Writing Linux Device Drivers in Assembly Language

(Full Contents)

0 Preface and Introduction 3
- 0.1 Randy's Introduction 3
- 0.2 Why Assembly Language? 3
- 0.3 Assembly Language Isn't That Bad 4

1 An Introduction to Device Drivers 5

2 Building and Running Modules 7
- 2.1 The "Hello World" Driver Module 8
- 2.2 Compiling and Linking Drivers 13
- 2.3 Version Dependency 14
- 2.4 Kernel Modules vs. Applications 16
- 2.5 Kernel Stack Space and The Current Process 18
- 2.6 Compiling and Loading 19
  - 2.6.1 A Make File for SKULL 19
- 2.7 Version Dependency and Installation Issues 20
- 2.8 Platform Dependency 20
- 2.9 The Kernel Symbol Table 21
- 2.10 Initialization and Shutdown 21
- 2.11 Error Handling in init_module 22
- 2.12 The Usage Count 23
- 2.13 Resource Allocation (I/O Ports and Memory) 24
- 2.14 Automatic and Manual Configuration 26
- 2.15 The SKULL Module 27
- 2.16 Kernel Versions and HLA Header Files 38
  - 2.16.1 Converting C Header Files to HLA and Updating Header Files 39
  - 2.16.2 Converting C Structs to HLA Records 41
  - 2.16.3 C Calling Sequences and Wrapper Functions/Macros 43
  - 2.16.4 Kernel Types vs. User Types 46
- 2.17 Some Simple Debug Tools 46

3 Character Drivers 51
- 3.1 The Design of scullc 51
- 3.2 Major and Minor Numbers 52
- 3.3 Dynamic Allocation of Major Numbers 53
- 3.4 Removing a Driver From the System 56
- 3.5 dev_t and kdev_t 56
- 3.6 File Operations 58
  - 3.6.1 The llseek Function 65
  - 3.6.2 The read Function 66
- 3.7 The write Function 66
- 3.8 The readdir Function 67
  - 3.8.1 The poll Function 67
  - 3.8.2 The _ioctl Function 67
  - 3.8.3 The mmap Function 68
  - 3.8.4 The open Function 68
  - 3.8.5 The flush Function 68

3.8.6 The release Function 68
3.8.7 The fsync Function 68
3.8.8 The fasync Function 69
3.8.9 The lock Function 69
3.8.10 The readv and writev Functions 69
3.8.11 The owner Field 70
3.9 The file Record 70
3.9.1 file.f_mode : linux.mode_t 70
3.9.2 file.f_pos : linux.loff_t 70
3.9.3 file.f_flags : dword 70
3.9.4 file.f_op : linux.file_operations 71
3.9.5 file.private_data : dword 71
3.9.6 file.f_dentry : linux.dentry 71
3.10 Open and Release 71
3.10.1 The Open Procedure 71
3.10.2 The release Procedure 78
3.10.3 Kernel Memory Management (kmalloc and kfree) 78
3.10.4 The scull_device Data Type 79
3.10.5 A (Very) Brief Introduction to Race Conditions 80
3.10.6 The read and write Procedures 82
3.11 The scullc Driver 92
3.11.1 The scullc.hhf Header File 92
3.12 The scullc.hla Source File 94
3.13 Debugging Techniques 108
3.13.1 Code Reviews 108
3.13.2 Debugging By Printing 110
3.13.2.1 linux.printk 110
3.13.2.2 Turning Debug Messages On and Off 111
3.13.2.3 Debug Zones 112
3.13.3 Debugging by Querying 113

