

NSA Security-Enhanced Linux (SELinux)

<http://www.nsa.gov/selinux>

Stephen D. Smalley

sds@tycho.nsa.gov

National Information Assurance Research Laboratory

National Security Agency

What is SELinux?

- Flexible Mandatory Access Control (MAC) for Linux.
- Configurable policy engine supporting:
 - Type Enforcement (TE), Role-Based Access Control (RBAC)
 - Optionally Multi-Level Security (MLS)
- Ability to enforce confidentiality and integrity guarantees.
- Ability to confine flawed and malicious applications.
- Ability to enforce assured pipelines.

SELinux: Key Properties

- Complete mediation
 - Control over all processes, objects, operations.
- Control based on all security-relevant information.
 - Properties of the actual process and object, not just its name.
- Configurable support for meeting application security requirements transparently.
 - Assured pipelines.
- Infrastructure for security-aware applications.
 - A secure system requires more than just a secure OS.

SELinux: Background

- Originated from NSA R&D.
- First public release by NSA in Dec 2000.
- Large and growing user and developer community.
- First packaged externally for Debian.
- Integrated into Hardened Gentoo.
- Integrated into mainline Linux 2.6 in Aug 2003.
- Included and enabled in Red Hat distributions.
 - Fedora Core 3, 4, and 5; Red Hat Enterprise Linux 4

Recent Advances in SELinux

- Improved integration with audit subsystem.
- Enhanced network packet labeling and control.
- Enhanced filesystem labeling support.
- Key management controls.
- Improved base policy.
- Loadable policy modules.
- Policy management infrastructure and tools.
- Improved and new policy development tools.

Improved Audit Integration

- Extended syscall audit records with security contexts.
- Enabled filtering based on security contexts.
- Added auditing of SELinux specific events.
- Enabled audit of netlink capability checks.
- Some parts included in Linux 2.6.17, further support added for 2.6.18.

Network Labeling: IPSEC/xfrm

- Implicit packet labeling via IPSEC/xfrm.
- Security context stored in xfrm policy rules and states.
- Authorize socket's use of policy based on context.
- Build SAs with context of policy.
- Included in Linux 2.6.16.
- TCP SO_PEERSEC support, UDP SCM_SECURITY support added in Linux 2.6.17.

Network Control: SECMARK

- Motivation: Existing SELinux network controls very limited in expressiveness and coverage.
- Solution: Separate labeling from enforcement.
 - Use iptables to select and label packets.
 - Use SELinux to enforce policy based on those labels.
- SECMARK and CONNSECMARK targets added.
- <http://james-morris.livejournal.com/11010.html>
- For 2.6.18.

Network Labeling: MLS enhancements

- Granular IPSEC associations
 - Allow a single xfrm policy rule to cover a MLS range.
 - Instantiate individual SAs for individual levels within the range.
- Flow labeling outside of socket context
 - Label based on origin when no socket involved (e.g. forward)
- Label socket IPSEC policy from socket.
- Label TCP child sockets from peer.
- In progress, see redhat-lspp and netdev lists.

Network Labeling: NetLabel

- Explicit packet labeling via IP option.
- Motivation: Compatibility with other trusted OSes.
 - Also avoids requiring use of IPSEC for labeling.
 - Also enables packet filtering based on the explicit labels.
- Presently limited to CIPSO, MLS labels.
- Code and info at http://free.linux.hp.com/~pmoore/projects/linux_cipso/

Filesystem Labeling

- Jffs2 xattr support (for 2.6.18)
- Improvements to mount context options (for 2.6.18)
- Atomic labeling of new files (2.6.14)
- VFS fallback for security xattrs (2.6.14)
- Canonicalization of getxattr results (2.6.15)

Key Management Controls

- Added security labeling of keys upon creation.
- Added basic permission checks on key operations.
- Added keycreate support to specify key labels.
- Randomized key serial number generation.
- Filtered /proc/keys output.
- For 2.6.18.

Reference Policy

- Improved base policy for SELinux, replaces old example policy.
- Strong modularity with explicit interfaces.
- Inline documentation.
- Ability to build policy variants from single source base.
- Deployed as the base policy in Fedora Core 5.
- <http://oss.tresys.com>

Loadable Policy Modules

- Ability to build and package policy modules separately.
- Avoids need for policy sources for local customizations.
- Enables third party policy and decomposition of distro policy.
- Initially deployed in Fedora Core 5.
- Ongoing work to migrate policy into individual packages for Fedora Core 6.

Policy Management

- Standard library for applications to use to manipulate policy (libsemanage).
- Designed to support multiple back-ends transparently.
 - Initial support for direct manipulation of policy store.
 - Work in progress for policy management server daemon.
- Used by policy management tools.
 - Semodule, semanage, setsebool

Policy Development Tools

- SLIDE, <http://oss.tresys.com>
 - Integrated Development Environment for policy
 - Eclipse plugin, integrates with reference policy
- SEEdit, <http://seedit.sourceforge.net>
 - Policy editor with simplified policy language, GUI
- Polgen, <http://www.mitre.org/tech/selinux>
 - Policy generation tool based on pattern recognition
- SETools, <http://www.tresys.com/selinux>
 - Policy analysis tools



Policy Expl...

- fhmod
- full
 - bin
 - doc
 - policy
 - modules
 - admin
 - apps
 - kernel
 - services
 - amavis
 - apache
 - apm**
 - arpwatch
 - asterisk
 - audioentropy
 - automount
 - avahi
 - bind
 - bluetooth
 - canna
 - cipe
 - clamav
 - comsat
 - courier

```
37
38#####
39#
40# apm client Local policy
41#
42
43allow apm_t self:capability { dac_override sys_admin };
44
45kernel_read_system_state(apm_t)
46
47dev_rw_apm_bios(apm_t)
48
49fs_getattr xattr fs(apm_t)
50
51term_use_all_terms(apm_t)
52
53domain_use_interactive_fds(apm_t)
54
55libs_use_ld_so(apm_t)
56libs_use_shared_libs(apm_t)
57libs_
58
59loggi
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100
101
102
103
104
105
106
107
108
109
110
111
112
113
114
115
116
117
118
119
120
121
122
123
124
125
126
127
128
129
130
131
132
133
134
135
136
137
138
139
140
141
142
143
144
145
146
147
148
149
150
151
152
153
154
155
156
157
158
159
160
161
162
163
164
165
166
167
168
169
170
171
172
173
174
175
176
177
178
179
180
181
182
183
184
185
186
187
188
189
190
191
192
193
194
195
196
197
198
199
200
201
202
203
204
205
206
207
208
209
210
211
212
213
214
215
216
217
218
219
220
221
222
223
224
225
226
227
228
229
230
231
232
233
234
235
236
237
238
239
240
241
242
243
244
245
246
247
248
249
250
251
252
253
254
255
256
257
258
259
260
261
262
263
264
265
266
267
268
269
270
271
272
273
274
275
276
277
278
279
280
281
282
283
284
285
286
287
288
289
290
291
292
293
294
295
296
297
298
299
300
301
302
303
304
305
306
307
308
309
310
311
312
313
314
315
316
317
318
319
320
321
322
323
324
325
326
327
328
329
330
331
332
333
334
335
336
337
338
339
340
341
342
343
344
345
346
347
348
349
350
351
352
353
354
355
356
357
358
359
360
361
362
363
364
365
366
367
368
369
370
371
372
373
374
375
376
377
378
379
380
381
382
383
384
385
386
387
388
389
390
391
392
393
394
395
396
397
398
399
400
401
402
403
404
405
406
407
408
409
410
411
412
413
414
415
416
417
418
419
420
421
422
423
424
425
426
427
428
429
430
431
432
433
434
435
436
437
438
439
440
441
442
443
444
445
446
447
448
449
450
451
452
453
454
455
456
457
458
459
460
461
462
463
464
465
466
467
468
469
470
471
472
473
474
475
476
477
478
479
480
481
482
483
484
485
486
487
488
489
490
491
492
493
494
495
496
497
498
499
500
501
502
503
504
505
506
507
508
509
510
511
512
513
514
515
516
517
518
519
520
521
522
523
524
525
526
527
528
529
530
531
532
533
534
535
536
537
538
539
540
541
542
543
544
545
546
547
548
549
550
551
552
553
554
555
556
557
558
559
560
561
562
563
564
565
566
567
568
569
570
571
572
573
574
575
576
577
578
579
580
581
582
583
584
585
586
587
588
589
590
591
592
593
594
595
596
597
598
599
600
601
602
603
604
605
606
607
608
609
610
611
612
613
614
615
616
617
618
619
620
621
622
623
624
625
626
627
628
629
630
631
632
633
634
635
636
637
638
639
640
641
642
643
644
645
646
647
648
649
650
651
652
653
654
655
656
657
658
659
660
661
662
663
664
665
666
667
668
669
670
671
672
673
674
675
676
677
678
679
680
681
682
683
684
685
686
687
688
689
690
691
692
693
694
695
696
697
698
699
700
701
702
703
704
705
706
707
708
709
710
711
712
713
714
715
716
717
718
719
720
721
722
723
724
725
726
727
728
729
730
731
732
733
734
735
736
737
738
739
740
741
742
743
744
745
746
747
748
749
750
751
752
753
754
755
756
757
758
759
760
761
762
763
764
765
766
767
768
769
770
771
772
773
774
775
776
777
778
779
780
781
782
783
784
785
786
787
788
789
790
791
792
793
794
795
796
797
798
799
800
801
802
803
804
805
806
807
808
809
810
811
812
813
814
815
816
817
818
819
820
821
822
823
824
825
826
827
828
829
830
831
832
833
834
835
836
837
838
839
840
841
842
843
844
845
846
847
848
849
850
851
852
853
854
855
856
857
858
859
860
861
862
863
864
865
866
867
868
869
870
871
872
873
874
875
876
877
878
879
880
881
882
883
884
885
886
887
888
889
890
891
892
893
894
895
896
897
898
899
900
901
902
903
904
905
906
907
908
909
910
911
912
913
914
915
916
917
918
919
920
921
922
923
924
925
926
927
928
929
930
931
932
933
934
935
936
937
938
939
940
941
942
943
944
945
946
947
948
949
950
951
952
953
954
955
956
957
958
959
960
961
962
963
964
965
966
967
968
969
970
971
972
973
974
975
976
977
978
979
980
981
982
983
984
985
986
987
988
989
990
991
992
993
994
995
996
997
998
999
1000
```

Interfaces

- admin (33)
- apps (28)
- kernel (12)
 - corecommands (43)
 - corenetwork (773)
 - corenet_dontaudit_tcp_bind_
 - corenet_dontaudit_tcp_bind_
 - corenet_dontaudit_tcp_bind_
 - corenet_dontaudit_tcp_conne
 - corenet_dontaudit_tcp_sendr
 - corenet_dontaudit_udp_bind_
 - corenet_non_ipsec_sendrecv
 - corenet_raw_bind_all_nodes
 - corenet_raw_receive_all_if
 - corenet_raw_receive_all_nod

Next Steps

- Securing the desktop
 - Reviving the XACE/XSELinux implementation, upstreaming it.
 - Labeled windowing.
 - Addressing other desktop infrastructure components.
 - Ensuring that user applications function properly in a secured environment.
- Improved useability
 - New troubleshooting tool
 - Continued improvements to policy tools

Next Steps (Cont)

- Policy Management
 - Completing the policy management server daemon and the libsemanage backend support.
 - Extending management to collections of SELinux hosts, including support for local variations and policy splitting.
 - Reconciling differences in policies between SELinux systems.
- Improvements to policy modules
 - Language support for interfaces
 - Integration with package management

Next Steps (Cont)

- Integration with SE-Xen
 - Flask architecture in Xen hypervisor.
 - Support for Xen object managers, like XenStore.
 - Policy management for Xen policy (shared toolchain).
 - Coordination with guest policies.
- NFS integration
 - Extending NFSv4 to support process and file security attributes.
 - Ensuring correct enforcement on client and server.

Credits

- HP (audit, MLS, NetLabel)
- IBM (audit, MLS, IPSEC labeling)
- MITRE (Polgen)
- NEC (SMP scalability, jffs2 xattr, embedded)
- Red Hat (audit, fs labeling, SECMARK, semanage)
- Tresys Technology (refpolicy, modules, semanage, policy server, SLIDE, SETools)
- Trusted Computer Solutions (audit, MLS, IPSEC labeling)
- And the entire SELinux community...

Resources

- SELinux News <http://selinuxnews.org>
- Sourceforge project <http://selinux.sourceforge.net>
- SELinux Symposium <http://selinux-symposium.org>
- NSA SELinux site <http://www.nsa.gov/selinux>
- Tresys Technology site <http://oss.tresys.com>

End of Presentation