Nouveau
reverse engineering NVIDIA

and saving kittens....

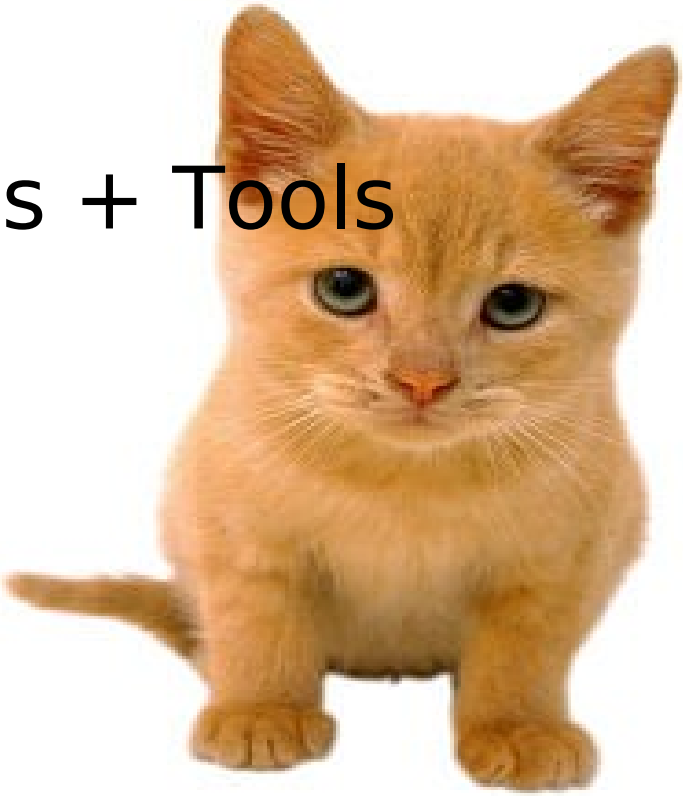
Dave Airlie + Ben Skeggs

airlied@linux.ie

linux.con f.au 2007

Introduction

- Who are we?
- What is with the kittens?
- Nouveau Project Introduction
- NVIDIA Card Info
- Reverse Engineering Methods + Tools
- Current status
- Future Direction



Kittens?

Kittens?

Nouveau Project

- Started by Stephane Marchesin – Feb 2005
- Serious work – Jun 2005
- Announced at FOSDEM – Feb 2006
- 5-6 current developers
  - pmdata - Patrice Mandin
  - Mat – Matthieu Castet
  - Jkolb – Jeremy Kolb
- Reverse Engineered

Why do this?

- Mainly personal reasons!!
- “Binary kept crashing even for 2D” - marcheu
- “Didn't like binary driver” - pmdata
- “Fun, sort of...” - darktama
- “Hey my G5 can't do dual-head” – me!!
- Interesting engineering challenge
- Future desktops involve using 3D

Why we don't do this

- Hype

Why we don't do this

- Hype
- Controversy

Why we don't do this

- Hype
- Controversy
- Fame

Why we don't do this

- Hype
- Controversy
- Fame
- Infamy

For any posters on...

Slashdot NEWS FOR NERDS. STUFF THAT MATTERS.

OGnews™ EXPLORING THE FUTURE OF COMPUTING

nvnews

You are correct...

- we are stupid

You are correct...

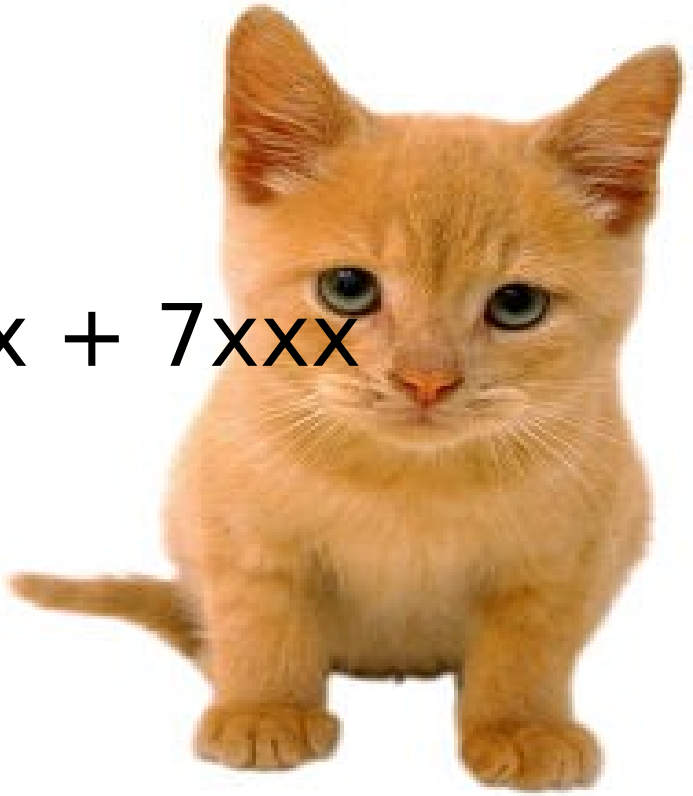
- we are stupid
- we had no idea that NVIDIA could obsolete us

You are correct...

- we are stupid
- we had no idea that NVIDIA could obsolete us
- NVIDIA are going to stop producing drivers because of us

NVIDIA Card Families

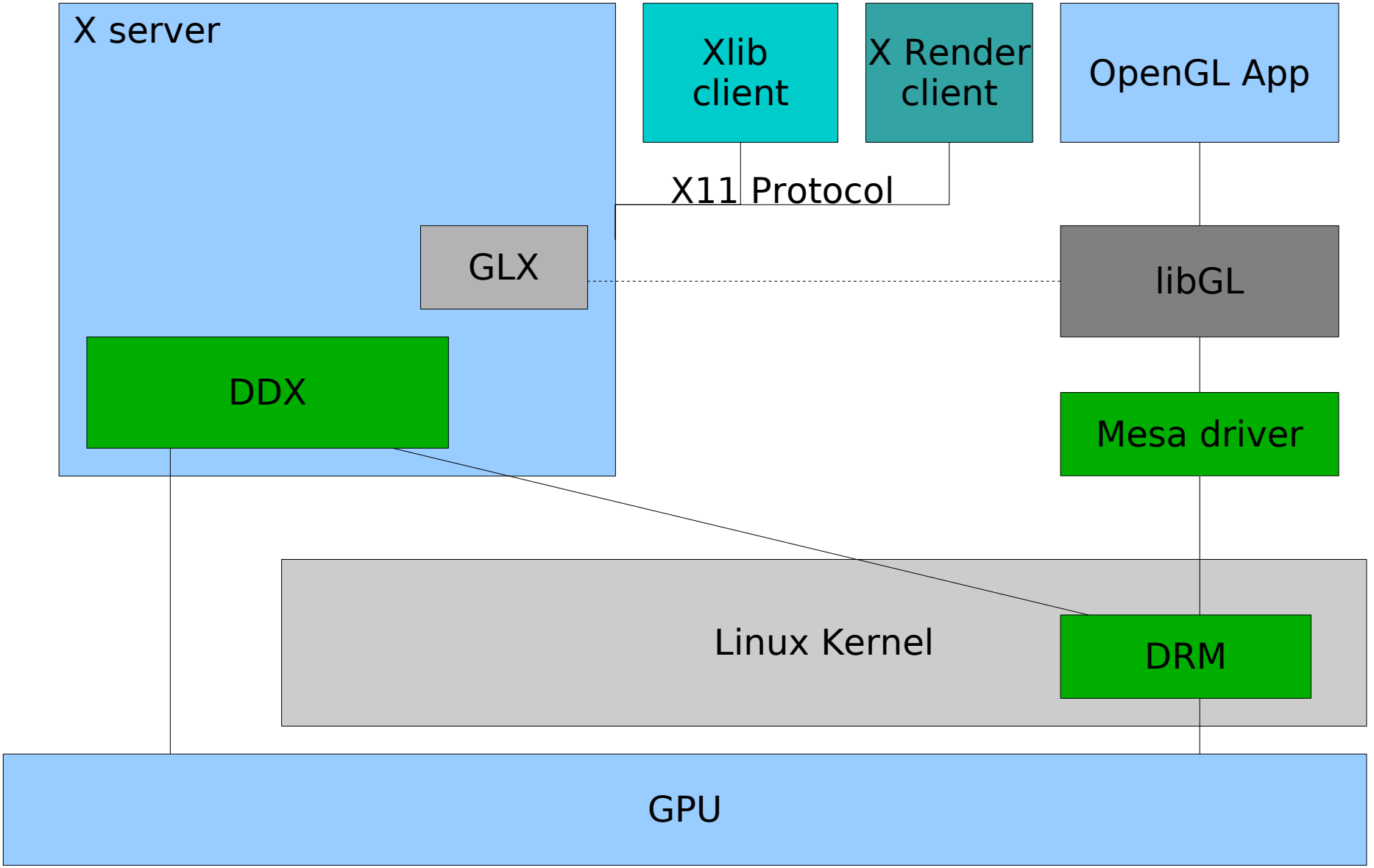
- nv04 - TNT1
- nv10 – GeForce 256
- nv11/5 – GeForce 2 + 4MX
- nv2x – GeForce 3 + 4TI
- nv3x – GeForce FX 5xxx
- nv4x/c5x/c7x – GeForce 6xxx + 7xxx
- nv5x/G80 – GeForce 8xxx



NVIDIA Card Architecture

- Multiple HW contexts since nv3
  - Multiple secure FIFOs
  - FIFOs reference objects allocated by secure component
- nv40 is OpenGL 2.0 hardware
- nv20-nv40 have hardware TNL
- Nv20 has vertex shading
- Nv30 onwards has full shaders

DRI Architecture



Reverse Engineering Tools

http://dri.freedesktop.org/wiki/ReverseEngineering

renouveau

- Blackbox Reverse Engineering
  - Create an OpenGL context
  - Scan process mappings for FIFO
  - Dump the FIFO and register contents
  - Do something interesting with GL
  - Redump the FIFO
  - Compare the two dumps
  - Rinse + repeat

Userspace MMIO tracers

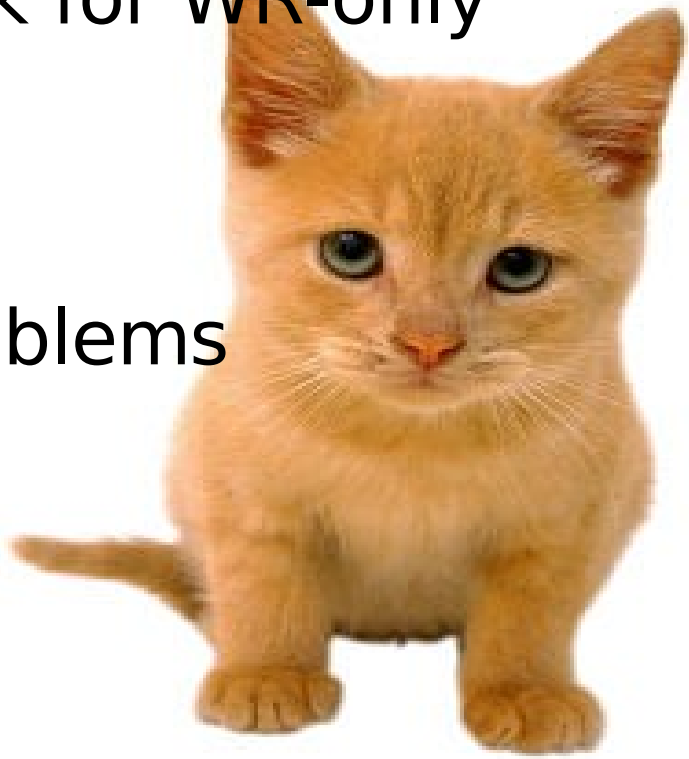
- Valgrind-mmt
  - Written by airlied for ATI RE work

Userspace MMIO tracers

- Valgrind-mmt
  - Written by airlied for ATI RE work
- Valgrind-mmt-extend
  - Extended by Tilman Sauerbeck for WR-only regs

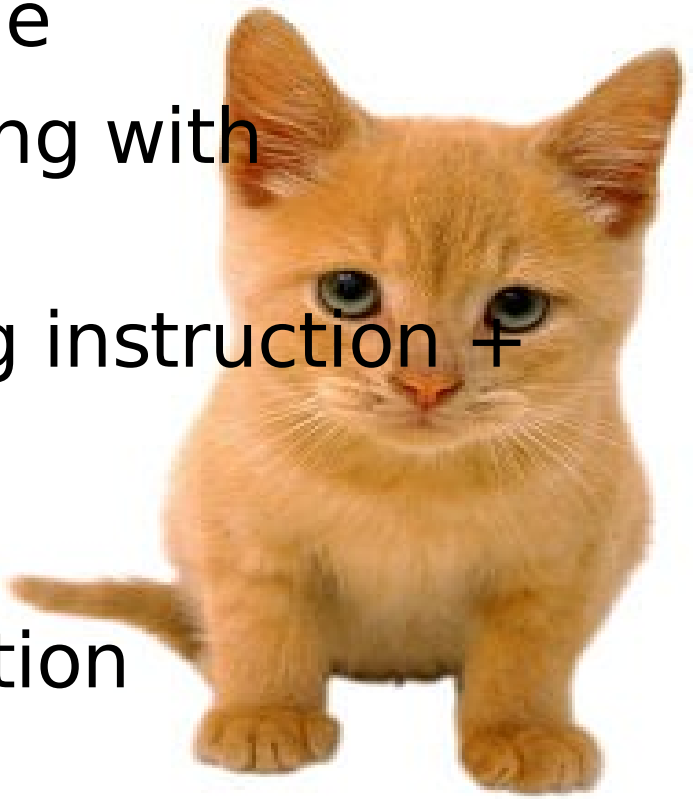
Userspace MMIO tracers

- Valgrind-mmt
  - Written by airlied for ATI RE work
- Valgrind-mmt-extend
  - Extended by Tilman Sauerbeck for WR-only regs
- Libsegfault
  - Jerome Glisse for ATI 9800 problems



kmmio

- Problem with tracing in-kernel MMIO access
- Written by Jeff Muizelaar
  - Trap ioremap/ioremap_nocache
  - Don't actually back the mapping with anything
  - On pagefault, read the faulting instruction + dump
  - Back the mapping
  - Singlestep the faulting instruction
  - Remove mapping back



BIOS tracing

- x86emu + vbetool
- Hacked up by airlied for ATI and Intel RE work
- Emulates the bios using x86emu
- Dump IO register access in emulation handler
- Add some smart dumping

Available Information

- “nv” driver
- Utah/GLX 3D up to nv18
- Haiku/BeOS 2D/3D up to nv18
- Nvidia SDK up to nv5
- Pre-obscured old driver in Xfree86

Status - DRM

- Instance RAM allocation
- FIFO initialization
- HW context switching on little-endian:
  - nv4x
  - Depends on wierd voodoo
- Being worked on for other cards and big endian

2D DDX

- Based on nv driver
- Basic EXA support using 2D engine
- Randr 1.2 support in branch
  - 2 CRTs works so far
  - TMDS + CRT not so good yet but getting there

3D driver

- Mesa SW TCL driver
  - nv04 -> nv4x
- No Texturing or objects
- State caching
- glxgears on nv4x – benchmarking in progress

Future Plans

- Quake 3 jump

Future Plans

- Quake 3 jump
- Texturing + memory manager
- Multiple DRI locks

Future Plans

- Quake 3 jump
- Texturing + memory manager
- Multiple DRI locks
- Randr 1.2 multi-head support
- Hopefully a beta driver in Q4 07...

Can I help?

- Developer time
  - Can you write C or device driver experience
  - Graphics drivers are not that hard...

Can I help?

- Developer time
  - Can you write C or device driver experience
  - Graphics drivers are not that hard...

  ... once you get past the TLAs

  DDX, DRM, DRI...

Can I help?

- Developer time
  - Can you write C or device driver experience
  - Graphics drivers are not that hard...

  ... once you get past the TLAs

  DDX, DRM, DRI...
- Lots of people providing renouveau dumps
- G80 renouveau support
- HW donations perhaps....
- #nouveau on irc.freenode.net

That $10000 pledge

- Not endorsed by nouveau project
- Independently started
- No-strings attached
- marcheu currently working out finer details
  - HW purchases most likely

That $10000 pledge

Just remember....

Just remember....

The HOFF uses binary drivers