

Contents

	<i>Page</i>
Preface	ix
Related publications	xi
Ordering Cray Research publications	xi
Conventions	xi
Reader comments	xiii
Introduction [1]	1
Introduction to security concepts	1
Concepts of computer security	1
DoD criteria for trusted systems	2
Security policy	3
Accountability	4
Assurance	4
The UNICOS implementation of MLS	4
Cray ML-Safe configuration of the UNICOS system	5
Discretionary access controls	6
Mandatory access controls	7
Security levels	8
Security compartments	8
Definition of dominance	9
User's security label ranges	10
Examples of security labels	11
System high and system low security labels	17
Special security levels	17
Accountability objective	18
SG-2111 10.0	iii

	<i>Page</i>
Assurance objective	18
Reference monitor concept	19
System management	19
Logging in and Using Passwords [2]	21
Interactive logins	21
Example 1: Interactive login screen and the <code>spget</code> command	23
Example 2: Use of the <code>login -L</code> command	24
Interactive Cray ML-Safe logins	24
Displaying the operating system's MLS environment	27
Example 3: Displaying the operating system's security environment (<code>spget -s</code>)	28
Remote logins with SecurID card	28
Passwords	29
Last login notification	30
Generic login message	30
Minimum password size	30
Password locking	32
Machine-generated passwords	32
Example 4: Machine-generated password example	33
Login limit and login disable time-out	33
Password aging	34
Example 5: Password aging messages	35
Using Access Control Lists (ACLs) [3]	37
Overview of ACLs	37
Maintaining ACLs	39
Creating entries in an intermediate ACL file	39
Interactive creation of intermediate ACL files (<code>spacl -a</code>)	40
Example 6: Creating ACL entries (<code>spacl -a</code>)	41

	<i>Page</i>
Creation of intermediate ACL file entries using an input file (<code>spacl -i</code>)	42
Example 7: Creating ACL entries (<code>spacl -i</code>)	42
Displaying intermediate ACL files (<code>spacl -l</code>)	42
Example 8: Displaying an intermediate ACL file (<code>spacl -l</code> and <code>-s</code>)	43
Removing entries in intermediate ACL file	43
Interactive removal of intermediate ACL files (<code>spacl -r</code>)	43
Example 9: Removing an intermediate ACL file entry (<code>spacl -r</code>)	45
Removing entries in intermediate ACLs files using an input file (<code>spacl -i</code>)	46
Modifying intermediate ACL files	46
Example 10: Modifying an existing ACL entry	47
Applying ACLs to files (<code>spset -a</code>)	48
Example 11: Applying ACLs (<code>spset -l</code>)	50
Example 12: Applying ACLs (<code>spset -a</code>)	51
Displaying ACLs applied to files (<code>spget -a</code>)	51
Example 13: Displaying ACL entries (<code>spget -e</code>)	52
Example 14: Displaying ACL entries (<code>spget -a</code>)	52
Duplicating ACLs (<code>spset -d</code> or <code>spacl -t</code>)	52
Example 15: Duplicating ACLs (<code>spset -d</code>)	53
Example 16: Duplicating ACLs (<code>spacl -t</code>)	54
Removing ACLs (<code>spclr -a</code>)	54
Example 17: Removing ACLs from files (<code>spclr -a</code>)	55
How ACLs are checked	55
Displaying masked ACL permissions (<code>spget -ae</code>)	57
Example 18: Displaying the masked ACL mode bits (<code>spget -ae</code>)	58
Example 19: Displaying the masked ACL mode bits (<code>spget -ae</code>)	59
Example 20: Displaying the masked ACL mode bits (<code>spget -ae</code>)	59
ACLs and root access	59
umask(1) default access permissions	60

	<i>Page</i>
Using Security Labels [4]	61
UNICOS security policy	61
Changing security labels (<code>setulvl</code> and <code>setucmp</code>)	62
Example 21: Example of <code>setulvl</code> command	63
Example 22: Example of <code>setulvl level2</code> command	64
Example 23: Example of <code>setucmp</code> command	65
MLS permissions	66
 Creating Directories and Files [5]	 69
Assigning security labels to objects	69
Assigning labels to directories	69
Example 24: Example of <code>mkdir -L</code> command	70
Wildcard directories	71
Multilevel directories (MLDs)	71
Example 25: Example of MLD <code>/tmp</code> structure	75
Assigning security labels to files	76
Terminal drivers	76
Displaying the security attributes of directories and files	78
Example 26: Displaying a file's security attributes (<code>ls -le</code> command)	79
Example 27: Displaying a file's security attributes (<code>spget -f</code> command)	80
Creating files	80
Example 28: Example of creating files (part 1)	81
Example 29: Example of creating files (part 2)	82
Example 30: Example of creating files (part 3)	83
Removing files and directories (<code>spclr</code> , <code>rm</code> , and <code>rmdir</code>)	83
Example 31: Example of <code>spclr -s</code> command	85
Example 32: Example of <code>rm</code> and <code>rmdir</code> commands	86
Setuid and setgid files	87

	<i>Page</i>
Example 33: Copying and linking setuid and setgid files	88
Archive commands	88
Network Access [6]	91
RQS controls	91
Station listable output	92
Miscellaneous Information [7]	93
The cron command	93
Example 34: Example of cron command using qsub	93
Example 35: Example of cron command without using qsub	94
Using the su command	94
Tape security	94
Data migration security	94
Cray/REELlibrarian security	95
Appendix A Overview of TCSEC Trusted System Divisions	97
Division D criteria	97
Division C criteria	97
Division B criteria	99
Division A criteria	101
Figures	
Figure 1. Concepts of computer security	3
Figure 2. Example of using hierarchical security labels	13
Figure 3. Example of using nonhierarchical labels	14
Figure 4. Example of security labels	16
Figure 5. Logging in on a Cray ML-Safe system configuration	26
Figure 6. The SecurID card	29
Figure 7. Password guidelines and features	31
SG-2111 10.0	vii

	<i>Page</i>
Figure 8. Connections between ACLs and files	49
Figure 9. Flowchart of how UNICOS ACLs are checked	56
Figure 10. Mandatory access controls; UNICOS security policy	62
Figure 11. Permissions	67
Figure 12. Structure of a multilevel directory (MLD)	72
Figure 13. Displaying a file's security attributes (<code>ls -le</code> command)	79
Figure 14. Divisions	98
 Tables	
Table 1. Accessing data with nonhierarchical labels	15