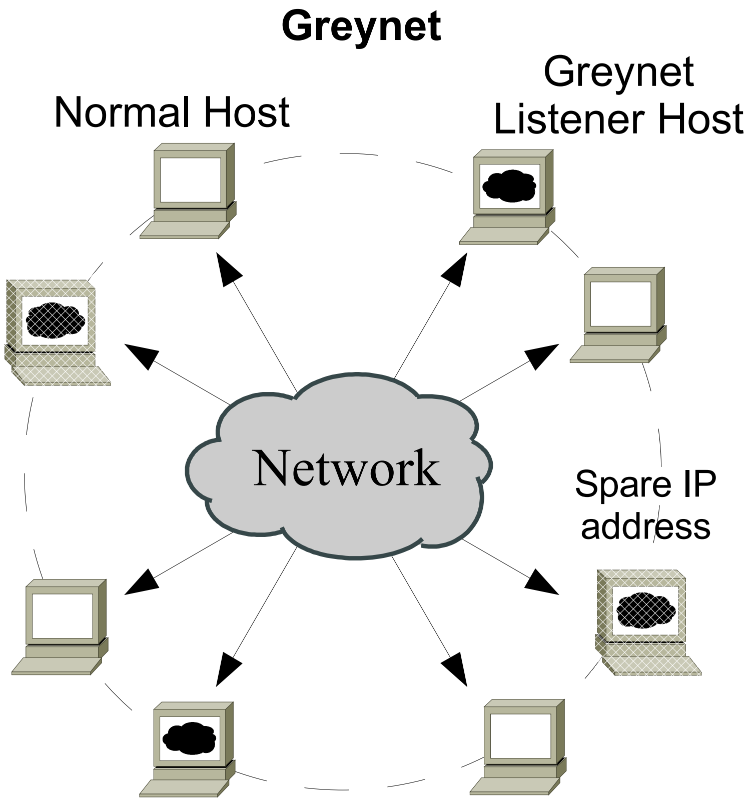
Darknet (2)

- Passively watch for these incoming packets
- Monitor the wider Internet for -
  - Network scans (Malware activity)
  - Internet backscatter (who's being DoSed?)



Greynet

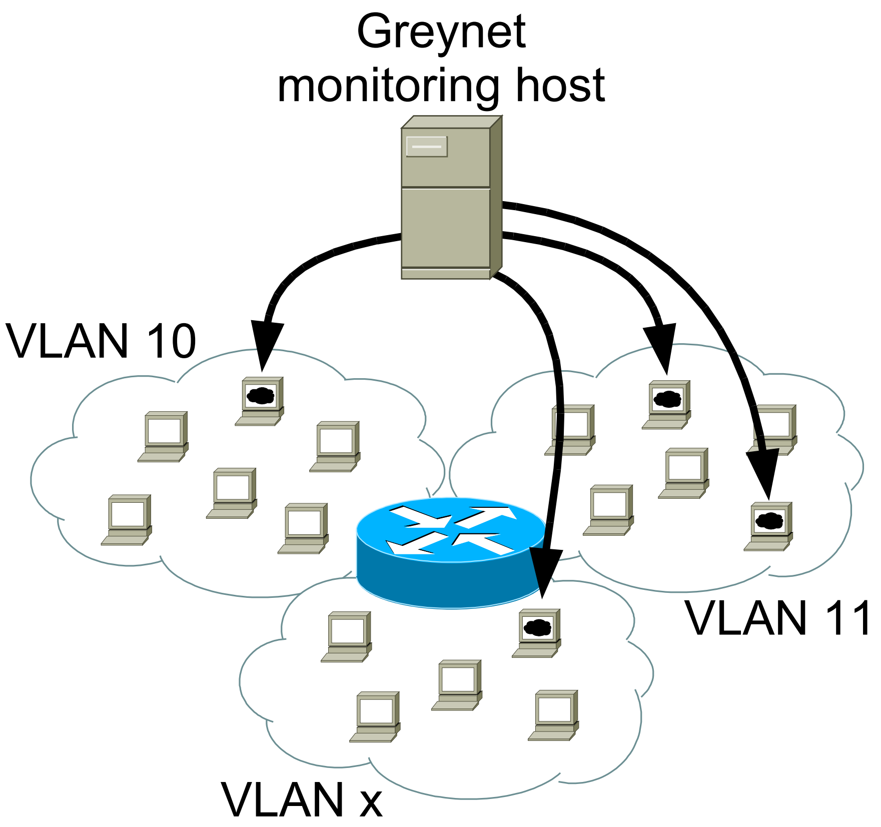
- “Distributed edge network darknet”
- Make the darknet look 'inwards'
  - Place the darknet inside your network
- Not many can afford an entire /24 for a darknet so ...
  - Put darknet hosts among 'regular' 'lit' network hosts
- Network scans find a greynet hard to avoid



Greynet (2)

- From the packets that come to the greynet you now know:
- Who's doing scanning inside my network?
  - Who's infected with malware?
    - What type of malware might be inferred from ports used and the scanning pattern

Implementation



Logical network layer view

Implementation

- For the service provider :
- Make the greynet hosts only sensitive to locally sourced traffic
  - Track break-in attempts by customers
  - Inform users of their infections
- Use on your own enterprise network
- Automatically send alerts
  - Or you could visualise the data coming out ... hmmm ...

“greynetd”

- Coming soon...
- FreeBSD package
- Ease greynet implementation & deployment
- Stir together a FreeBSD machine & VLAN trunk –
  - DHCP integration
  - SNMP monitoring interface
  - Web interface for setup and control
- Demo...

SWINBURNE CENTRE FOR ADVANCED INTERNET ARCHITECTURES

.auDA FOUNDATION

Visualisation and Control

- PhD work
- Made possible in part by a grant from Cisco
  - Cisco University Research Program Fund (URP)

“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 the multiple, 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 admins lend a helping hand
    - Train them quicker
- Help you see the thing you didn't know you didn't know
    - by...
- Creating suitably high-level, interactive and real-time abstractions and visualisations

L3DGE project

- L3DGE
  - “Leveraging 3D Game Engines”
  - http://caia.swin.edu.au/urp/l3dge
- Not a “product” – active research
  - (Not to say we wont take your money)

L3DGE

- 3D world, data visualisation and control tool
- Based on 'OpenArena'
  - Based on Quake III Arena
- Modular design
- Developed to monitor data networks (in real-time)
  - But not limited to this
- Lucas Parry
  - 12 months of development

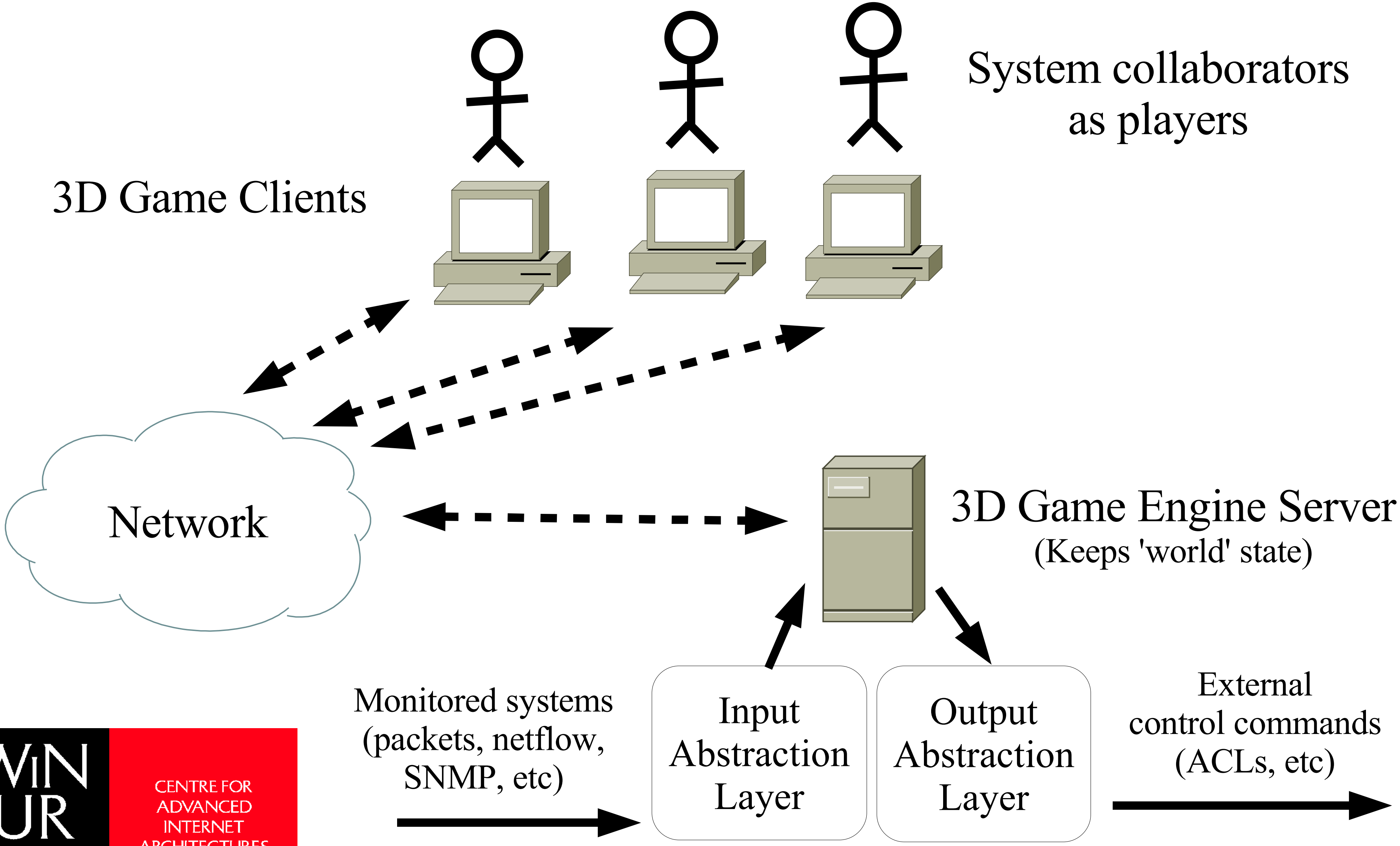
L3DGE

- Monitored systems are represented by in-world entities
- Entity attributes (spin rate, colour... etc.) are tied to monitored real-world metrics
- Viewer sees multiple metrics concurrently
  - Multiple viewers in-world
- In-world interactions translated into external actions
  - Basic permissions system implemented

L3DGE

- Released - GPL
  - Input, output abstractions layers
  - Binary versions for Windows, FreeBSD, Linux and Mac OS X
- http://caia.swin.edu.au/urp/l3dge/

How does it work?


System collaborators as players

3D Game Clients

Network

3D Game Engine Server
(Keeps 'world' state)

Monitored systems (packets, netflow, SNMP, etc)

Input Abstraction Layer

Output Abstraction Layer

External control commands (ACLs, etc)

SWINBURNE CENTRE FOR ADVANCED INTERNET ARCHITECTURES

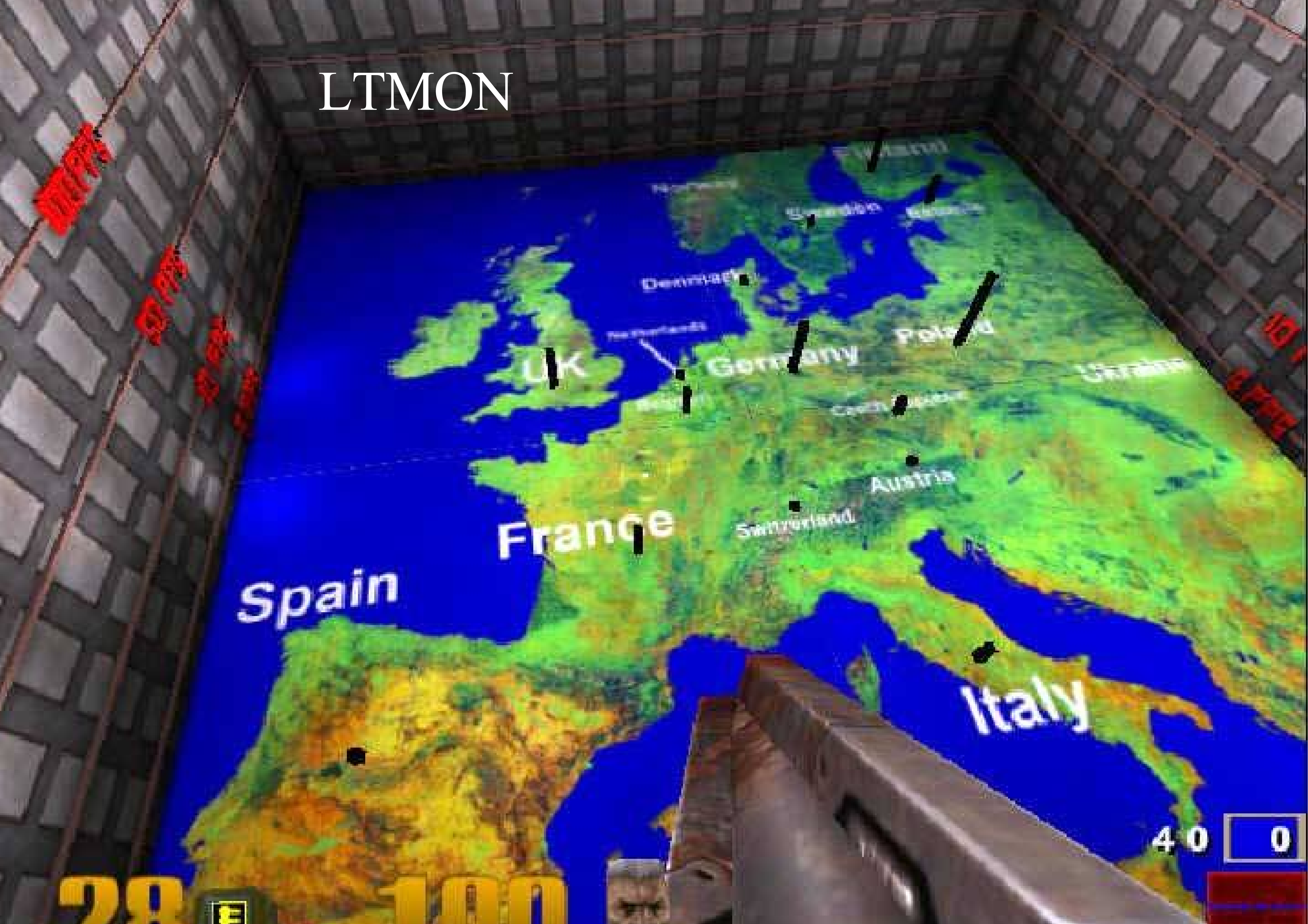
Why use a game engine?

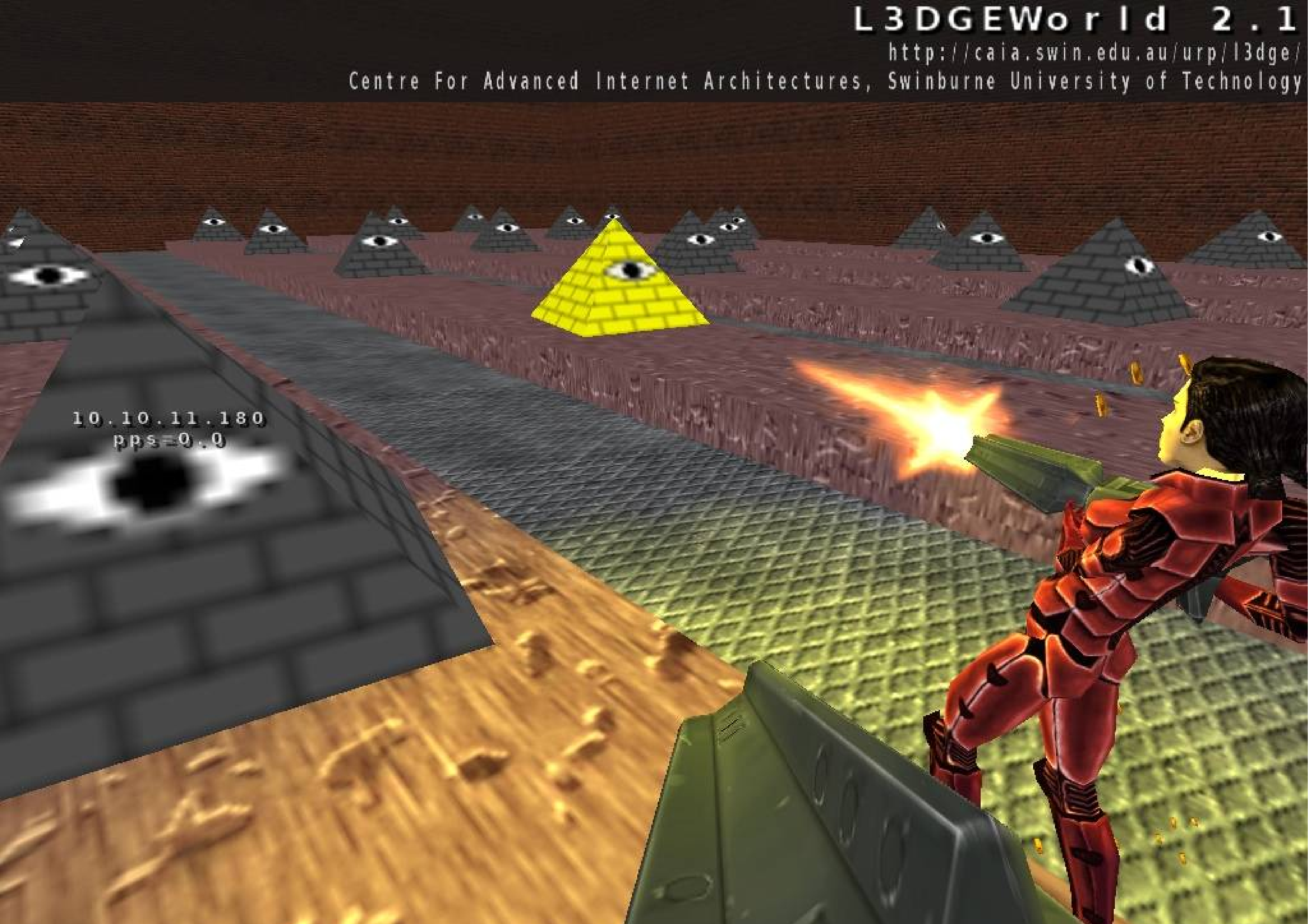
- Advanced graphics ability and 3D rendering
- Collaboration
- Interaction
- Real-time optimised code
- Proven (defacto) world navigation system
- Human spatial senses leveraged
  - Detection of anomalies with human pattern recognition
- Allowing for simplified presentation of complicated (“non-physical”) systems

L3DGE software

- Precursor
  - LTMON L3DGE Traffic Monitor by Alex Shoolman (Released January 2007)
- L3DGEWorld 2.3 by Lucas Parry (Released December 2007)
  - Using the L3DGE engine:
    - LupsMON 0.2 by Michael Allen (Released May 2008)
      - (L3DGEWorld Uninterruptible Power Supply Monitoring)
    - LCMON 1.1 by Carl Javier and Adam Black (Released December 2007)
      - (L3DGEWorld Cluster-node Monitoring)

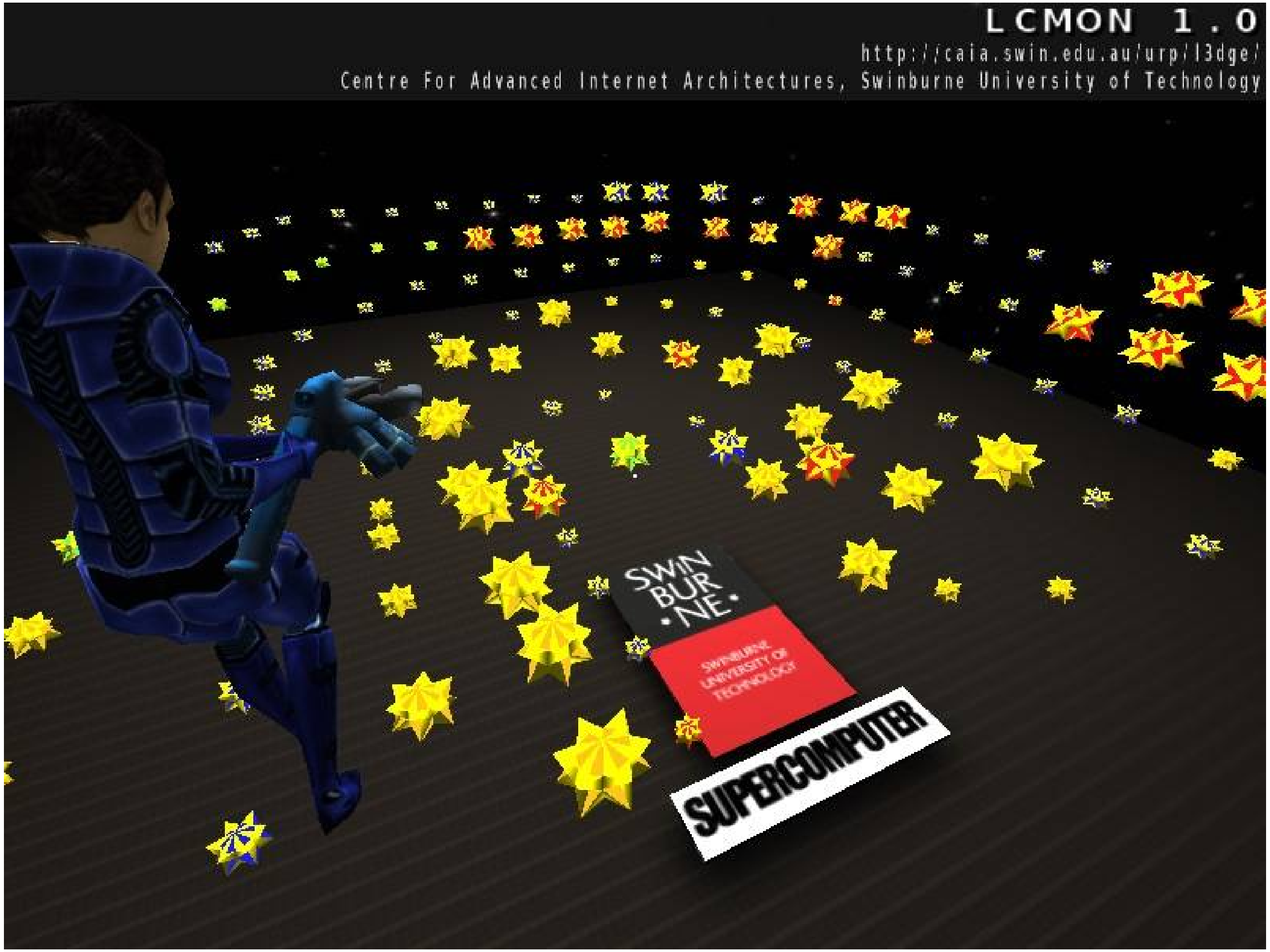
LTMON


Finland
Norway
Sweden
Estonia
Denmark
Netherlands
UK
Germany
Poland
Ukraine
Belgium
Czech Republic
Austria
France
Switzerland
Spain
Italy
40
0
28
100


L3DGEWorld 2.1
http://caia.swin.edu.au/urp/l3dge/
Centre For Advanced Internet Architectures, Swinburne University of Technology
10.10.11.180
pps=0.0

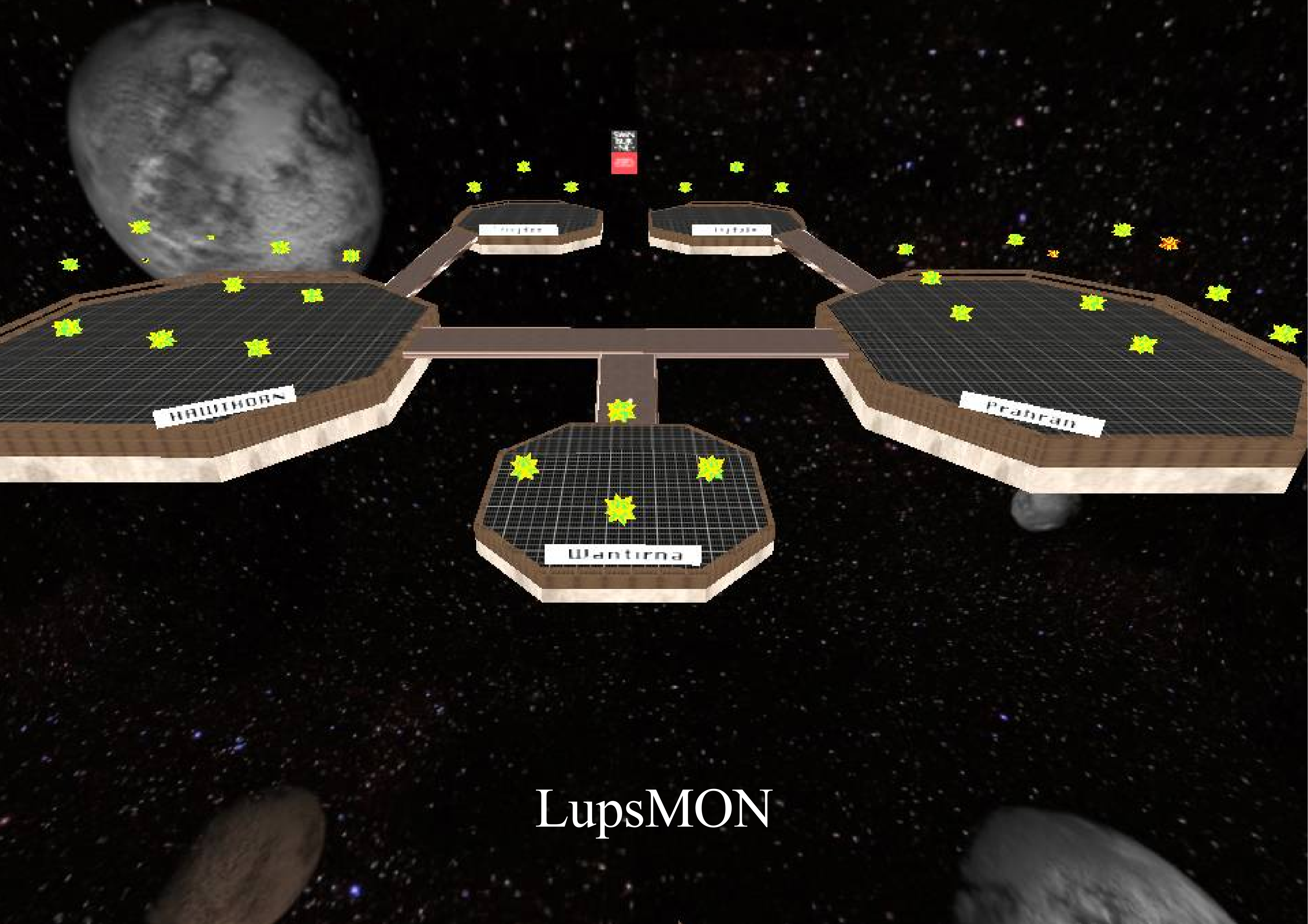
LCMON

- Demo


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

SWIN BUR NE

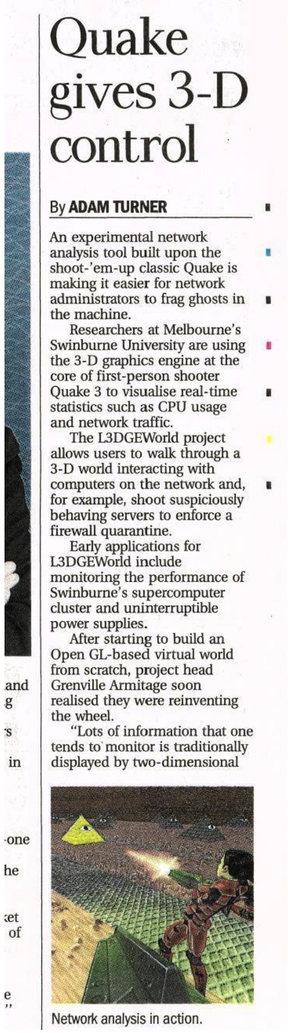
CENTRE FOR ADVANCED INTERNET ARCHITECTURES

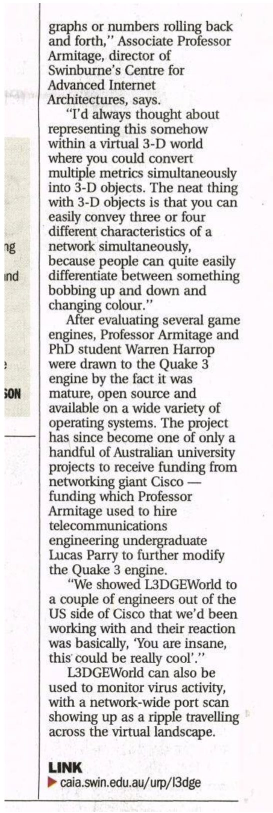


LupsMON

L3DGE in the 'media'

- http://caia.swin.edu.au/urp/l3dge/media.html
- The Age
  - Physical
  - Online





Quake gives 3-D control

By **ADAM TURNER**

An experimental network analysis tool built upon the shoot-'em-up classic Quake is making it easier for network administrators to frag ghosts in the machine.

Researchers at Melbourne's Swinburne University are using the 3-D graphics engine at the core of first-person shooter Quake 3 to visualise real-time statistics such as CPU usage and network traffic.

The L3DGEWorld project allows users to walk through a 3-D world interacting with computers on the network and, for example, shoot suspiciously behaving servers to enforce a firewall quarantine.

Early applications for L3DGEWorld include monitoring the performance of Swinburne's supercomputer cluster and uninterruptible power supplies.

After starting to build an Open GL-based virtual world from scratch, project head Grenville Armitage soon realised they were reinventing the wheel.

"Lots of information that one tends to monitor is traditionally displayed by two-dimensional graphs or numbers rolling back and forth," Associate Professor Armitage, director of Swinburne's Centre for Advanced Internet Architectures, says.

"I'd always thought about representing this somehow within a virtual 3-D world where you could convert multiple metrics simultaneously into 3-D objects. The neat thing with 3-D objects is that you can easily convey three or four different characteristics of a network simultaneously, because people can quite easily differentiate between something bobbing up and down and changing colour."

After evaluating several game engines, Professor Armitage and PhD student Warren Harrop were drawn to the Quake 3 engine by the fact it was mature, open source and available on a wide variety of operating systems. The project has since become one of only a handful of Australian university projects to receive funding from networking giant Cisco — funding which Professor Armitage used to hire telecommunications engineering undergraduate Lucas Parry to further modify the Quake 3 engine.

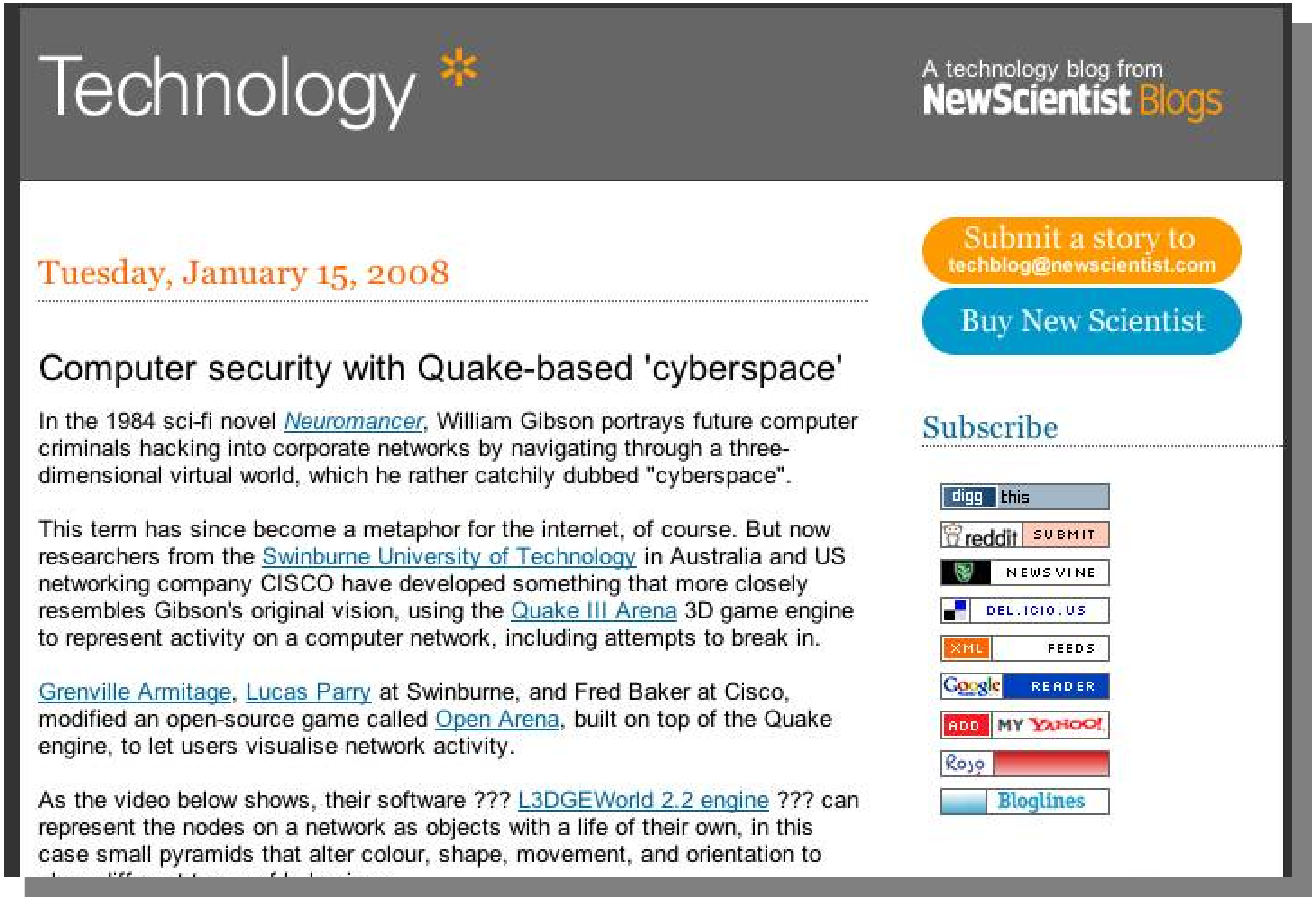
"We showed L3DGEWorld to a couple of engineers out of the US side of Cisco that we'd been working with and their reaction was basically, 'You are insane, this could be really cool'."

L3DGEWorld can also be used to monitor virus activity, with a network-wide port scan showing up as a ripple travelling across the virtual landscape.

Network analysis in action.

LINK
▶ caia.swin.edu.au/urp/l3dge

L3DGE in the 'media' (2)



Tuesday, January 15, 2008

Computer security with Quake-based 'cyberspace'

In the 1984 sci-fi novel *Neuromancer*, William Gibson portrays future computer criminals hacking into corporate networks by navigating through a three-dimensional virtual world, which he rather catchily dubbed "cyberspace".

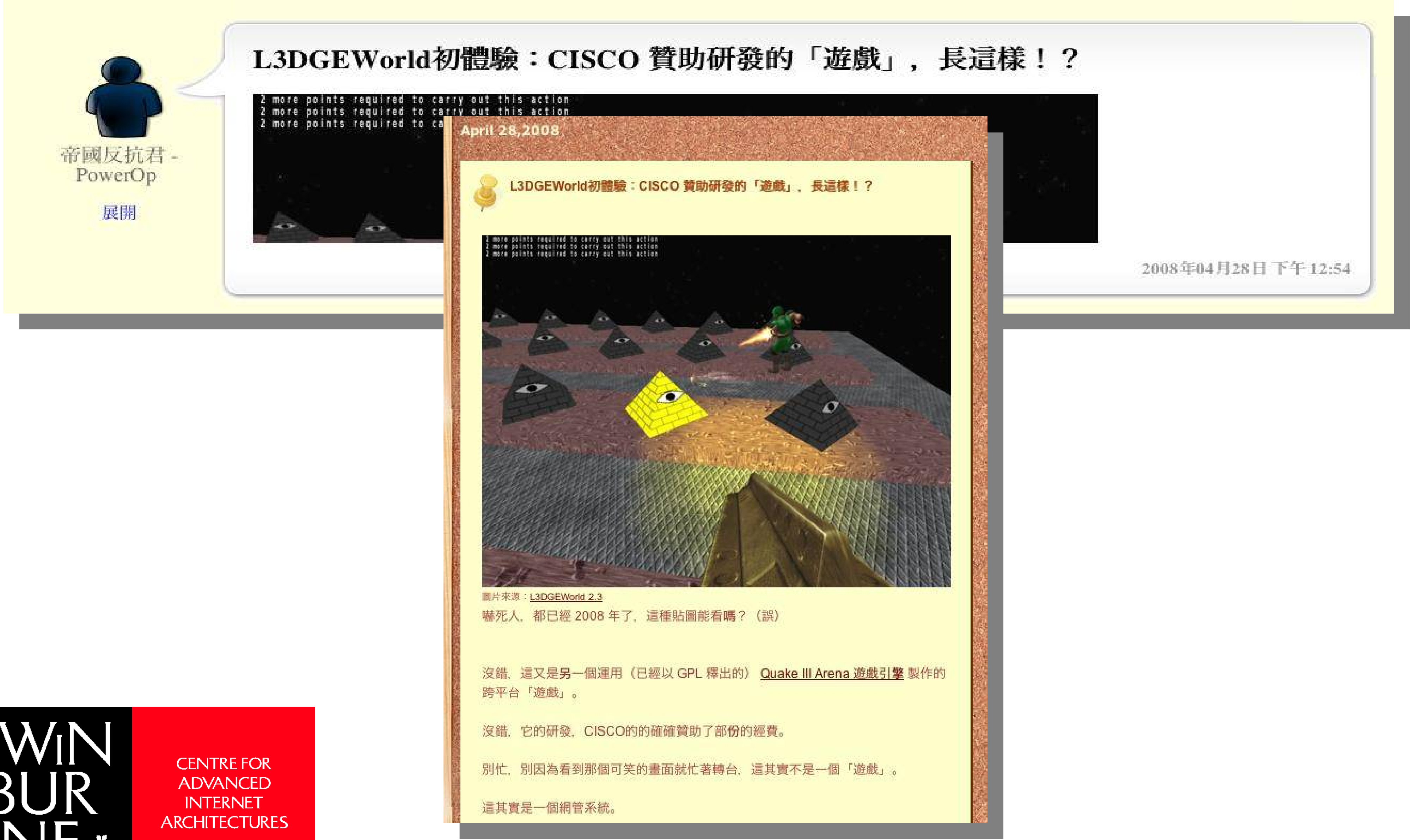
This term has since become a metaphor for the internet, of course. But now researchers from the Swinburne University of Technology in Australia and US networking company CISCO have developed something that more closely resembles Gibson's original vision, using the Quake III Arena 3D game engine to represent activity on a computer network, including attempts to break in.

Grenville Armitage, Lucas Parry at Swinburne, and Fred Baker at Cisco, modified an open-source game called Open Arena, built on top of the Quake engine, to let users visualise network activity.

As the video below shows, their software ??? L3DGEWorld 2.2 engine ??? can represent the nodes on a network as objects with a life of their own, in this case small pyramids that alter colour, shape, movement, and orientation to

http://www.newscientist.com/blog/technology/2008/01/computer-security-with-quake-based.html

L3DGE in the 'media' (3)



帝國反抗君 - PowerOp

展開

L3DGEWorld初體驗：CISCO 贊助研發的「遊戲」，長這樣！？

```
2 more points required to carry out this action
2 more points required to carry out this action
2 more points required to ca
```

2008年04月28日 下午 12:54

April 28,2008

L3DGEWorld初體驗：CISCO 贊助研發的「遊戲」、長這樣！？

```
2 more points required to carry out this action
2 more points required to carry out this action
2 more points required to carry out this action
```

圖片來源：L3DGEWorld 2.3

嚇死人，都已經 2008 年了，這種貼圖能看嗎？（誤）

沒錯，這又是另一個運用（已經以 GPL 釋出的） Quake III Arena 遊戲引擎 製作的跨平台「遊戲」。

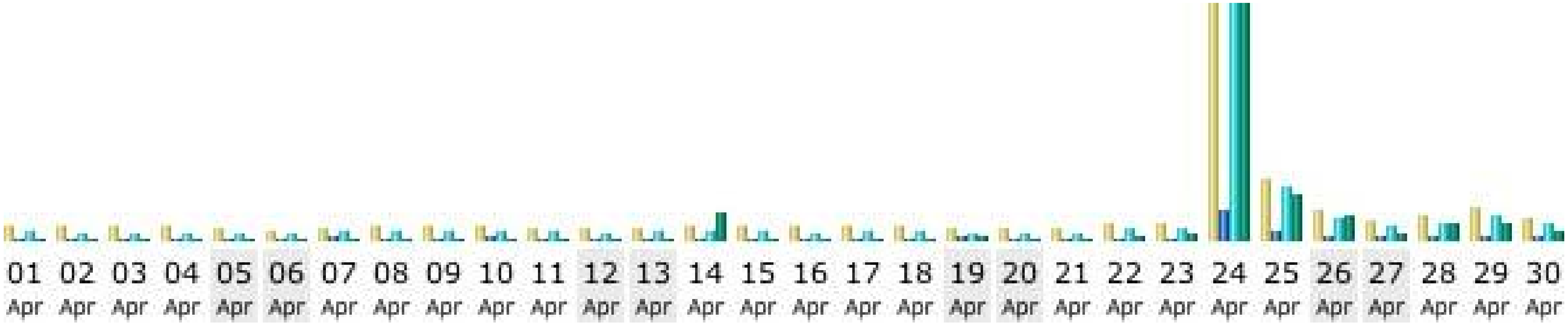
沒錯，它的研發，CISCO的的確確贊助了部份的經費。

別忙，別因為看到那個可笑的畫面就忙著轉台，這其實不是一個「遊戲」。

這其實是一個網管系統。

L3DGE in the 'media' (4)

- and blogging leads to...



Future work

- Speculative research – years of life span
- Community contributions...?
- Long term
  - Change of game engine
  - Some advanced features to negate having to leave the world
    - Eg. ssh in-world
- And...and....and...

Conclusion

- Reintroduced a “greynet”
  - Introduced “greynetd”
- L3DGE – Leveraging 3D Game Engines
  - L3DGEWorld
  - LCMON – Super cluster monitoring
  - LUPSMON – UPS monitoring
- Future work
- Thank you

SWiN BUR NE

CENTRE FOR ADVANCED INTERNET ARCHITECTURES