Trusted Linux – It's not an Oxymoron!

Doc Shankar
IBM Federal Strategy/Architecture
dshankar@us.ibm.com

Agenda

- Part I – Why trust Linux?
  - Common Criteria
  - Roadmap/Achievements
  - Open Sourcing Evaluation material
  - What's different about open source?
  - Certification value
  - Open source security Initiatives
- Part II – Why trusted Linux?
  - What is SELinux?
  - What is trusted Linux?
  - What are the trusted Linux enhancements?
  - Why trusted Linux?

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

Why should you trust Linux ?

- 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 CC 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	01/07
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	06/06

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	06/07

IBM Sponsored Evaluation Partners

- **IBM:**
  - Sponsor the project, project management, and coordination
  - Codevelop the audit & MLS subsystems
  - 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:**
  - Codevelop the audit & MLS subsystems
  - 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

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 Architectures
  - VM, LPAR
  - Blades, Clusters,…
- Open Source Community
  - Up Streaming (e.g. Audit, MAC)
  - Acceptance (OLS Paper/BOF)
- Open sourced evidence material
- Site Visit/Site Security - multiple sites
- Design Documentation
  - FS used man pages
  - HLD/LLD referred to public documentation
- Vulnerability Analysis
  - Vulnerability descriptions in public domain
  - Task somewhat 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

Open Source Linux Security Initiatives

- Security Certification*
  - Common Criteria
  - EAL2+ achieved*
  - CAPP/EAL3+ achieved*
  - CAPP/EAL4+ achieved*
  - Working LSPP/EAL4+*
- Crypto*
  - OpenCryptoki*
  - HW crypto acceleration*
  - FIPS 140-2**
- Trusted Computing*
  - TCG's TPM/TSS Implementation*
- Networking Security**
  - OpenSSL**
  - OpenSSH
  - IPSec**
- Base Security**
  - LSM**
  - Audit *
  - Kerberos
  - PKI
- Applications Security**
  - Encrypted File System*
  - Firewall
  - Antivirus
  - IDS**
  - Security Scanners
  - Position Independent Executables
  - Exec Shield
- Mandatory Security**
  - SELinux**
  - MLS**
- Secure Configuration**
  - Bastille**
- Vulnerability reduction/reporting**
- Secure Programming**
  - BogoSec
- Verification Tools*
  - Vali*
  - Gokyo*
  - UT tool**

*** IBM Leading** **** IBM Participating**

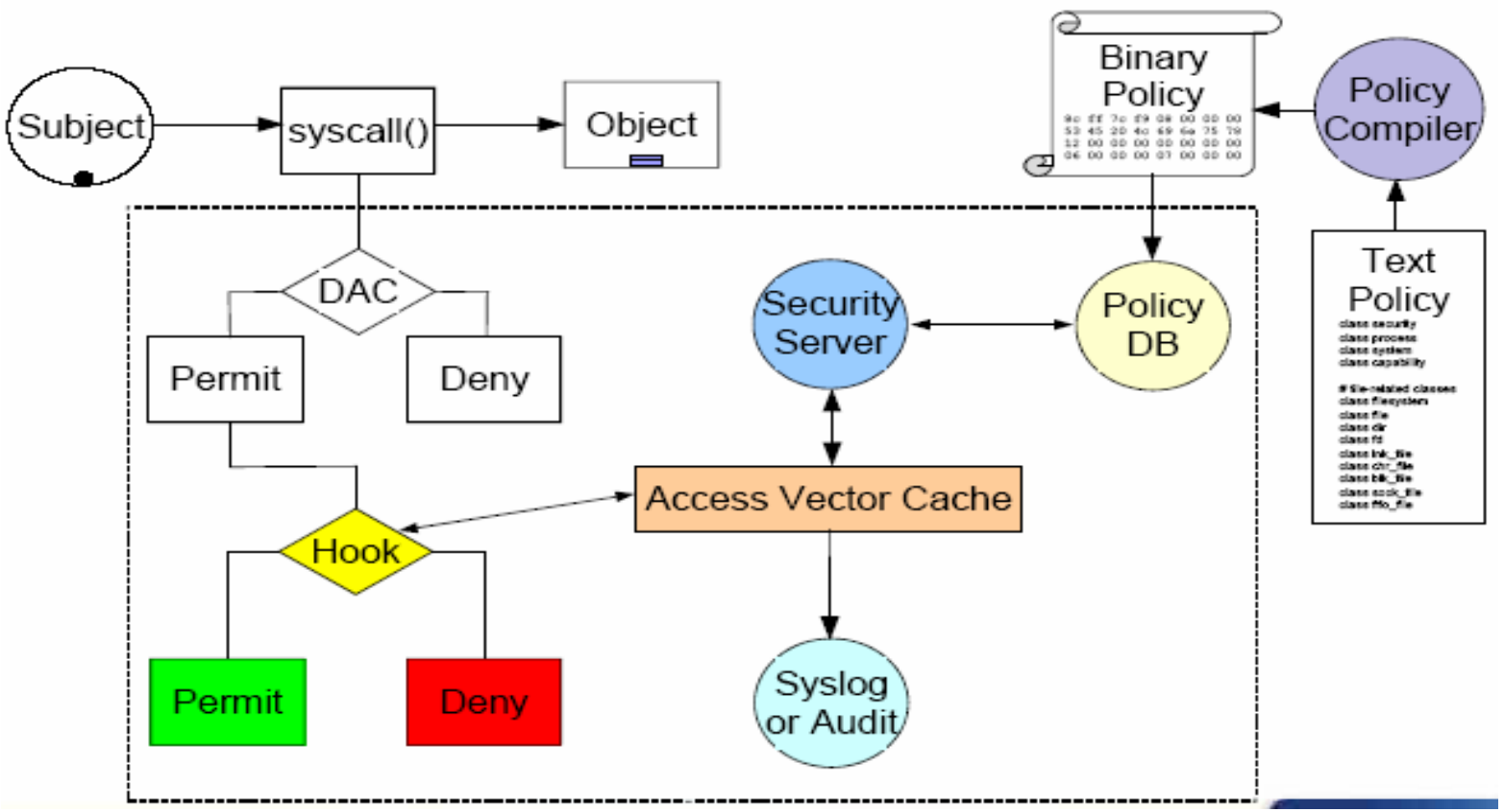
Summary

- 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 12 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

What is SELinux?

- Originally a huge kernel patch, which Linus disliked.
- Led to creation of Linux Security Module (LSM) architecture.
- Implemented as a set of LSM hooks.
- Separates policy from implementation.
- Flexible TE policy language is excruciatingly granular.
- Orthogonal to DAC; non-authoritative-can only deny.
- RBAC—roles aggregate types a user can take on.
- MLS implemented as an additional constraint on the TE policy

SELinux Operation



What is Trusted Linux?

- Additional access controls on top of Standard Linux (DAC)
  - MAC capability
    - TE
    - MLS
  - CAPP Compliance
  - LSPP Compliance
  - RBACPP Compliance
  - Assurance

LSPP Community

- A true open source effort - challenging
- IBM sponsors a weekly teleconference (open telecon)
  - 60+ participants from 14+ 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
  - Red Hat hosts test kernels for features pending kernel maintainer acceptance
- Real users provide feedback during development
- Schedule
  - In Evaluation (09/05)
  - Development Complete (03/07)
  - Certification Complete (06/07)

LSPP Overview

- LSPP is based on B1 class of the “Department of Defense Trusted Computer Systems Evaluation Criteria” (DoD 5200.28) coloquially known as the “Orange Book”
- LSPP requires the OS implement MAC
- 5 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

LSPP Enhancements

- Base SELinux Enhancements: Augmentation and test of MLS mode, user and role management utilities
- MLS Policy
- Labeled Networking
- MLS-Aware Network Services: racoon SA management; xinetd labeled networking, ssh role/level selection
- Labeled Print
- Polyinstiantiation (Multi-Level Directory) support for MLS
- Label Translation Daemon
- Multi-level Cron
- Labels in Audit Records
- Additional Audit Events & Audit Filtering on Labels

Business Reasons

- Available in main stream OS (e.g. RHEL5)
- All modifications up streamed
  - Accepted by open source community
- NSA prototyped SELinux & open sourced
- NSA participated in complete design and implementation
- Easily available skills
- CC Evaluation – Single cert covers 7 platforms
- Solution stack available
  - e.g. TCS thin client, guards, web shield,…
- Open source advantages
  - Revalidation of open source methodology
  - Patch speed
- Hardware Agnostic (runs on intel, opteron, power, blades, main frame,….)
- Avoids one vendor lock in
- Accredited Solutions – TSABI obtained by USCG; SABI in works
- Lower Cost
  - Proprietary hardware is more expensive than intel
  - COTS software (support cost only)
- Scalability – up, down & out

Technical Reasons

- Flexible MAC architecture (Flask)
  - LSM framework
  - TE comes along with MLS
- Restrictive security
  - DAC (Standard Linux) + TE (SELinux) + MLS (Trusted Linux)
- Supports labeled networking (IPSec, CIPSO)
- Policy development tools (e.g. Brickwall)
- Definable policy – Enforced by Security Server
- Reference policy
  - Modular framework
- Support for policy modules
- Policy choices
  - Targeted Policy
  - Strict policy
- Application object managers
- EAL4+ Assurance
- Deployment (UK Government)
- Vendor Enhancements
  - Trusted X
  - Government Label Translations (MITRE)

Conclusions

- Key Points to avoid risk and lock in
  - COTS hardware
  - COTS software
  - Hardware platform agnostic
  - Open standards
  - Open source
  - Evaluated
  - Accredited
  - Lower support costs
- IBM is committed to providing MLS & cross domain solutions on Linux