

Mission: ~~IM~~POSSIBLE

Security Certification of Linux!



Diane R Brent, PMP

drbrent@us.ibm.com

IBM Linux Technology
Center
Poughkeepsie, NY

Agenda

- **Common Criteria**
- **Project Objectives**
- **Challenges**
- **Approach**
- **Creating the Roadmap**
- **Scope of Linux Certification**
- **What we had, what was missing**
- **Lessons Learned**
- **Community Value**
- **Beyond EAL2+**
- **IBM's Commitment to Certification**

Common Criteria?

What is it?

The Common Criteria for Information Technology Security Evaluation (CC) is an international specification used to evaluate IT security. World Wide Government and Financial agencies are most likely to employ this and some require it for procurements.

What's involved?

Function – security capabilities

Assurance – confidence in capabilities

3rd Party evaluation

Project Objectives

- **Prove Linux CAN be certified**
- **Allay concerns that Linux isn't ready for Enterprise computing**
- **Satisfy Federal Gov't mandates**
- **Contribute back to community**
- **Do it ASAP!**

Challenges

- Evaluation criteria rooted in *closed source* model
- Development process *unlike* proprietary products
- Ownership of Linux
- Lack of *typical* internal product documentation
- “Show me the money!”

CERTIFICATION

Approach

- **Cooperative Effort**

- IBM not a Linux distributor

- **Schedule Acceleration**

- Leverage AIX certification experience

- Pooling Resources

- Augment distributor team with IBM development and test

- Financial sponsorship

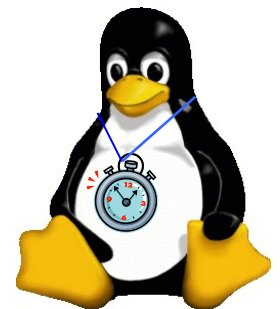
- Engaging *motivated* evaluation laboratory

- Lead open source operating system certification!

- **“Don’t bite off more than you can chew!”**

- Uncharted territory calls for step-wise plan

- Build upon experience



Creating the Roadmap

Where's the Competition?

CAPP/EAL4 is most prevalent for general purpose operating systems: AIX, Solaris, HP-UX, Windows 2000

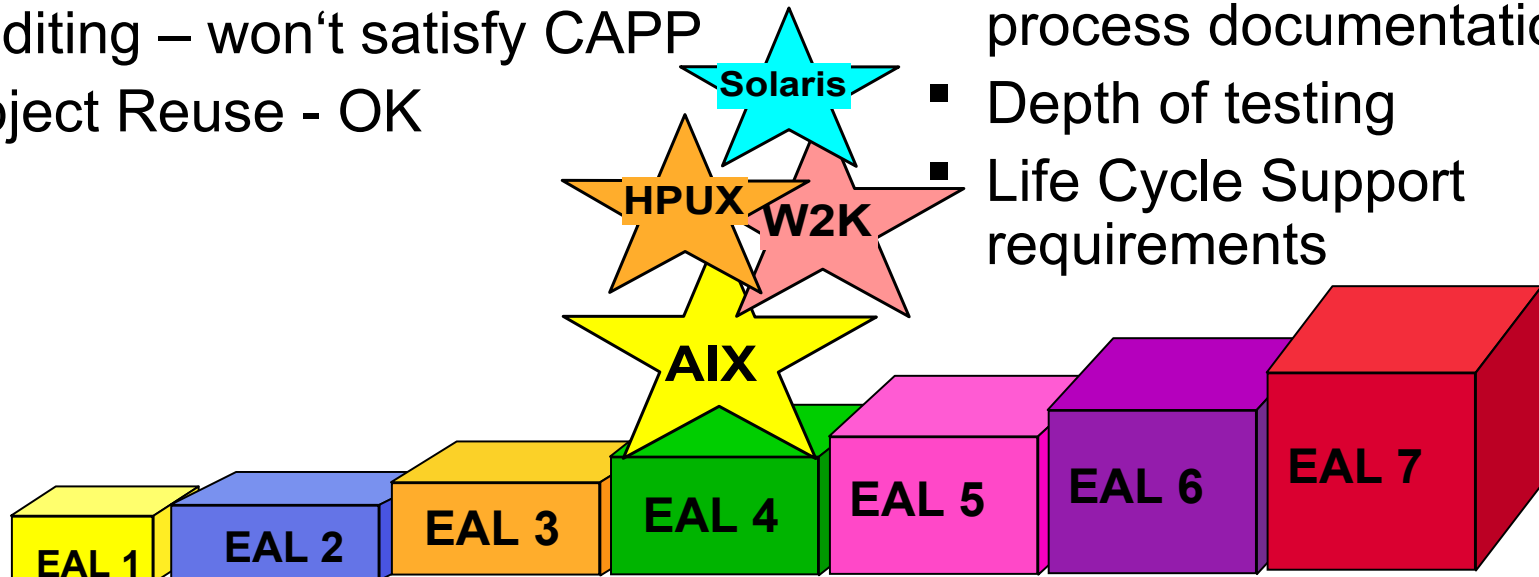
How does Linux compare?

Functional Criteria – close

- Authentication via PAM
- Authorization via ACLs
- Auditing – won't satisfy CAPP
- Object Reuse - OK

Assurance Criteria – much to do

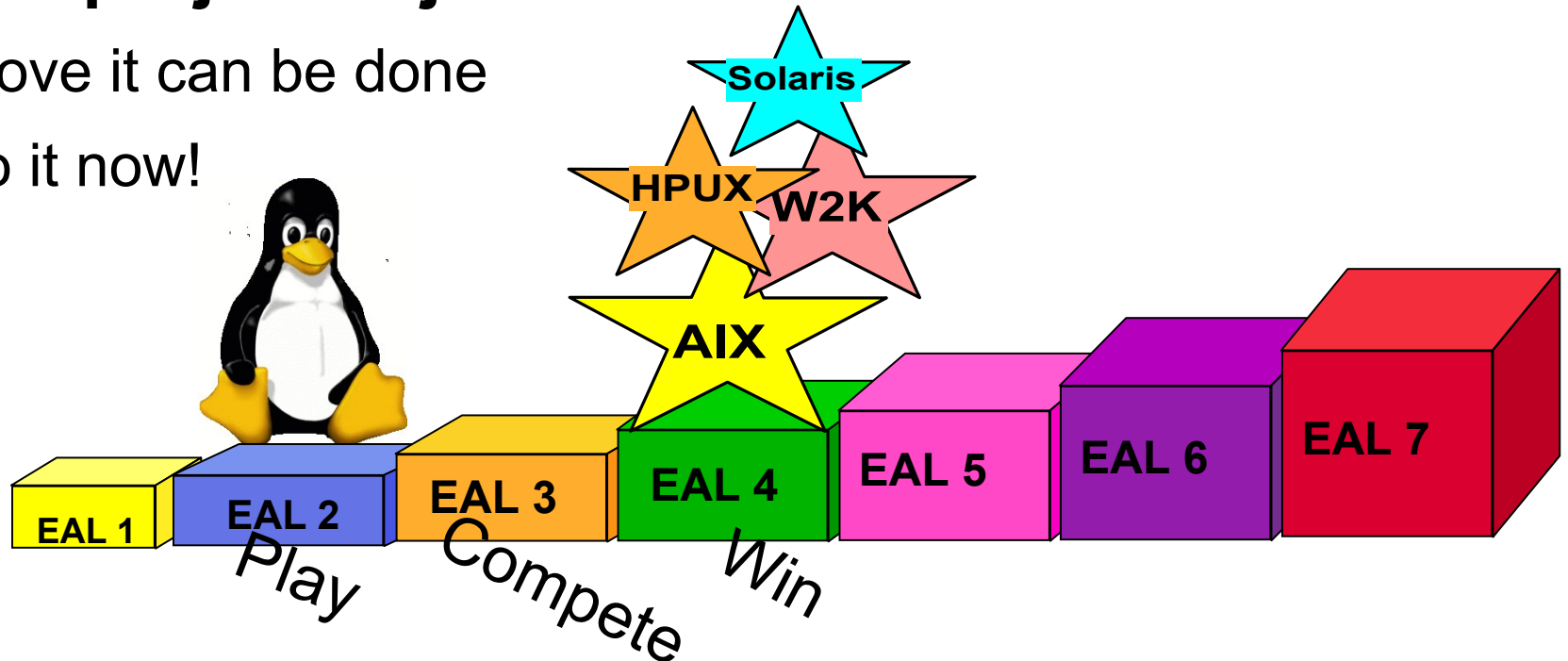
- Formal product and internal process documentation
- Depth of testing
- Life Cycle Support requirements



Roadmap... continued

- **Recall project objectives...**

- Prove it can be done
- Do it now!



- **as is/EAL2+:**

- Certify existing release of Linux
- Define Security Target based on existing capabilities – no new code development
- Don't claim compliance to CAPP, yet... use CAPP as guideline
- Create a roadmap for increasing certification levels

Scope of Linux Certification

- **Target of Evaluation:**

SuSE Linux Enterprise Server 8

- **Security Functions: *as is* for server system**

- Password based Identification and Authentication using the 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).
- VSFTP and SSH as the only trusted network applications
- Focus on the ability of the kernel to protect itself.










Scope... continued



- **EAL2+ Assurance Requirements:**
 - ACM: Configuration List
 - ADO: Delivery Procedures, Install and Configuration
 - ADV: Functional Specification, High Level Design
 - AGD: User and Administrator Guidance
 - ATE: Test Plan, Test Coverage
 - AVA: Strength of Function Analysis, Vulnerability Analysis

 - ALC: Flaw Remediation Procedure (the “+”)

What we had, what was missing...

Requirement	Disposition	
Configuration Mgmt	Covered by SuSE's configuration management procedures!	
Delivery & Operations	Covered by SuSE's install and config procedures!	
Development Environment	FSP – had to be written. Started with man pages, ensuring coverage for system calls and config files. HLD – had to be written, with focus on security function.	
Guidance Doc	Had to be written and shipped with product	
Testing/Plans	Built upon LTP, significant number of test cases for security developed.	
Vulnerability Analysis	Had nothing. Developed this area	
Life Cycle Support	Covered by SuSE's flaw remediation procedures!	

Lessons Learned

A stylized illustration in the background features a pencil with a green eraser and a yellow body, positioned diagonally across several overlapping sheets of paper. The papers are depicted with light green horizontal lines and some faint circular patterns, suggesting a document or blueprint. The entire scene is set against a light pinkish-red background with soft, overlapping shapes.

- Improved quality
 - Security defects identified through evaluation
 - Problems resolved and included
- Easy access to source code made for quick clarification of evaluation questions
- Design and user documentation is a weakness of open source
 - this project has tried to enhance the situation
- Boundaries of “development environment” more challenging for the open source development model

Community Value

Material provided to open source community

- Functional Specification: greater coverage of system calls and security related configuration files
- High Level Design: single, current reference document for 2.4.19 kernel with security focus
- User Documentation: details and scripts on how to install and administer the secure configuration
- Test Suite: new set of security test cases linked off Linux Test Project site
- Security Target: information on the scope of the “as is”/EAL2+ certification

Linux now has a good starting point for higher assurance levels AND for the evaluation of other distributions

Beyond EAL2+...

CAPP/EAL3+

- SuSE Linux Enterprise Server 8, with service package, currently in evaluation
 - audit capability
 - test tool for underlying hardware
 - additional network security functions
 - broader development environment focus
- Valid across IBM eServer
- More contributions to open source community anticipated
- Expected within 2-4 months.

CAPP/EAL4

- Desired place to be in 2004
- Need to consider Linux distributor plans/needs
- Need to consider evolving Protection Profiles – maybe

IBM's Commitment to Certification

- Linux
 - Continue to work with the open source community and Linux distributors to pursue increasing levels of certification
- IBM Operating Systems and Middleware
 - Comprehensive plans in place
 - Various states: certified or in progress

Complete	In Progress
AIX LPAR Linux on xSeries	zOS, z/VM, DB2, Tivoli Access Manager, IBM Directory Server, Websphere Application Server, WMQ, Linux on eServer

Contributors

- Doc Shankar, Security Architect, IBM LTC
- Helmut Kurth, Principle Evaluator, @sec GmbH

Legal Statement

- This work represents the view of the authors and does not necessarily represent the view of IBM.
- AIX, DB2, IDS, WebSphere, MQ, Tivoli Access Manager, IBM, eServer, are registered trademarks of International Business Machines Corporation in the United States, other countries, or both.
- UNIX is a registered trademark of The Open Group in the United States and other countries.
- SuSE Linux is a trademark of SuSE AG.
- Solaris is a trademark of Sun Microsystems.
- HP-UX is a trademark of Hewlett-Packard.
- Windows 2000 is a trademark of Microsoft.
- Linux is a registered trademark of Linus Torvalds.
- Intel is a trademark of Intel Corporation in the United States, other countries, or both.
- Other company, product, and service names may be trademarks or service marks of others.