L3DGEWorld 1.0 Input/Output Layer Specifications

Warren Harrop, Lucas Parry
Centre for Advanced Internet Architectures. Technical Report 070402A
Swinburne University of Technology
Melbourne, Australia
{wazz,lparry}@swin.edu.au

***Abstract*-This technical report briefly describes 'L3DGEWorld 1.0' a plug-in modification to the Quake III Arena game engine to allow network monitoring and control of a live network to take place 'in-game'. This report then, in detail, outlines the initial interface specifications for conveying network activity from a greynet (or similar network monitoring system) to the 3D game engine for real-time visualisation and representation. It also defines the initial interface specifications for the signaling and control protocol that re-configures a standard Cisco enterprise router's ACLs based on the resulting in-game actions.**

Keywords- L3DGE project, L3DGEWorld 1.0, visualisation, specification

I. Introduction

Network monitoring and control leveraging 3D game engines as a development platform, has previously been described by Harrop and Armitage [1] [2] [3]. In [1] a set of mapping were defined between in-game metaphors and network metrics to allow live network events to be displayed in a 3D world. A major goal of this work was to create mappings that allow in-game events to intuitively represent underlying network anomalies in real-time. [2] first used a 3D game engine to implement the metaphors defined in [1] and detailed technical descriptions of the prototype implementation and 3D game engine modifications appear in [3].

L3DGEWorld 1.0 is a plug-in modification for the Quake III Arena (Q3A) game engine [4]. Although the full Q3A engine was recently released under the open source GPL license, L3DGEWorld version 1.0 only utilises the pre-existing modification hooks. The advantage of this is that modifications can be distributed in the portable and self contained .pk3 file format and run on client and servers regardless of the executing platform. If modification of the core engine is performed, the Q3A client and server will most likely need to be recompiled on (or for) each destination platform. With the current version of L3DGEWorld, this has been avoided.

The input to L3DGEWorld 1.0 is a 'greynet' [5] (or in other terms a 'distributed sparse enterprise based darknet'). A greynet is a set of 'dark' passive listener hosts dispersed amongst 'lit' (normal) network hosts on an enterprise network. When malware scans across the network attempting to detect vulnerable hosts, it not only scans real network hosts, but also alerts network administrators to its presence as the greynet hosts report their incoming packets.

In our design of the L3DGEWorld 1.0 software, we have opted to develop a set of abstractions between the 3D game engine server and the underlying network devices. Doing so allows us to develop the software in a modular fashion enabling the ability to write new input/output modules without additional modification the 3D game server.

In this document we will describe the interface for communication between the upper abstraction layer and the lower abstraction layer as previously defined in [3] and seen in Figure 1 below.

For our initial version of L3DGEWorld, we propose the use of a flat file-system for communicating

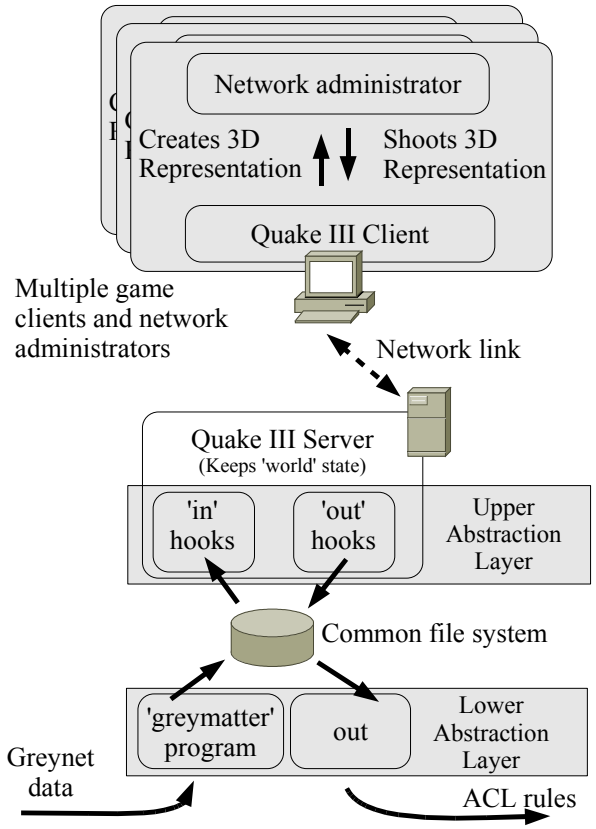

Figure 1 L3DGEWorld abstraction layers to allow external input to influence world state and world actions to influence outside systems

information and actions between the 3D game world and the monitoring and controlling processes.

II. L3DGEWorld 1.0

L3DGEWorld 1.0 comprises of an input daemon (the greynet listener program 'greymatter'), a Q3A client & server running the L3DGEWorld modification, and an output daemon. The greymatter daemon generates statistics about traffic entering greynet hosts and writes them to relevant files on the file system. The modified Q3A server periodically reads and interprets this information and updates the 3D world. This world state is then automatically transferred (through core Q3A server/client functionality) from server to all connected clients. Conversely, actions by clients are transferred to the server and as appropriate, network configuration commands are output to the file system. The output daemon monitors for these files, and performs the commands within on the router defined in the configuration file.

L3DGEWorld 1.0 has been designed to be modular, so that new input and output daemons can easily be written in order to interface with other hardware and software.

Users in the L3DGEWorld 3D world see pyramids representing the hosts of the associated greynet under scrutiny as in Figure 2 below. This is an improved version of an earlier prototype based on the 'Cube' game engine [3].

Figure 2 L3DGEWorld: An overview of greynet activity

In [3] an object's spin rate was boolean, there was no indication of magnitude. In L3DGEWorld the host's spin is based on the packets per second that are destined for the IP they represent.

L3DGEWorld 1.0 has the beginnings of the multiple administrator permissions system described in [3]. In version 1.0 the default setting requires two administrators to agree that traffic is anomalous and "shoot" the same host within a configurable period of time, for an action to be turned into a 'live' ACL on a router. If required, a single-user mode can be enabled allowing only one user to configure an ACL. (In version 1.0 the "shoot" operation is achieved with the 'machine gun'.)

Users are able to pick up and move host avatars (using the 'rail gun' to pick, and pressing 'enter' to drop), in order to arrange the representation of their network in a manner that is intuitive to them. These changes are persistent in the 3D world, meaning that the Q3A server may be shutdown or restarted and the objects will retain their positions.

Users are also provided with more detailed data as they require it. When a user comes within an arbitrary range of hosts, additional information is shown in textual from overlaid above the host. This is currently used to show the attacking hosts IP or host-name and the numerical packets per second into a greynet host, but could be used to represent any relevant information.

Figure 3 Moving closer to a greynet avatar reveals additional information in the form of a textual overlay

III. Testbed Configuration

The L3DGEWorld testbed is shown in Figure 4 and consists of a Cisco 7140 router (running IOS 12.3) and 3 standard PCs. One interface on the router has two sub-interfaces created in VLANs 10 and 11. The PC representing the attacker is placed on VLAN 10, the

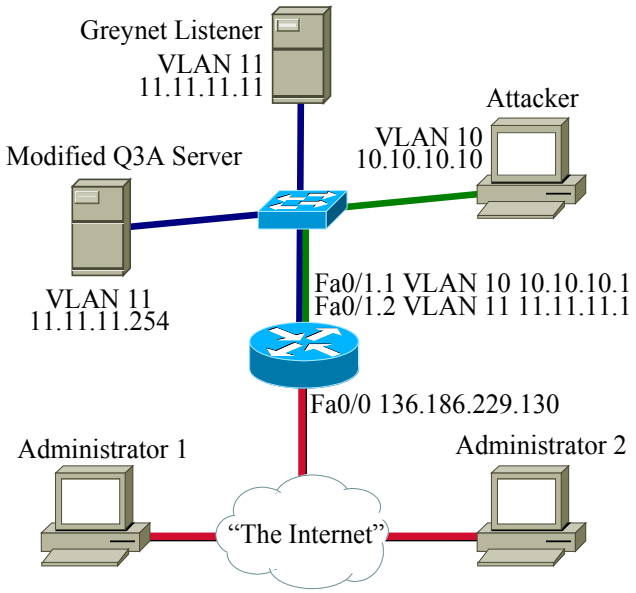

Figure 4 Testbed configuration

other two PCs, representing the Greynet listener and the Q3A server are placed on VLAN 11.

The second interface on the 7140 is placed on Swinburne's 136.186.229.0/24 network, representing the Internet. PCs on the "Internet" running the modified Q3A client (and with appropriate routes in their table) are able to connect to the server and monitor and control traffic routed between the two VLANs.

IV. Directory Structure

All files related to configuration, conveying statistics to the game world, and conveying commands to external networking equipment are stored within a directory named "hosts" within the Q3A modification directory. This simplifies access to these files from within the game engine.

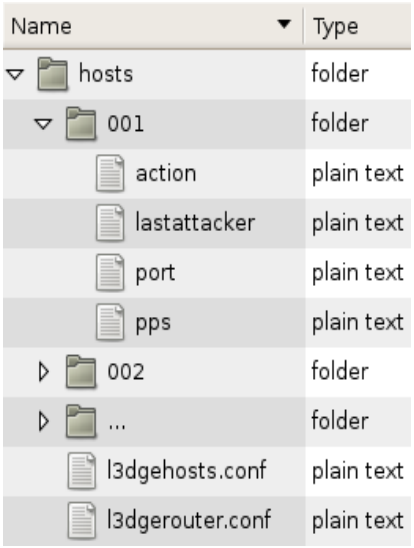

Figure 5 Directory structure hierarchy

The hosts directory contains one directory per host, named '001', '002', etc. along with these directories, two configuration files exist named 'l3dgehost.conf' and 'l3dgerouter.conf'.

Each of the hosts directories contain files where the file name is a key and where the values of these keys are stored within the files as plain ASCII. For L3DGEWorld 1.0 files named 'position', 'pps', 'action' and 'lastattacker' exist, the contents of these files will be discussed in the next section of this document.

V. File Contents

A. 'l3dgehost.conf' contents

The 'l3dgehosts.conf' file is used to assign IP addresses for the various greynet hosts that are monitored. The greynet monitoring software "greymatter" writes to these files, L3DGEWorld 1.0 reads from these files.

Lines beginning with a '#' are treated as comments and ignored.

Lines beginning with a '[' are interpreted as definitions of VLAN membership for the proceeding hosts. Such lines are in the format '[vlan 1]'. All hosts following such a line belong to the specified VLAN until another VLAN is defined.

All other lines associate an IP address with a 3D game avatar ID. These are in the format 'IPAddress IDNumber' eg: '10.10.10.10 10'

B. 'l3dgerouter.conf' contents

The 'l3dgerouter.conf' file is used to store the details required to access and update a Cisco router. In this initial version, only one router may be specified.

Lines beginning with a '#' are treated as comments and ignored.

The IP or hostname of the router is set using a line in the format 'ip=therouter.caia.swin.edu.au'.

The telnet password of the router is set using a line in the format 'telnet=password'.

The enable password of the router is set using a line in the format 'enable=password'.

The interface of the router on which to apply ACLs is set using a line in the format 'int=Fa0/0.2'.

C. 'position' contents

The 'position' file is used to store the coordinates of hosts in the 3D game world, allowing persistent placement of objects. These files are not intended to be modified by the user directly as they are created and read by the game engine itself

The format of these files is simply three floats separated by commas. eg. 'X.x,Y.y,Z.z'.

D. 'pps' contents

The 'pps' file is used to store the packets per second rate that each greynet host is detecting.

The contents of the file is updated by the greynet monitor software greymatter and is stored in the form of a single integer. eg. '10'

E. 'action' contents

An 'action' file is created when an administrator or group of administrators perform an in-game action that is to result in a change in the network configuration.

Actions are written to the relevant action file in the form 'deny' or 'no deny'. By taking the described action and the contents of the lastattacker file, a standard ACL rule is constructed by the output lower abstraction layer, and placed on the configured router.

F. 'lastattacker' contents

The 'lastattacker' file is used to store the IP address of the last source of traffic destined for a particular greynet host.

This is updated by the greymatter program and used by L3DGEWorld to configure the Cisco router to deny traffic from this particular host.

VI. Example attack scenarios

The following is an example attack, detected and acted upon using L3DGEWorld 1.0 running on the test bed described previously.

We first outline the attack from the perspective of the in-game network administrators.

1. Two administrators 'in-game' monitor the unmoving greynet hosts (as in Figure 2)
2. Greynet avatars located geographically close to each other within the map begin to spin
3. The network administrators move closer to one of the avatars and receive textual information explaining precisely the packets per second and the attacking host the greynet host is detecting
4. The first network administrator decides that the event they are seeing is indeed a malicious network anomaly that needs to be prevented
5. The first network administrator shoots one of the spinning greynet host avatars. It turns yellow to indicate it has been acted upon (as in Figure 6)
6. The second network administrator agrees on the course of action and shoots the same host avatar
7. A message is displayed to both users informing them of a successful block being placed against the attacking host and the shot avatar returns to a grey colour.
8. All greynet avatars stop rotating, as further malicious scans on the network have been prevented

We now outline the same attack from a the technical perspective of L3DGEWorld's underlying systems:

1. L3DGEWorld 1.0 and its support programs greymatter are launched
2. In the L3DGEWorld all greynet avatars are stationary
3. An 'attack' (portscan) is launched from the attacking host at IP address 10.10.10.10 directed at the entire 10.10/16 network
4. The greymatter program, listening passively to a number of IP addresses in the 10.10.10/24 space, detects the scan
5. greymatter writes out data to the files 'lastattacker', 'port' and 'pps' for each greynet host that detects activity
6. The L3DGEWorld 1.0 server modification reads these values and updates the spin rates of the scanned hosts based on their received pps
7. The server sends out these changes to all connected clients in the next world update.
8. Two network administrators 'in-game' each shoot a spinning greynet host avatar within a small number of seconds

Figure 6 A collaborating network administrator marks a greynet for ACL placement.

9. The server tracks this, then places an ACL on the Cisco router against the attacker machine
10. The attacking machine can no longer send packets onto the network, and all greynet avatars return to an initial stationary state

VII. Conclusion

This technical report has described 'L3DGEWorld 1.0' a plug-in modification to the Quake III Arena game engine. It allows users to perform network monitoring and control of a live network 'in-game'. We have detailed our initial interface specifications for conveying network activity from a greynet to the Q3A game engine for real-time visualisation and representation. At this stage, this simply consists of key-value pairs stored on a file system as text files. We have also defined the initial interface specifications for the signaling and control protocol that re-configures a standard Cisco enterprise router's ACLs based on resulting in-game actions.

References

[1] W.Harrop, G.Armitage. "Intuitive Real-Time Network Monitoring Using Visually Orthogonal 3D Metaphors," Australian Telecommunications Networks & Applications Conference 2004, (ATNAC2004), Sydney, Australia, December 2004

[2] W. Harrop, G. Armitage, "Real-Time Collaborative Network Monitoring and Control Using 3D Game Engines for Representation and Interaction," VizSEC'06 Workshop on Visualization for Computer Security, Virginia, USA, October-November 2006.

[3] W. Harrop, G. Armitage, "Modifying first person shooter games to perform real time network monitoring and control tasks," 5th Workshop on Network System Support for Games 2006 (Netgames 2006) Singapore, 30-31 October 2006.

[4] "id Software, Doom 1, 2, Quake 1, 2 and III", http://www.idsoftware.com/, July 2006

[5] 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.