Common Criteria Evaluation Challenges for SELinux

Doc Shankar
IBM Linux Technology Center
dshankar@us.ibm.com

Agenda

- Common Criteria
- Roadmap/Achievements
- CAPP/LSPP Overview
- EAL4 Overview
- Open Sourcing Evaluation Material
- LSPP Compliant SELinux

Common Criteria

- Multinational security evaluation criteria
- Defines seven Evaluation Assurance Levels EAL1-EAL7
- Mutual recognition up to EAL4
- Common Criteria 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

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
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 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	02/05 (E)
RHEL4 UP1	TBD	2.6	CAPP	EAL4+	atsec	NIAP	02/05	TBD

Parties Involved in the Evaluation

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

CAPP Overview

- CAPP is based on C2 class of the “Department of Defense Trusted Computer Systems Evaluation Criteria” (DoD 5200.28) colloquially known as the “Orange Book”
- CAPP requires the OS implement DAC
- Five Categories of Functional Requirements:
  - Security Audit
  - User Data Protection
  - Identification & Authentication
  - Security Management
  - Protection of the TSF
- Requires EAL3

LSPP Overview

- LSPP is based on B1 class of the “Department of Defense Trusted Computer Systems Evaluation Criteria” (DoD 5200.28) colloquially known as the “Orange Book”
- LSPP requires the OS implement MAC
- Five Categories of Functional Requirements:
  - Security Audit (includes labeling, import/export of data)
  - User Data Protection (includes MAC/MLS)
  - Identification & Authentication (includes Security Levels)
  - Security Management (includes MAC policy controls)
  - Protection of the TSF (very similar to CAPP)
- Requires EAL3 augmented by ADV_SPM.1

MLOSPP Overview

- MLOSPP is based on “B2” class of the “Department of Defense Trusted Computer Systems Evaluation Criteria” (DoD 5200.28) colloquially known as the “Orange Book”
- MLOSPP requires the OS implement MAC, MIC & Crypto
- Nine Categories of Functional Requirements:
  - Security Audit (includes MAC, MIC, import/export of data)
  - Cryptographic Support (FIPS 140-2+)
  - User Data Protection (includes MAC/MIC/MLS)
  - Identification & Authentication (includes Security & Integrity Levels)
  - Security Management (includes MAC & MIC policy controls)
  - Protection of the TSF (includes TOE data transfer, Replay, Recovery, etc.)
  - Resource Utilization (Quotas for Disk, Memory & Processor)
  - TOE Access (Location, Concurrent sessions, Session Locking, etc.)
  - Trusted Path (Secure Attention key)
- Requires EAL4+ (four EAL5 & one EAL6 requirement)
- Unclear if commercial development can achieve this

EAL4 Overview

- Configuration Management:
  - **Automation: authorization controls, TOE generation, CM tools**
  - Capability: defined configuration, management procedures, **acceptance plan**
  - Scope: source code, design docs, user docs, test docs, Configuration Management docs, **security flaws**
- Delivery & Operations:
  - Delivery: secure delivery documents, **modification detection, detect developer masquerade**
  - Operations: secure installation, generation, and start-up procedures
- Development:
  - Functional Specification: describe each interface with complete details and all effects and exceptions, **TSF completeness in spec.**
  - High Level Design: TSF structure and subsystems, subsystem interface definitions, separation of TSP enforcing, and non-TSP
  - **Low Level Design: interface description and purpose of each TSF module**
  - Representation Correspondence: ST -> FS -> HLD -> **LLD -> IMP**
  - **Security Policy: Informal TSP model, correspondence between TSP model and Functional spec.**

Note - Highlighted items are EAL4 specific

EAL4 Overview

- Guidance Documents:
  - Administrator: Admin Guide (functions and interface available)
  - User: User Guide (functions and interface available)
- Life Cycle Support:
  - Development Security: Protect Confidentiality & Integrity of the TOE design and implementation
  - Flaw Remediation: Track and correct security flaws in a timely manner
  - **Life Cycle Definition: Life cycle model for development and maintenance of TOE**
  - **Tools: Identify and document all tools used**
- Testing:
  - Coverage: Demonstrate test coverage between TSF functional spec. and the identified tests
  - **Depth: Show identified tests can demonstrate TSF operations in accordance with the HLD**
  - Functional: test plans, procedures, cases and results
  - Independent: evaluator testing
- Vulnerability Assessment:
  - Misuse: examine guidance documentation for insecure states, **demonstrate completeness of guidance documentation**
  - Strength of Function: strength analysis of probabilistic security mechanisms
  - Vulnerability Analysis: show all identified vulnerabilities cannot be exploited in the TOE environment; **penetration attacks with low attack potential**

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-124.ibm.com/linux/pubs/?topic_id=5

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

LSPP/SELinux Development

- Audit:
  - Sensitivity Labels:
    - Include sensitivity labels of subjects and objects in the audit record
    - This includes audit records generated by trusted processes (e.g. login)
  - Additional Audit Records:
    - All attempts to export and import information
    - All attempts to change labels on I/O devices, FS objects, etc.
    - All decisions on requests of information flow
  - Label Handling:
    - Include labels on all audit information
    - Selectable audit review based on labels
    - Generation of audit records based on labels
- Identification & Authentication:
  - User Definition & Subject Binding:
    - Include user clearance (change login prompt to specify level of session)
    - Include sensitivity label in subject to enforce MAC
  - No Change (Strength of Authentication data, Protected Authentication feedback)

LSPP/SELinux Development

- User Data Protection:
  - Export Control:
    - Single level devices - MAC enforcement on implicit label of the device, e.g. Single level printer
    - Multi-level devices - MAC enforcement on explicit labels of exported objects, e.g. Multilevel printer
  - Import Control:
    - Single level devices - MAC enforcement on implicit label of the device
    - Multi-level devices - MAC enforcement on explicit label of imported objects
  - MAC Policy/Enforcement:
    - SS property
    - * property
  - No Change from CAPP (DAC, Object Reuse)
- Security Management
  - Label Management:
    - Enforce MAC for modifying object sensitivity labels
  - Object Creation:
    - Enforce MAC on new objects (level same as the creating process)
  - Revocation/Modification of security attributes:
    - Enforce MAC
  - No Change (Management of audit trail, events, user attributes & authentication data)
- Protection of TSF:
  - No Change (Abstract Machine testing, Reference Mediation, Domain Separation, Time Stamp)

LSPP/SELinux Assurance

- Site Visit
- Security Guide (including SELinux functions)
- SELinux API documentation
- Description of SELinux security critical configuration files
- SELinux HLD (including SELinux utilities)
- SELinux LLD (significant work)
- Representation correspondence for some part of SELinux
- Development security, LC model, flaw remediation
- Document all tools used by SELinux
- Develop all SELinux EAL4+ test cases (significant work)
- SElinux vulnerability analysis
- Policy verification:
  - Show policy complies with LSPP
  - Show implementation correctness
  - Perform vulnerability analysis (no covert channel analysis)

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.

Red Hat and its logo are registered trademarks of Red Hat, Inc.

IBM, IBM logo, 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.

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