# Kernel Loading on Macs (the sad story)

Dave Eckhardt
de0u@andrew.cmu.edu



# The Problem

We just wanted to step through the first few instructions, but Open Firmware never accepted the binary no matter how much tweaking we did with the command line parameters. We transfer the file over but can't get past a "CLAIM failed" which suggests memory is corrupted or memory allocation failed.



# "CLAIM failed"

- Means that the $claim method of the package whose instance handle is the "memory" property of /chosen threw an exception
- It does this when you ask for a range of *physical* memory which is
  - Already in use – this is why you often need to "reset-all" to run a



# Mac OpenFirmware Loader

- Good news
  - It loads PE
  - It loads XCOFF
  - It loads ELF!
- Bad news
  - It loads *one* XCOFF on a routine basis
  - It loads *two* ELFs on a routine basis
    - which are derived from each other

## Central Problem

- OpenFirmware on Macs likes to run with VM on
  - ?real-mode == 0
- It likes everything to be direct-mapped
- This is great for the One True XCOFF (BootX)
  - Which wants to run V=0xsmall, R=0xsmall



## Central Problem

- The Approved Structure
  - Load a kernel image into memory
  - Link in some modules
  - Using V=R=0xsmall for text, data, stack
  - Then vanish like a puff of smoke



## Features of 9mac

- Linked to run at 0x8big
- This assumption embedded in kernel code
- Also present in libmach executable library
  - (rough equivalent of GNU "bfd")
- Would be nice to maintain this



## Executable File Formats

- Plan 9 a.out
  - Simple, fairly clear
  - OpenFirmware won't load it
- XCOFF - "native" OpenFirmware format
  - ql can emit this
  - allows specification of independent V,R for text, data sections!
- ELF

## Let's try XCOFF

- XCOFF - "native" OpenFirmware format
  - ql can emit this
  - allows specification of independent V, R for text, data sections!
  - Issue: XCOFF files spat out by ql set V, R to same value
    - Now, why would it do that???
  - Resolution: hack ql to emit independent V, R



## Let's try XCOFF

- XCOFF - "native" OpenFirmware format
  - OpenFirmware XCOFF loader doesn't interpret separate V, R correctly
    - Older machine: tries to fetch entry point out of procedure descriptor using virtual address, though it never set up a mapping
    - Newer machine: tries to claim physical memory located at 0x8big, which fails
    - Regardless: behavior is *different* – not



## Let's try XCOFF

- XCOFF - "native" OpenFirmware format
  - OpenFirmware XCOFF loader doesn't interpret separate V, R correctly
    - Older machine: tries to fetch entry point out of procedure descriptor using virtual address, though it never set up a mapping
    - Newer machine: tries to claim physical memory located at 0x8big, which fails
    - Regardless: behavior is *different* – not



## Let's *not* try XCOFF?

- ELF
  - What will happen if V != R?
    - On which machines?
  - What does ql spit out for V, R for ELF files?
  - By the way, acid won't debug ELF or XCOFF binaries
- How about Plan 9 a.out?
  - Can we teach OpenFirmware to load

## Teaching OF about a.out

- It should be possible
  - OF based on a general-purpose programming language
  - Has portable operations for memory-allocate, memory-map, initialize-register-to-value, etc.
- Constructive proof
  - /lib/tftpd/lumbering actually loads a Plan 9 a.out, which runs



## Teaching OF about a.out

- ✓ It should be possible
- ✓ Constructive proof
- But Apple doesn't want us to do this
  - New iMac in lab hides several necessary ingredients
    - Unpublished old way to determine OF CI entry point has been hidden
    - *Published* "state-valid" interface has



## Options

- Teach OF about a.out – nope
- Link 9mac as XCOFF or ELF?
  - At mercy of random/lame object file interpretations since V != R
- Gee, that general-purpose Mac OpenFirmware sure likes to load little secondary boot loaders which are V=R!
  1. Have it load a virtually-linked



## Suggestion

- Write tiny secondary boot loader
  - XCOFF or ELF, who cares?
  - Contains actual a.out file in a character array
  - Calls OF client services to claim, map memory
    - Example code (in Forth) in /lib/tftpd/lumbering :-)
- Result

## Another Suggestion

- It would be nice if Apple's OF could load more than one program!