Modifying first person shooter games to perform real time network monitoring and control tasks

Warren Harrop, Grenville Armitage
{wazz,garmitage}@swin.edu.au

Outline

- The problem
- Previous work
- Metaphors for representation and interaction
- Overall architecture
- Advantages of leveraging 3D game engines
- Prototype
- Future work
- Conclusion
The problem

- Network administration is hard
  - Complicated
    - Compounded by attacks
- Question...
- Could suitably high-level, 3D interactive and real-time abstractions be created to...
  - Lower the skills needed to make a positive contribution to network administration?
  - Allow skilled personnel quicker diagnosis of network issues?

Previous work

Rationale

- Previous work
- 3D cheap and convent to create
  - Convey large amounts of information quickly
- Keeping humans 'in the loop' in complex systems
  - Advantage over automated systems

- So how?
  - Definitions...

Metaphors

<table>
<thead>
<tr>
<th>Visual Metaphor</th>
<th>Network Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location</td>
<td>IP address, port number</td>
</tr>
<tr>
<td>Shape</td>
<td>Representation of object type (subnet, host or connection)</td>
</tr>
<tr>
<td>Size</td>
<td>Time aggregate of unique connections</td>
</tr>
<tr>
<td>Colour/Texture</td>
<td>Content type</td>
</tr>
<tr>
<td>Rotational Velocity</td>
<td>Throughput</td>
</tr>
<tr>
<td>Oscillation about a fixed point</td>
<td>User defined alert</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Interaction Metaphor</th>
<th>Network Administration Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shoot (with gun)</td>
<td>Place firewall rule</td>
</tr>
<tr>
<td>Heal (with syringe)</td>
<td>‘Undo’ (remove changes)</td>
</tr>
<tr>
<td>Fine tune (with pliers)</td>
<td>Bandwidth rate-shape</td>
</tr>
</tbody>
</table>
Architecture

System collaborators as players

3D Game Clients

Network

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

Input Abstraction Layer

Output Abstraction Layer

External metrics

External control commands

Multiple game clients and network administrators

Network link

3D Game Engine Client

Network administrator

Creates 3D Representation

Shoots 3D Representation

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

Upper Abstraction Layer

Lower Abstraction Layer

Greynet data

ACL rules

Architecture (Detail)
Leveraging 3D Game Engines

- Proven Code
  - Distributed
  - Collaboration
  - Real-time (10s of ms)
- Provides advanced 3D capabilities
- High level content creation tools
- Hooks for 3rd party modifications

Collaboration

- Collaborative monitoring of systems
  - Multiple administrators as players in the same world
  - Physically remote of system under control
- Advanced control possibilities
  - Multiple players required to 'shoot' to instantiate changes
  - Different abilities can be set for each 'player'
    - Allowing a permissions system to be developed
Prototyping a System

- Cube
  - Open source 3D game engine
  - Cosmetic changes
    - Avatars
  - Source changes
    - To allow input and output to the system
- Input to the system was a greynet
- Output are Cisco ACLs

System Layout
A day in the life...

Operator shoots a greynet host

Initial state returned
Future Work

- Different engine
  - Quake 3
- More network metrics monitored / controlled
- User trials
  - Technical tests (bugs / scalability...)
  - Usability
- Cisco funding
  - Full time development

Conclusion

- Inspired by previous work
- Defined interaction metaphors
- Created prototype software
- Many plans for the future...
- Thanks:
  - Thanks to Carl Javier for creating the 3D pyramid avatars
  - This work has been made possible in part by a grant from the Cisco University Research Program Fund at Community Foundation Silicon Valley.