Integrated/unsupported permissions in Simplified Policy for Ver 2.1

November 13, 2006

Contents

Simplified Policy Description Language(SPDL) simplifies SELinux by reducing number of permissions. This reduction is done by not supporting permissions and integrating permissions. This document describes what kind of permissions are not supported in Simplified Policy Description Language(SPDL) and what kind of permissions are integrated in SPDL rules. *Not supported* means the permissions are allowd to all domains. *Integrated* means permissions are treated as one permission.
Not supported permissions are listed in section 1. Integration of permission is described in section 2.

1 How to look at tables

Permissions are listed in table format. How to look at table is explained.

(1) Notation to represent domain and type

- global
  It means all domains.
- from, entry, to
  from domain, entry point, to domain in domain transition rule.

(2) Notation to represent many permissions
Following are used to describe set of permissions(it is to save space.)

- file_type
  All types for files.
- all_file_class
  It means all object classes related to file(dir file lnk_file sock_file fifo_file chr_file blk_file)
- notdevfile_class
  Means all file related object classes except device(dir file lnk_file sock_file fifo_file)
- notdevdir_class
  Means file related object classes except device and dir(file lnk_file sock_file fifo_file)
- notdir_class
  Means file related object classes except dir(file lnk_file sock_file fifo_file chr_file blk_file)
- socket_common_all_perms
  Permissions common to sockets(ioctl readwrite create getattr setattr lock relabelfrom relabelto append bind connect listen accept getopt setopt shutdown recvfrom sendto recv_msg send_msg name_bind)

- tcp_socket_all_perms
  Permissions common to tcp socket(ioctl read write create getattr setattr lock relabelfrom relabelto append bind connect listen accept getopt setopt shutdown recvfrom sendto recv_msg send_msg name_bind connectto newconn acceptfrom node_bind name_connect)
- udp_socket_all_perms
  Permissions common to udp socket(ioctl read write create getattr setattr lock relabelfrom relabelto append bind connect listen accept getopt setopt shutdown recvfrom sendto recv_msg send_msg name_bind node_bind)

(3) Tables in section 2
These tables describes what kind of permissions are not supported. Titles of table show why these permissions are not supported. For example, the title of table 1 is Dead permission. It means permissions in table is not supported because these are dead permission in SELinux. Detailed reason why unsupported will be described in future :-)
Let's see example. First line in table1, all_file_class, swapon, global , file_type is described. It means, all domains(global) are allowed permission swapon for all object class related to file(all_file_class), to all types related to file(file_type). It equals following allow statement in SELinux.

```
allow global file\_type:all\_file\_class swapon;
```

So this means, swapon permission is allowed(=not supported).

(4) Tables in section 3
These tables describe how permissions are integrated in SPDL. Let's see example. Look at table 11. This table describes permissions allowed when using *allow filename r;* statement. *all_file_class, ioctl lock read, domain, type* are described here. This means, ioctl lock read permissions for all file related object classes are allowed.

Following was automatically generated by genmacro.py

2 Unsupported permission

Table 1: Dead Permission

Object class	Permission	Domain	Type
blk_file chr_file dir fifo_file file lnk_file sock_file	swapon	global	file_type
all_socket_class	relabelfrom relabelto	global	global
unix_stream_socket	acceptfrom newconn	global	global
netlink_firewall_socket	nlmsg_read	global	global
netlink_ip6fw_socket	accept append bind connect create getattr getopt ioctl listen lock name_bind nlmsg_read nlmsg_write read recv_msg recvfrom relabelfrom relabelto send_msg sendto setattr setopt shutdown write	global	global
netlink_tcpdiag_socket	nlmsg_write	global	self
ipc	associate create destroy getattr read setattr unix_read unix_write write	global	global

Table 2: Unsupported features in SPDL

Object class	Permission	Domain	Type
security	compute_member setcheckreqprot	global	security_t

Table 3: Unsupported because related to DAC and POSIX capabilities

Object class	Permission	Domain	Type
process	getcap setcap	global	global

Table 4: Unsupported because low effect to security

Object class	Permission	Domain	Type
blk_file chr_file dir fifo_file file lnk_file sock_file	getattr	global	file_type global
process	execheap execmem execstack fork getpgid getsched getsession noatsecure rlimitinh setpgid share siginh	global	global
system	ipc_info	global	global
capability	lease	global	self
filesystem	associate	file_type	fs_type
filesystem	getattr quotaget	global	fs_type

Table 5: Unsupported because of complete overlap

Object class	Permission	Domain	Type
capability	audit_write ipc_owner kill net_bind_service sys_ptrace	global	self
dir	add_name remove_name	global	file_type global

Table 6: Unsupported because of Partly overlap

Object class	Permission	Domain	Type
process	setrlimit setsched	global	global
capability	audit_control	global	self

Table 7: Implicit overlap

Object class	Permission	Domain	Type
fd	use	global	global
process	setexec	global	global
tcp_socket	accept append bind connect create getattr getopt ioctl listen lock read setattr setopt shutdown write	global	self
udp_socket	accept append bind connect create getattr getopt ioctl listen lock read setattr setopt shutdown write	global	self
unix_dgram_socket	create getattr getopt ioctl lock relabelfrom relabelto setattr setopt shutdown	global	global
unix_stream_socket	create getattr getopt ioctl lock relabelfrom relabelto setattr setopt shutdown	global	global

Table 8: Pending.. May be changed

Object class	Permission	Domain	Type
packet	recv send	global	unlabeled_t
file	execmod	global	file_type
packet_socket	accept append bind connect create getattr getopt ioctl listen lock name_bind read recv_msg recvfrom relabelfrom relabelto send_msg sendto setattr setopt shutdown write	global	self
key_socket	accept append bind connect create getattr getopt ioctl listen lock name_bind read recv_msg recvfrom relabelfrom relabelto send_msg sendto setattr setopt shutdown write	global	self

Table 9: Does not support user space AVC

Object class	Permission	Domain	Type
passwd	chfn chsh crontab passwd rootok	global	self
dbus	acquire_svc send_msg	global	global
nscd	admin getgrp gethost getpwd getstat shmemgrp shmemhost shmempwd	global	global
association	*	global	unlabeled_t

3 Integrated permissions by SPDL

3.1 Integrated permissions for file allow

Table 10: Option:s

Object class	Permission	Domain	Type
dir	read search	domain	type

Table 11: Option:r

Object class	Permission	Domain	Type
fifo_file file lnk_file sock_file	ioctl lock read	domain	type
dir	ioctl lock	domain	type

Table 12: Option:x

Object class	Permission	Domain	Type
dir fifo_file file lnk_file sock_file	execute	domain	type
file	execute_no_trans	domain	type

Table 13: Option:w

Object class	Permission	Domain	Type
dir fifo_file file lnk_file sock_file	append create link rename setattr unlink write	domain	type
dir	reparent rmdir	domain	type

Table 14: Option:o

Object class	Permission	Domain	Type
fifo_file file lnk_file sock_file	write	domain	type

Table 15: Option:a

Object class	Permission	Domain	Type
fifo_file file lnk_file sock_file	append	domain	type

Table 16: Option:e

Object class	Permission	Domain	Type
dir	rename reparent rmdir unlink write	domain	type
fifo_file file lnk_file sock_file	rename unlink	domain	type

Table 17: Option:c

Object class	Permission	Domain	Type
dir	append create link write	domain	type
fifo_file file lnk_file sock_file	create link	domain	type

Table 18: Option:t

Object class	Permission	Domain	Type
dir	setattr	domain	type
fifo_file			
file			
lnk_file			
sock_file			

Table 19: Option:relabel,This is used intenally in allowpriv part_relabel

Object class	Permission	Domain	Type
blk_file	relabelfrom	domain	type
chr_file	relabelto		
dir			
fifo_file			
file			
lnk_file			
sock_file			

Table 20: Option:devcreate,This is used internally in allowpriv devcreate

Object class	Permission	Domain	Type
blk_file	create	domain	type
chr_file	link		
	rename		
	unlink		

Table 21: Option:setattr,This is used internally in allowpriv setattr

Object class	Permission	Domain	Type
blk_file	setattr	domain	type
chr_file			
dir			
fifo_file			
file			
lnk_file			
sock_file			

3.2 Integrated permissions for allowdev

In directory pointed by allowdev -root, following are additionally allowed for allowfile rules. By default, directory under /dev.

Table 22: Option:s

Object class	Permission	Domain	Type
blk_file chr_file	getattr	domain	type

Table 23: Option:r

Object class	Permission	Domain	Type
blk_file chr_file	ioctl lock read	domain	type

Table 24: Option:x

Object class	Permission	Domain	Type
blk_file chr_file	execute	domain	type

Table 25: Option:w

Object class	Permission	Domain	Type
blk_file chr_file	append setattr write	domain	type

Table 26: Option:o

Object class	Permission	Domain	Type
blk_file chr_file	write	domain	type

Table 27: Option:a

Object class	Permission	Domain	Type
blk_file chr_file	append	domain	type

Table 28: Option:e

Object class	Permission	Domain	Type
blk_file chr_file	rename unlink	domain	type

Table 29: Option:c

Object class	Permission	Domain	Type
blk_file chr_file	create link	domain	type

Table 30: Option:t

Object class	Permission	Domain	Type
blk_file chr_file	setattr	domain	type

3.3 Permissions integrated in allowdev -tty rules

Table 31: Option:r

Object class	Permission	Domain	Type
chr_file lnk_file	getattr ioctl lock read	domain	type
dir	getattr ioctl lock read search	domain	type

Table 32: Option:w

Object class	Permission	Domain	Type
chr_file lnk_file	append setattr write	domain	type
dir	setattr write	domain	type

Table 33: Option:admin

Object class	Permission	Domain	Type
chr_file lnk_file	create relabelfrom relabelto rename unlink	domain	type
dir	create link reparent rmdir unlink	domain	type

3.4 Permissions integrated in allowdev -pts rules

Table 34: Option:r

Object class	Permission	Domain	Type
chr_file lnk_file	getattr ioctl lock read	domain	type
dir	getattr ioctl lock read search	domain	type

Table 35: Option:w

Object class	Permission	Domain	Type
chr_file lnk_file	append setattr write	domain	type
dir	setattr write	domain	type

Table 36: Option:admin

Object class	Permission	Domain	Type
chr_file lnk_file	create relabelfrom relabelto rename unlink	domain	type
dir	create link reparent rmdir unlink	domain	type

3.5 Integrated permissions for allownet rules

Table 37: Option:tcp suboption:use

Object class	Permission	Domain	Type
tcp_socket	accept append bind connect create getattr getopt ioctl listen lock read setattr setopt shutdown write	domain	type

Table 38: Option:udp suboption:use

Object class	Permission	Domain	Type
udp_socket	accept append bind connect create getattr getopt ioctl listen lock read setattr setopt shutdown write	domain	type

Table 39: Option:raw suboption:use

Object class	Permission	Domain	Type
rawip_socket	accept bind connect create getattr getopt ioctl listen lock setattr setopt shutdown	domain	type
rawip_socket	append read write	domain	type
capability	net_raw	domain	self

Table 40: Option:tcp suboption:server

Object class	Permission	Domain	Type
tcp_socket	name_bind	domain	type
tcp_socket	recv_msg send_msg	domain	port_type

Table 41: Option:tcp suboption:client

Object class	Permission	Domain	Type
tcp_socket	name_connect recv_msg send_msg	domain	type

Table 42: Option:udp suboption:server

Object class	Permission	Domain	Type
udp_socket	name_bind	domain	type
udp_socket	recv_msg send_msg	domain	unpriv_port_type

Table 43: Option:udp suboption:client

Object class	Permission	Domain	Type
udp_socket	recv_msg send_msg	domain	type

Table 44: Option:node suboption:tcp_send

Object class	Permission	Domain	Type
node	tcp_send	domain	type

Table 45: Option:node suboption:udp_send

Object class	Permission	Domain	Type
node	udp_send	domain	type

Table 46: Option:node suboption:rawip_send

Object class	Permission	Domain	Type
node	rawip_send	domain	type

Table 47: Option:node suboption:tcp_recv

Object class	Permission	Domain	Type
node	tcp_recv	domain	type

Table 48: Option:node suboption:udp_recv

Object class	Permission	Domain	Type
node	udp_recv	domain	type

Table 49: Option:node suboption:rawip_recv

Object class	Permission	Domain	Type
node	rawip_recv	domain	type

Table 50: Option:node suboption:tcp_bind

Object class	Permission	Domain	Type
tcp_socket	node_bind	domain	type

Table 51: Option:node suboption:udp_bind

Object class	Permission	Domain	Type
udp_socket	node_bind	domain	type

Table 52: Option:node suboption:rawip_bind

Object class	Permission	Domain	Type
rawip_socket	node_bind	domain	type

Table 53: Option:netif suboption:tcp_send

Object class	Permission	Domain	Type
netif	tcp_send	domain	type

Table 54: Option:netif suboption:udp_send

Object class	Permission	Domain	Type
netif	udp_send	domain	type

Table 55: Option:netif suboption:rawip_send

Object class	Permission	Domain	Type
netif	rawip_send	domain	type

Table 56: Option:netif suboption:tcp_recv

Object class	Permission	Domain	Type
netif	tcp_recv	domain	type

Table 57: Option:netif suboption:udp_recv

Object class	Permission	Domain	Type
netif	udp_recv	domain	type

Table 58: Option:netif suboption:rawip_recv

Object class	Permission	Domain	Type
netif	rawip_recv	domain	type

3.6 Integrated permissions for allowcom rules

Table 59: Option:unix suboption:r

Object class	Permission	Domain	Type
unix_dgram_socket	accept bind listen name_bind read recv_msg recvfrom	domain	type
unix_stream_socket	accept bind listen name_bind read recv_msg recvfrom	domain	type

Table 60: Option:unix suboption:w

Object class	Permission	Domain	Type
unix_dgram_socket	append connect send_msg sendto write	domain	type
unix_stream_socket	append connect connectto send_msg sendto write	domain	type

Table 61: Option:sem suboption:r

Object class	Permission	Domain	Type
sem	associate getattr read unix_read	domain	type

Table 62: Option:sem suboption:w

Object class	Permission	Domain	Type
sem	create destroy setattr unix_write write	domain	type

Table 63: Option:msg suboption:r

Object class	Permission	Domain	Type
msg	send	domain	type

Table 64: Option:msg suboption:w

Object class	Permission	Domain	Type
msg	receive	domain	type

Table 65: Option:msgq suboption:r

Object class	Permission	Domain	Type
msgq	associate getattr read unix_read	domain	type

Table 66: Option:msgq suboption:w

Object class	Permission	Domain	Type
msgq	create destroy enqueue setattr unix_write write	domain	type

Table 67: Option:shm suboption:r

Object class	Permission	Domain	Type
shm	associate getattr read unix_read	domain	type

Table 68: Option:shm suboption:w

Object class	Permission	Domain	Type
shm	create destroy lock setattr unix_write write	domain	type

Table 69: Option:pipe suboption:r

Object class	Permission	Domain	Type
fifo_file	getattr ioctl lock read	domain	type

Table 70: Option:pipe suboption:w

Object class	Permission	Domain	Type
fifo_file	append create execute link lock mounton quotaon relabelfrom relabelto rename setattr unlink write	domain	type

Table 71: Option:sig suboption:c

Object class	Permission	Domain	Type
process	sigchld	domain	type

Table 72: Option:sig suboption:k

Object class	Permission	Domain	Type
process	sigkill	domain	type

Table 73: Option:sig suboption:s

Object class	Permission	Domain	Type
process	sigstop	domain	type

Table 74: Option:sig suboption:n

Object class	Permission	Domain	Type
process	signull	domain	type

Table 75: Option:sig suboption:o

Object class	Permission	Domain	Type
process	signal	domain	type

3.7 Integrated permissions in allowpriv rule

Table 76: Option:audit_read

Object class	Permission	Domain	Type
netlink_audit_socket	nlmsg_read nlmsg_readpriv	domain	self

Table 77: Option:audit_write

Object class	Permission	Domain	Type
netlink_audit_socket	nlmsg_relay	domain	self

Table 78: Option:audit_adm

Object class	Permission	Domain	Type
netlink_audit_socket	nlmsg_write	domain	self

Table 79: Option:klog_read

Object class	Permission	Domain	Type
system	syslog_read	domain	kernel_t

Table 80: Option:klog_adm

Object class	Permission	Domain	Type
system	syslog_console syslog_mod	domain	kernel_t

Table 81: Option:cap_sys_pacct

Object class	Permission	Domain	Type
capability	sys_pacct	domain	self

Table 82: Option:cap_sys_module

Object class	Permission	Domain	Type
capability	sys_module	domain	self

Table 83: Option:netlink

Object class	Permission	Domain	Type
netlink_socket	accept append bind connect create getattr getopt ioctl listen lock name_bind read recv_msg recvfrom relabelfrom relabelto send_msg sendto setattr setopt shutdown write	domain	self
netlink_route_socket	accept append bind connect create getattr getopt ioctl listen lock name_bind nlmsg_read read recv_msg recvfrom relabelfrom relabelto send_msg sendto setattr setopt shutdown write	domain	self
netlink_firewall_socket	accept append bind connect create getattr getopt ioctl listen lock name_bind read	domain	self

Table 84: Option:relabel

Object class	Permission	Domain	Type
blk_file	relabelfrom	domain	file_type
chr_file	relabelto		fs_type
dir	setattr		
fifo_file			
file			
lnk_file			
sock_file			

Table 85: Option:part_relabel

Object class	Permission	Domain	Type
blk_file	relabelfrom	domain	writable_type
chr_file	relabelto		
dir			
fifo_file			
file			
lnk_file			
sock_file			
process	setfscreate	domain	self

Table 86: Option:getsecurity

Object class	Permission	Domain	Type
dir	getattr read search	domain	security_t
file	getattr read	domain	security_t
security	check_context compute_av compute_create compute_relabel compute_user	domain	security_t

Table 87: Option:setsecurity

Object class	Permission	Domain	Type
file	write	domain	security_t

Table 88: Option:setenforce

Object class	Permission	Domain	Type
security	setenforce	domain	security_t

Table 89: Option:setbool

Object class	Permission	Domain	Type
security	setbool	domain	security_t

Table 90: Option:load_policy

Object class	Permission	Domain	Type
security	load_policy	domain	security_t

Table 91: Option:getsecattr

Object class	Permission	Domain	Type
process	getattr	domain	global

Table 92: Option:setsecparam

Object class	Permission	Domain	Type
security	setsecparam	domain	security_t

Table 93: Option:devcreate,In addition, allow_file_devcrete is used in file write

Object class	Permission	Domain	Type
capability	mknod	domain	self
blk_file chr_file	create link rename unlink	domain	writable_type

Table 94: Option:search

Object class	Permission	Domain	Type
dir	getattr read search	domain	file_type
blk_file chr_file dir fifo_file file lnk_file sock_file	getattr	domain	file_type
lnk_file	read	domain	file_type

Table 95: Option:read

Object class	Permission	Domain	Type
blk_file chr_file dir fifo_file file lnk_file sock_file	getattr ioctl lock read	domain	file_type

Table 96: Option:write

Object class	Permission	Domain	Type
blk_file	append	domain	file_type
chr_file	create		
dir	link		
fifo_file	rename		
file	setattr		
lnk_file	unlink		
sock_file	write		
dir	reparent	domain	file_type
	rmdir		

Table 97: Option:cap_net_admin

Object class	Permission	Domain	Type
capability	net_admin	domain	self
netlink_route_socket	nlmsg_write	domain	self

Table 98: Option:cap_sys_boot

Object class	Permission	Domain	Type
capability	sys_boot	domain	self

Table 99: Option:cap_dac_override

Object class	Permission	Domain	Type
capability	dac_override	domain	self

Table 100: Option:cap_dac_read_search

Object class	Permission	Domain	Type
capability	dac_read_search	domain	self

Table 101: Option:cap_setuid

Object class	Permission	Domain	Type
capability	setuid	domain	self

Table 102: Option:cap_setgid

Object class	Permission	Domain	Type
capability	setgid	domain	self

Table 103: Option:cap_chown

Object class	Permission	Domain	Type
capability	chown	domain	self

Table 104: Option:cap_setpcap

Object class	Permission	Domain	Type
capability	setpcap	domain	self

Table 105: Option:cap_fowner

Object class	Permission	Domain	Type
capability	fowner	domain	self

Table 106: Option:cap_fsetid

Object class	Permission	Domain	Type
capability	fsetid	domain	self

Table 107: Option:cap_linux_immutable

Object class	Permission	Domain	Type
capability	linux_immutable	domain	self

Table 108: Option:quotaon

Object class	Permission	Domain	Type
file	quotaon	domain	file_type
filesystem	quotamod	domain	fs_type

Table 109: Option:mount

Object class	Permission	Domain	Type
dir	mounton	domain	file_type
filesystem	mount remount unmount	domain	fs_type

Table 110: Option:cap_sys_rawio

Object class	Permission	Domain	Type
capability	sys_rawio	domain	self

Table 111: Option:cap_sys_chroot

Object class	Permission	Domain	Type
capability	sys_chroot	domain	self

Table 112: Option:unlabel

Object class	Permission	Domain	Type
dir	add_name getattr ioctl lock read remove_name reparent rmdir search	domain	file_t unlabeled_t
blk_file chr_file dir fifo_file file lnk_file sock_file	append create getattr ioctl link lock read rename setattr unlink write	domain	file_t unlabeled_t
file	execute execute_no_trans	domain	file_t unlabeled_t

Table 113: Option:cap_ipc_lock

Object class	Permission	Domain	Type
capability	ipc_lock	domain	self

Table 114: Option:cap_sys_nice

Object class	Permission	Domain	Type
capability	sys_nice	domain	self

Table 115: Option:cap_sys_resource

Object class	Permission	Domain	Type
capability	sys_resource	domain	self

Table 116: Option:cap_sys_time

Object class	Permission	Domain	Type
capability	sys_time	domain	self

Table 117: Option:cap_sys_admin

Object class	Permission	Domain	Type
capability	sys_admin	domain	self

Table 118: Option:cap_sys_tty_config

Object class	Permission	Domain	Type
capability	sys_tty_config	domain	self

Table 119: Option:ptrace

Object class	Permission	Domain	Type
process	ptrace	domain	global

3.8 Integrated permissions for kernel key subsystem

Table 120: Option:v

Object class	Permission	Domain	Type
key	view	domain	type

Table 121: Option:r

Object class	Permission	Domain	Type
key	read	domain	type

Table 122: Option:w

Object class	Permission	Domain	Type
key	write	domain	type

Table 123: Option:s

Object class	Permission	Domain	Type
key	search	domain	type

Table 124: Option:l

Object class	Permission	Domain	Type
key	link	domain	type

Table 125: Option:t

Object class	Permission	Domain	Type
key	setattr	domain	type

Table 126: Option:c

Object class	Permission	Domain	Type
key	create	domain	type

3.9 Rules integrated in transition rule

Table 127: Option:Normal domain transition,This is allowed in domain_trans rule

Object class	Permission	Domain	Type
process	transition	from	to
file	entrypoint	to	entry
process	sigchld	to	from
fifo_file	append getattr ioctl lock read write	to	from

Table 128: Option:Dynamic domain transition,This is allowed in domain_trans rule when entry point is not specified.

Object class	Permission	Domain	Type
process	dyntransition	from	to
process	setcurrent	from	self

Table 129: Option:File type transition,This is allowed in allow exclusive rule

Object class	Permission	Domain	Type
dir	getattr ioctl lock read search write	from	entry