White Paper

Raytheon
Trusted Computer Solutions

Security Enhanced Linux Multi-Level Security Performance Implications

Security will always be the primary concern for Multi-Level Security (MLS) solutions, but system performance cannot be ignored. Many Raytheon Trusted Computer Solutions (RTCS) customers inquire about system performance requirements as they embark on an MLS implementation. Performance can be a primary concern for both new application development and for porting existing applications. However, the performance impact of the additional security provided by MLS operating systems is not well documented, which leaves many questions unanswered. This paper examines the performance impact of Security Enhanced Linux® (SELinux) MLS on Red Hat® Enterprise Linux® 5.

July 2010

1. Introduction

Raytheon Trusted Computer Solutions is a recognized leader in cross domain solutions and custom high assurance products, with over a decade of experience providing secure software solutions and services to both Federal and commercial organizations. Most vendors in the information assurance space focus on architecting and implementing complex technical solutions to solve customers' needs and neglect to consider key business questions such as performance issues. The RTCS Professional Services team; however, focuses on delivering services across the full value chain of solving organizations' complex high assurance and cross domain business needs in order to increase our customers return on investment. The RTCS Professional Services approach takes into account that high assurance and cross domain solutions go beyond system development and configuration and typically involve strategy, process, organizational and architectural development threads as well as business integration with key software and technology configuration components.

RTCS operating system developers and professional services integrators work very closely with the open source community to enhance Red Hat Enterprise Linux 5 (with Security Enhanced Linux) so that it includes all of the necessary security controls and policies required by the cross domain and multi-level security community. The SecureOffice® Suite of products are a continuation of that effort and leverage the Red Hat Enterprise Linux operating system.

Throughout the years of developing, testing, and implementing MLS operating systems and cross domain solutions it became apparent that there was a lack of information on performance impacts that might result from adding in the additional complexities of security. The following paper demonstrates the performance differences between standard Red Hat Enterprise Linux 5 and a Red Hat Enterprise Linux 5 system with the SELinux controls and policies activated and provides related observations on security versus performance.

2. Test Components

The operating system used for all tests is the Common Criteria certified configuration of Red Hat Enterprise Linux 5 that meets the Labeled Security Protection Profile (LSPP). This bare-bones command-line-only MLS OS runs kernel version 2.6.18-8.1.3.lspp.81.el5, which is essentially an updated security-patched version of the stock Red Hat Enterprise Linux 5 Server kernel version 2.6.18-1.el5. The following tools were also employed in various tests: OpenSSL 0.98b, FBENCH 200709, Netperf 2.4.4-1, MPICH2 1.1, and MPPTEST 1.4b.

The 64-bit Red Hat Enterprise Linux 5 LSPP MLS computer used for all performance testing has two 1.8GHz dual-core AMD Opteron 265 processors, a Super Micro H8DAE motherboard, dual gigabit Ethernet, 2GB RAM, and a 3ware 6-drive SATA RAID. The 64-bit IBM x226 network client computer used for network performance testing has two 3GHz Intel Xeon processors, gigabit Ethernet, and 4GB RAM. The two computers were connected with either a crossover cable or a Dell 6224 network switch as noted in the individual test descriptions.

3. Test Performance Categories

All tests fall into three primary performance categories: calculation, storage, and networking. The calculation tests address memory, integer, binary, and floating point operations. The storage tests address file system, device driver, large block size, and small block size operations. The networking tests address maximum throughput and Message Passing Interface (MPI) operations.

4. Test Setup

The tests were run under three configurations: with SELinux completely disabled, SELinux MLS enforcing with unlabeled networking, and with SELinux MLS enforcing with CIPSO labeled networking as appropriate.

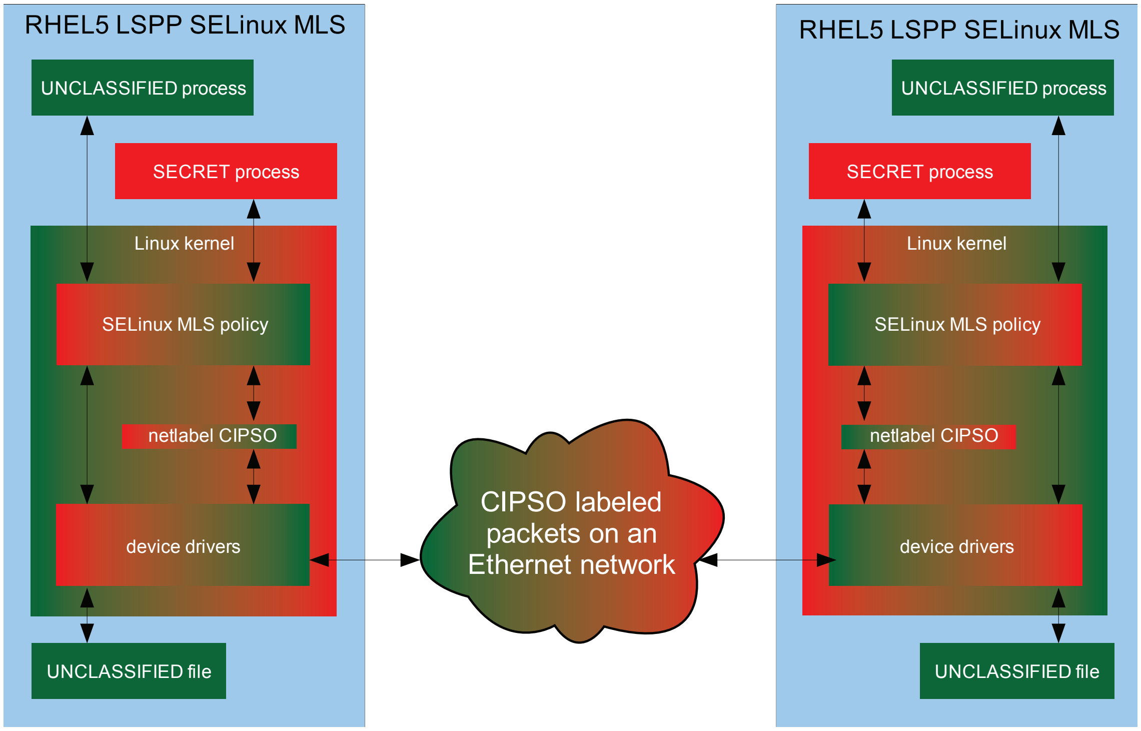

Figure 1: SELinux MLS Mandatory Access Control

Most tests ran as the `adminusr` account with the `staff_r` role at the `SystemLow` sensitivity label. If a test required root access, it ran as the `root` account with the `sysadm_r` role at the `SystemLow` sensitivity label.

5. Test Results

The test results reported are the average of three test runs.

The MLS sensitivity label used during testing had no impact on performance because the sensitivities of subjects (like processes) and objects (like files) are always compared by the kernel during access attempts, as shown in Figure 1.

There was little degradation in calculation, storage, or networking performance for most tests and the system performed better in some cases with the additional security. With SELinux MLS enforcing and CIPSO labeled networking, **the average relative calculation performance was -0.35%, the average relative storage performance was +0.87%, and the average relative networking performance was -3.1%** when compared to SELinux disabled.

There was significant degradation **(-48%)** when performing full-throttle localhost network testing, which **decreased from 5.9Gbps to 3.0Gbps** when run with SELinux MLS and CIPSO labeled networking compared to SELinux disabled and unlabeled networking. However, this upper limit on packet labeling and handling performance would only affect MLS router, storage, server, or management systems that have more than 3Gbps aggregate network connectivity and a need for that throughput. Increasing the underlying hardware performance can likely raise this limit significantly and additional gains may be available through kernel customizations.

6. Conclusion

In general, it is expected that an SELinux MLS system would perform **within 1%** of a conventional Linux system for calculations, **within 1%** for storage, and **within 4%** for networking if the workloads are distributed evenly as shown in these averaged test results. If the types of operations a system or application performs is known more accurately, a better performance estimate could be determined using the individual test performance numbers in Table 1, Figure 2, and Figure 3 rather than the category averages. For example, if your application does nothing but 1B/block I/O, you can expect around 8% degradation. If your MPI application is bound by communication speed, you may expect around 5% degradation.

The exact performance of SELinux MLS for your solution will obviously depend on your workload distribution, however, if you are not bound by absolute packet throughput, these results point to the fact that MLS performance should be within 5% to 10% of performance of a conventional Red Hat Enterprise Linux 5 Server with SELinux disabled. These conclusions are based on the worst-case individual test results.

category	test	units	selinux mls enforcing labeled networking	selinux mls enforcing unlabeled networking	selinux mls disabled unlabeled networking	relative performance of selinux mls in worst case	average category performance
calculation	openssl speed, average KB/s all algorithms	KB/s		87633.95	87717.74	-0.10%	-0.35%
	openssl speed, average operations/s RSA DSA	ops/s		6534.01	6651.98	-1.77%	
	time ./fbench 10000000	s		42.51	43.81	2.95%	
	time for ((x=0; $x<10; x=$x+1)); do ./ffbench; done	s		14.28	13.93	-2.49%	
storage	sync; sleep 5; echo 3 > /proc/sys/vm/drop_caches; sleep 5; time `find / > /dev/null`	s		15.85	17.33	8.52%	0.87%
	hdparm -t /dev/sda	MB/s		167.88	169.68	-1.06%	
	hdparm -T /dev/sda	MB/s		1381.8	1347.32	2.56%	
	dd bs=1M count=100 if=/dev/urandom of=/dev/shm/smallfile sync; sleep 5; echo 3 > /proc/sys/vm/drop_caches; sleep 5 time for((x=0;$x<100;x=$x+1));do dd bs=1M if=/dev/shm/smallfile of=/var/log/smallfile$x; done	s		82.35	84.5	2.55%	
	dd bs=1M count=100 if=/dev/urandom of=/dev/shm/smallfile sync; sleep 5; echo 3 > /proc/sys/vm/drop_caches; sleep 5 time for((x=0;$x<10;x=$x+1));do dd bs=1 if=/dev/shm/smallfile of=/var/log/smallfile$x; done	s		5917.98	5467.35	-8.24%	
networking	netperf -I 99,1 -i 50	megabits/s	3029.88	5668.39	5895.91	-48.61%	
	netperf -H 10.2.10.150 -I 99,1 -i 50 (crossover cable)	megabits/s	933.71	941.5	941.5	-0.83%	-3.10%
	netperf -H 10.2.10.150 -I 99,1 -i 50 (network switch)	megabits/s	740.19	745.54	745.54	-0.72%	
	mpdringtest 100000 (network switch)	s	31.52	30.71	29.48	-6.92%	
	./runmpptest -short -blocking -givedy -gnuplot -fname pt2pt-selinuxstate-labelstate.mpl (network switch)	avg %diff	-3.76%	-1.70%	baseline	-3.76%	
	./runmpptest -long -nonblocking -givedy -gnuplot -fname pt2ptnb-selinuxstate-labelstate.mpl (network switch)	avg %diff	-3.27%	-0.82%	baseline	-3.27%	

Table 1: Performance Test Results

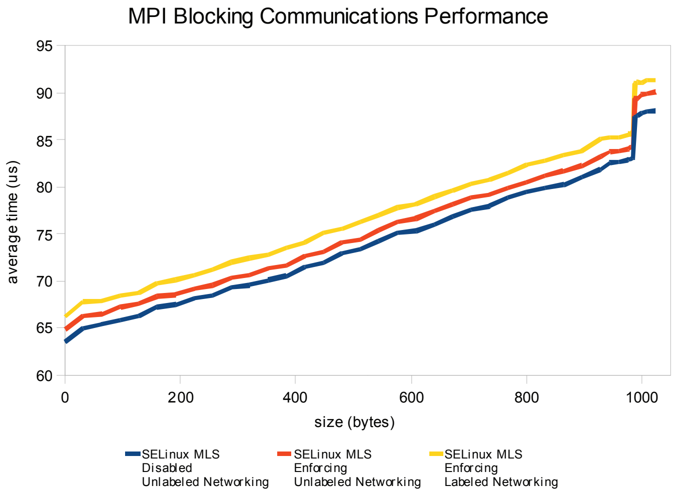

Figure 2: MPI Blocking Communications Perfomance

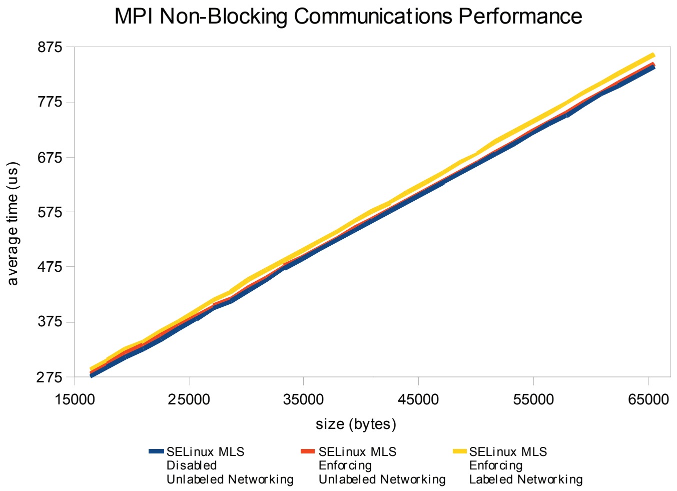

Figure 3: MPI Non-Blocking Communications Performance

References

Common Criteria certified configuration of Red Hat Enterprise Linux 5
http://www.commoncriteriaportal.org/

Labeled Security Protection Profile (LSPP)
http://www.commoncriteriaportal.org/files/epfiles/st_vid10165-st.pdf

Netperf
http://www.netperf.org/netperf/

FBENCH
http://www.fourmilab.ch/fbench/

MPICH2
http://www.mcs.anl.gov/research/projects/mpich2/

MPPTEST
http://www.mcs.anl.gov/research/projects/mpi/mpptest/

About the Author

Gregory Hildstrom is a Senior Secure Systems Engineer with Raytheon Trusted Computer Solutions, Inc (RTCS). He has over 4 years of industry experience in the information assurance field, with a specific focus on trusted operating system and cross domain solution requirements, analysis, development, and implementation. Mr. Hildstrom was the Principal Investigator for the US Navy's Multi-Level Data Storage Technology (MLDST) Small Business Innovative Research (SBIR) effort. He prototyped the integration of streaming video technology and Provision Networks' connection broker technology into the RTCS SecureOffice Trusted Thin Client product. Among his other duties, he has written certification and accreditation test procedures for the Red Hat Enterprise Linux 5 and Sun Solaris 10 Trusted Extensions multi-level secure operating systems. In addition, he has worked closely with customers to propose, develop, test, and deploy many other CDS projects. Prior to RTCS, he had an additional 5 years of industry experience in the high performance computing (HPC) field, with a specific focus on Linux clusters and data analysis.

ghildstrom@trustedcs.com

For further information contact:
Raytheon Trusted Computer Solutions
12950 Worldgate Drive, Suite 600
Herndon, VA 20170
866.230.1307
www.TrustedCS.com

Trusted Computer Solutions was acquired by Raytheon as a wholly owned subsidiary on 4 November 2010 under the name Raytheon Trusted Computer Solutions.

Cleared for public release. Reference #2011-115.

Printed in the U.S.A. WM 0311 200 300110.0710

Raytheon
Trusted Computer Solutions