

Certifying Linux on all IBM Platforms - Achievements, Roadmap & Experience

Doc Shankar

IBM Linux Technology Center, Austin

dshankar@us.ibm.com

Agenda

- CC Overview
- Achievements/Roadmap
- Challenges for CAPP/EAL4+
- Challenges for LSPP/EAL4+
- Open Sourcing Evaluation Material
- What's different about Open Source?
- Certification Valve
- Futures
- Summary

Common Criteria

- Multinational security evaluation criteria
- Defines seven Evaluation Assurance Levels EAL1-EAL7
- Mutual recognition up to EAL4
- CC defines functional and assurance requirements
- Protection Profiles
 - Predefined set of functional and assurance requirements
 - Controlled Access Protection Profile applies to DAC based access
 - Label Security Protection Profile applies to MAC based access
 - New profiles evolving
- Common Criteria certified products required for national security systems

Linux and Common Criteria

- Until 2003, many people believed that Linux would not be able to get CC certified
- Now, three years later, no other operating system has got more Common Criteria certificates than Linux®
 - Two distributions (Novell SUSE and Red Hat)
 - Two different kernel versions (2.4 and 2.6)
 - Many different hardware platforms
 - IBM® Pentium, XEON, and Opteron systems
 - IBM pSeries®, iSeries™, and zSeries® systems
 - HP Pentium, XEON, and Itanium systems
 - SGI Itanium systems
 - Two certifying agencies (BSI & NIAP)
 - Assurance levels up to EAL4 augmented by ALC_FLR.3

Evaluation Achievements/Roadmap

Product	Hardware	Kernel	PP	Assurance Level	Evaluator	Certifying Body	Application Date	Certification Date
SLES 8	xSeries® 335	2.4	ST	EAL 2+	atsec	BSI	02/03	08/03
SLES 8 SP3	xSeries 335, pSeries® 630, iSeries™ 825, zSeries® 900, eServer™ 325	2.4	CAPP	EAL3+	atsec	BSI	07/03	01/04
RHEL 3	Dell PowerEdge 6650 (AS) HP Proliant ML 570 (AS) Dell PowerEdge 2650 (ES) HP Proliant ML 570 (ES) Dell Precision 650 (WS) HP d350 (WS)	2.4	ST	EAL2+	Syntegra	CESG	02/03	02/04
RHEL3 UP2	xSeries 335 AS/WS, pSeries 630 AS iSeries 825 AS, zSeries 990 AS, eServer 325 AS	2.4	CAPP	EAL3+	atsec	BSI	03/04	07/04
SLES 8 SP3	Range of HP Pentium, Xeon and Itanium based systems	2.4	CAPP	EAL3+	atsec	BSI	04/04	09/04
RHEL 3 UP3	Range of HP Pentium, Xeon and Itanium based systems	2.4	CAPP	EAL3+	atsec	BSI	04/04	09/04
SLES 9 SP2	SGI Altix 350 SGI Altix 3700	2.6	CAPP	EAL3+	atsec	BSI	10/04	10/05
RHEL 3	Unisys ES7000	2.4	CAPP	EAL3+	SAIC	NIAP	12/04	
RHEL 4	Unisys ES7000	2.4	CAPP	EAL4+	SAIC	NIAP	12/04	
SLES 8 SP3	xSeries 345, 365, 445 & eServer 326	2.4	CAPP	EAL3+	atsec	BSI	07/05	09/05
RHEL 4 UP2	Range of HP Pentium, Xeon and Itanium based systems	2.4	CAPP	EAL3+	atsec	NIAP	10/05	

Evaluation Achievements/Roadmap

Product	Hardware	Kernel	PP	Assurance Level	Evaluator	Certifying Body	Application Date	Certification Date
SLES 9	xSeries model x335 machine type 8676 pSeries model 520 machine type 9111 (LPAR SF220_049) iSeries model 520 machine type (9406) (OS/400® V5R3 LPAR) zSeries 990, eServer 325	2.6	CAPP	EAL4+	atsec	BSI	03/04	03/05
RHEL4 UP1	xSeries model x336 machine type 8837 (AS/WS) pSeries model 550 machine type 9124 with pSeries LPAR (AS only) iSeries model 550 machine type 9406 with OS/400 v5R3 LPAR (AS only) zSeries z/VM 5.1 Logical Partition (AS only) eServer model 326 based on the AMD 64 (Opteron) processor machine type 8848 (AS only)	2.6	CAPP	EAL4+	atsec	NIAP	02/05	02/06
RHEL5	xSeries model x346 machine type xxxx & model HS20 Blade (AS/WS) zSeries z/VM 5.1 Logical Partition – includes z800, z890, z990, z9 (AS only) eServer model 327 based on the AMD 64 (Opteron) processor machine type xxxx & model LS 20 Blade (AS only)	2.6	CAPP LSPP RBAC	EAL4+	atsec	NIAP	09/05	03/07

Parties involved in the evaluations (Sponsored by IBM)

- IBM:
 - Sponsor the project, project management, and coordination
 - Codevelop the audit subsystem
 - Develop design documentation (FS, HLD, LLD)
 - Develop test cases and test plan
 - Conduct developer testing
 - Document development/security procedures (i.e. Configuration Management for test suites, document control, and test results)
 - Produce Vulnerability Assessment Report
- Distributors – SUSE & Red Hat:
 - Codevelop the audit subsystem
 - Update development and security procedures documentation
- atsec:
 - Codevelop the evaluation strategy
 - Provide guidance documents and a configuration script
 - Perform the evaluation
- Certifying Bodies - BSI & NIAP:
 - Supervise the evaluation and issue the certificate

Challenges for CAPP/EAL4

- New functionality
 - Now kernel version 2.6 (was 2.4 in the previous evaluations)
 - New design of the kernel audit functions
- Low-level design
 - Required for the kernel and all trusted processes
 - Large documents focusing on the security functions
 - Describing the details of the 2.6 kernel and trusted processes
- Additional vulnerability analysis
 - More in-depth analysis
 - Penetration testing
 - Crypto/Keygen/RNG/Primality tests
- Impacts on the distro development processes
 - Enhancements in flaw remediation
 - Acceptance procedures

Reuse from Previous Evaluations

- Security Target mainly re-used from CAPP/EAL3+
- High level design required only minor changes:
 - Impact of changes made from 2.4 kernel to 2.6 kernel
 - New kernel part of audit subsystem
- Functional specification partly re-used (required some changes):
 - New and modified system calls
 - Complete parameter description of system calls (not just libc wrapper functions)
- Testing mostly reused:
 - Required some changes and some additional tests
- distro processes did not change significantly:
 - Most documents could be re-used

Security Target

- TOE: SLES 9 & RHEL 4 UP1 with fixes and additional functions (audit, self-test)
- Security Functions selected for server system:
 - Password based Identification and Authentication using PAM Framework
 - Discretionary Access Control using the POSIX ACLs for the ext3 file system (permission bits for other file systems).
 - Discretionary Access Control for Inter-Process Communication (including access control for sockets).
 - Configurable audit for security relevant actions.
 - VSFTP, Stunnel, and SSH as the only trusted network applications
 - Trusted processes for security management.
 - Focusing on the ability of the kernel to protect itself.
- Assurance level achieved is higher than required by CAPP:
 - EAL 4 augmented by ALC_FLR.3 (CAPP requires only EAL 3)

Problems Identified

- Several security flaws have been identified by the evaluation team during the evaluation and have been fixed.
- Other security flaws identified by the Open Source Community during the time of the evaluation also have been fixed.
 - Race Conditions
 - Memory Leaks
 - Overflows
 - Parameter Validation
 - Kernel Hangs
 - Missing DAC Checks

Towards LSPP Compliance

- A true open source effort - challenging
- IBM sponsors a weekly teleconference
 - 40 participants from 9 organizations on the invitation
 - IBM, Red Hat, NSA, @sec, HP, TCS, Tresys, OSDL, and PSU + various individuals
 - All development takes place on open mailing lists
- Development goes upstream and is collected in rawhide
 - Fedora Rawhide provides daily builds for xSeries and pSeries.
 - Red Hat hosts test kernels for features pending kernel maintainer acceptance.
- Schedule
 - In Evaluation (09/05)
 - Development Complete (03/06)
 - Certification Complete (03/07)

Towards LSPP Compliance (Contd.)

- Major Enhancements
 - Kernel
 - SELinux MLS Support
 - IPsec labelled networking
 - Audit augmentation
 - VFS polyinstantiation
 - User Space
 - MLS Policy using reference policy
 - Enhanced user management
 - Audit filtering
 - Browsing augmentation
 - Device allocation
 - Labelled print
 - Multilevel network services
 - Multilevel cron

Towards LSPP Compliance (Contd.)

- Work remaining
 - Complete MLS development
 - Get it upstream
 - Ensure MLS work is incorporated into RHEL5
 - Augment exiting test suite
 - Enhance design documentation
 - Functional Specification
 - High Level Design
 - Low Level Design
 - Run tests and produce documentation
 - Undergo evaluation by lab.
 - Obtain certificate from NIAP
 - Open source documentation

Evaluation evidence open sourced

- Functional Specification*
 - Man pages existed, but not for all system calls and configuration files.
 - Additional man pages have been developed.
- High Level Design*
 - Very good general material and books exists, but partly not up-to-date and not focused on security
 - a new security focused High Level Design has been developed
- User Documentation*
 - Some very good security related documents and books exist, but they are generic and not dedicated to a specific distribution.
 - An additional Security Guide has been developed.
- Test Documentation**
 - Test cases for security functions didn't exist, so a comprehensive set of tests were developed for each assurance level.

Linux® now has a good starting point for further evaluations, and for the evaluation of other distributions.

* <http://www-128.ibm.com/developerworks/linux/library/os-ltc-security/>

** <http://ltp.sourceforge.net/EAL3.html>

What's different about open source ?

- Sponsor vs Vendor
 - IBM & distros
 - Less control
 - Process IP
- Multiple Platforms
 - Across all IBM eServers including opetron
 - VM, LPAR
 - Blades, Clusters,...
- Open Source Community
 - Acceptance (OLS paper, OLS BOF)
 - Changes into standard kernel (Audit, MAC)
- Open sourced evidence material
 - FS, HLD, User Docs, Security Guide, Test cases
- Site Visit/Site Security

What's different about open source ?

- Design Documentation
 - Available in public domain with varying detail
 - Functional Specs. used man pages as a basis
 - HLD/LLD referred to public documentation – e.g. Linux VMM book (Mel Gorman)
 - Use of scripts
 - Reading a document with numerous links is cumbersome
 - Collate relevant pieces into a common html format
 - Evaluator executes a script & then uses a browser
- Vulnerability Analysis
 - Vulnerability descriptions in public domain, e.g. <http://www.novell.com/linux/security/advisories/>
 - Task was simpler
- Evidence Reuse
 - SUSE/RH
 - HP
 - SGI
 - Unisys
- Distro Release/Schedule – alignment of priorities
- Open Question - How long do we want to sponsor?

Certification Value

- Business Value
 - 3rd party trust
 - Competition
 - Mandatory for DoD market
 - Other government agencies to follow
 - Reuse of evaluation material
 - Towards high assurance/robust Linux
- Technical Value
 - Audit capability
 - MLS capability
 - Hardware testing utility
 - Inline with the “many eyes” philosophy
 - Several security flaws identified

Futures

- LSPP Compliance (in progress)
- MLOSPP Compliance
- EAL5 Linux
- HA Linux (EAL7) – Separation kernels
- Integration with other Linux security projects—eCryptfs, TPM
- Integration with middleware
- More security functions as part of the TSF:
 - Additional authentication methods
 - Directory integration
 - VPN functions
 - Linux for desktop systems
- User space policy management server
- Policy development framework
- Enhancing the security of existing functions:
 - SAMBA
 - Trusted X-Windows
 - NFS®

Summary

- First Linux evaluation at EAL2+ performed in less than six months!
 - Started in February and finished in June of 2003.
- Evaluation at EAL3+ with CAPP compliance achieved in less than one year!
 - Including the development of a new auditing subsystem.
- Evaluation at EAL4+ with CAPP compliance achieved one year later.
 - This was based on the latest version of the kernel.
- Total of 10 Linux evaluations; 4 in progress
- First operating system evaluated on a variety of hardware platforms!
- Open Sourced Evaluation Evidence – has been reused
- Working towards LSPP compliance

Conclusion

- Linux has much to offer in terms of security
- Linux has a bright future ahead
- IBM is committed to elevating Linux as a **secure operating system of choice** in today's business environment

Legal Statement

This work represents the view of the authors and does not necessarily represent the view of IBM.

SUSE and its logo are registered trademarks of Novell.

IBM, IBM logo, AIX, AS/400, eServer, xSeries, iSeries, pSeries, zSeries, are registered trademarks of International Business Machines Corporation in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the US, other countries or both.

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Other company, product, and service names may be trademarks or service marks of others.