PS2 Network Analyzer

Overview

- Network Analysis/Monitoring Overview
- PS2 Architectural Overview
- Project Goals

Network Analysis – Why

- Discover faulty equipment
- Detect malicious users/hackers
- Determine usage patterns and bottlenecks

Network Analysis – Implementation

- Listen to all network traffic
- Process all `interesting' packets
- Record relevant information
- Produce a useable report

Network Analysis – Issues

- Bottlenecks – Network traffic is too much for equipment to handle
- Buffer overflow
- Lost packets due to processing delays
- Erroneous reporting
- Memory intensive tables

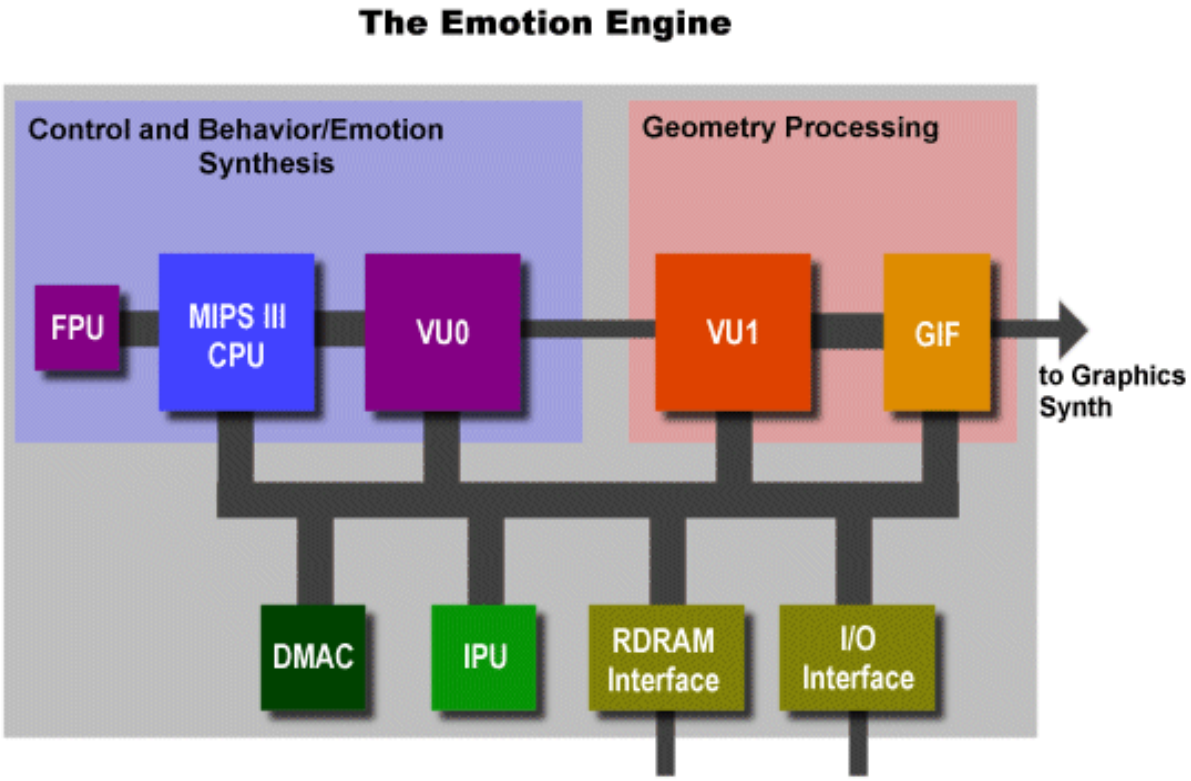
Network Analysis – Solutions

- Layered Architecture
  - Filter out data as soon as we know we can ignore it
- Fast (hash based) network flow table lookups
- Expiry timers
- External Report Generation

PS2 Architecture

- Geared toward multimedia applications (i.e. games)
- Very little data cache
- Fine grained parallelism
- Wide data bus

PS2 Architecture (cont.)



Obstacles

- Memory Requirements
  - How does one fit an over 10MB of libraries plus a 2.5MB kernel into 8MB
- Library/Kernel Compatability
- Library bugs
  - Flawed network driver implementation

Solutions

- Use equivalent libraries
  - uClibc
  - Dietlibc
- Compression
- Open Source Kernel Upgrades
- Available Betas

Implementation

- Remove extraneous libraries.
- Create boot image and compress it.
- Write scripts so that the boot sequence immediately executes the Argus port.

Results


16 Dec 02 01:33:11 tcp 80.144.185.115.* ?> 192.168.1.3.551
16 Dec 02 01:33:12 tcp 66.183.251.225.* ?> 192.168.1.3.400
16 Dec 02 01:33:11 tcp 80.192.168.1.3.* -> 216.6.84.109.634
16 Dec 02 01:33:20 tcp 66.192.168.1.3.* -> 195.132.204.42.634
16 Dec 02 01:33:05 tcp 192.168.1.3.* -> 217.39.127.192.634
16 Dec 02 01:33:25 tcp 192.168.1.3.* -> 213.13.243.155.634
16 Dec 02 01:33:11 tcp 192.168.1.3.* -> 157.193.29.90.987
16 Dec 02 01:33:24 tcp 192.168.1.3.* -> 216.6.84.109.634
16 Dec 02 01:33:15 tcp 192.168.1.3.* -> 195.132.204.42.634
16 Dec 02 01:33:07 tcp 192.168.1.3.* -> 217.39.127.192.634
16 Dec 02 01:33:13 tcp 192.168.1.3.65535 -> 157.193.29.90.987
16 Dec 02 01:33:28 udp 192.168.1.1.* -> 192.168.1.255.520
SONY
DELL

Q & A

- Why?
  - I wanted to do something `practical' and this seemed more practical than spending $300 for a Rabbit card which I wouldn't use in the future
  - Why not