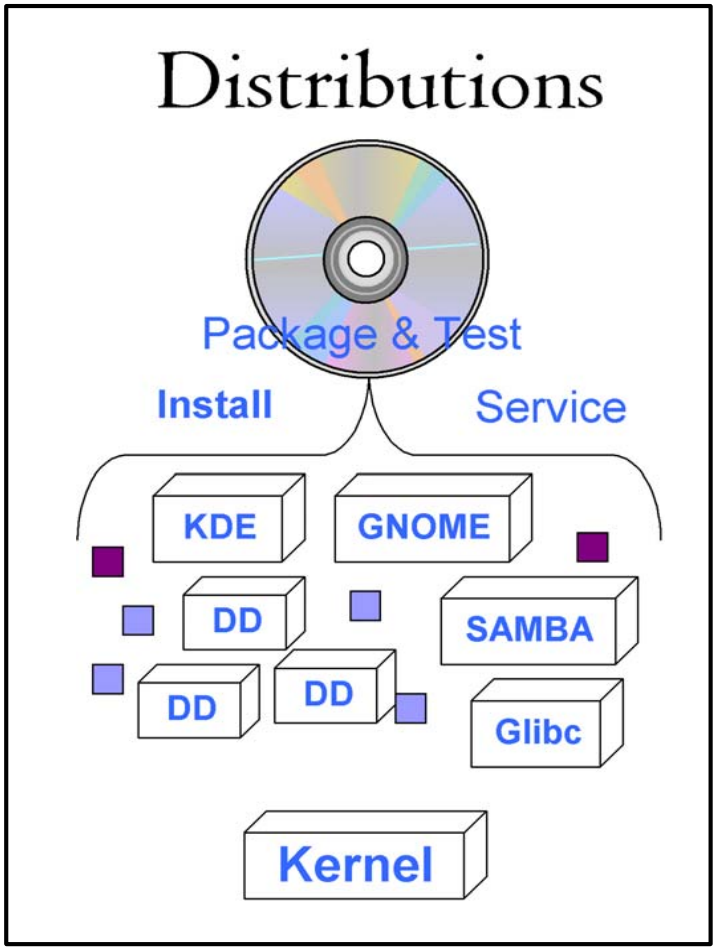
Open and Secure: Linux Today and Tomorrow

Dan Frye
VP, Open Systems Development
IBM

What is Linux?

- A free open source operating system developed by a world wide team of volunteer programmers and sold by several large software companies
- Usually acquired on a support subscription basis from a Linux Distributor
  - *Red Hat, SUSE / Novell, Turbolinux, Miracle Linux, Debian*
  - *Other regional distributors: Red Flag, Mandriva, Ubuntu, etc..*



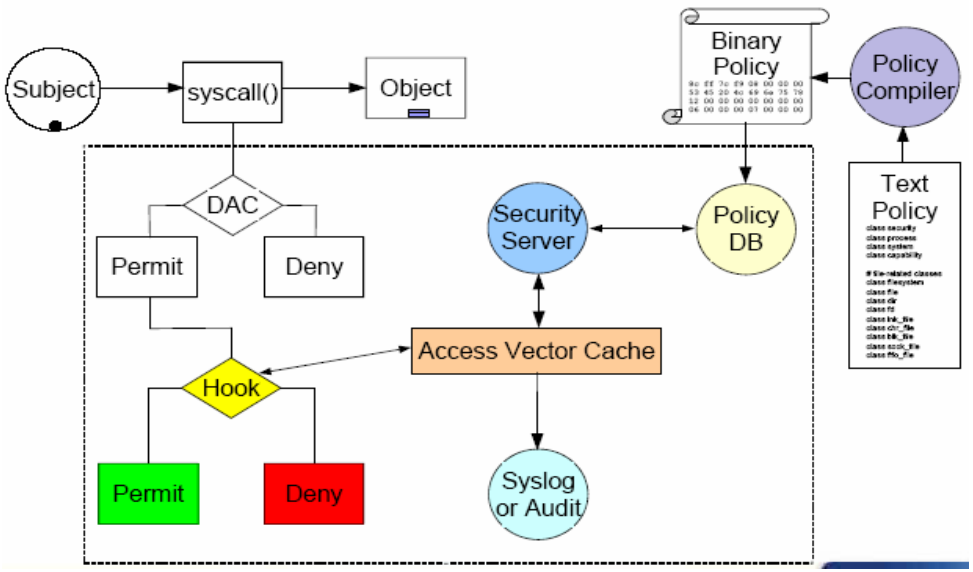
"Hello everybody... I'm doing a (free) operating system (just a hobby, won't be big and professional...)."

Linus Torvalds, creator of Linux, from the first Internet announcement on August 25, 1991. Even he initially underestimated its potential.

What is SELinux?

- A Linux Security Framework created to secure critical infrastructure
- An implementation of Mandatory Access Control (MAC)
- Mechanism to enforce separation of information by integrity and confidentiality labels

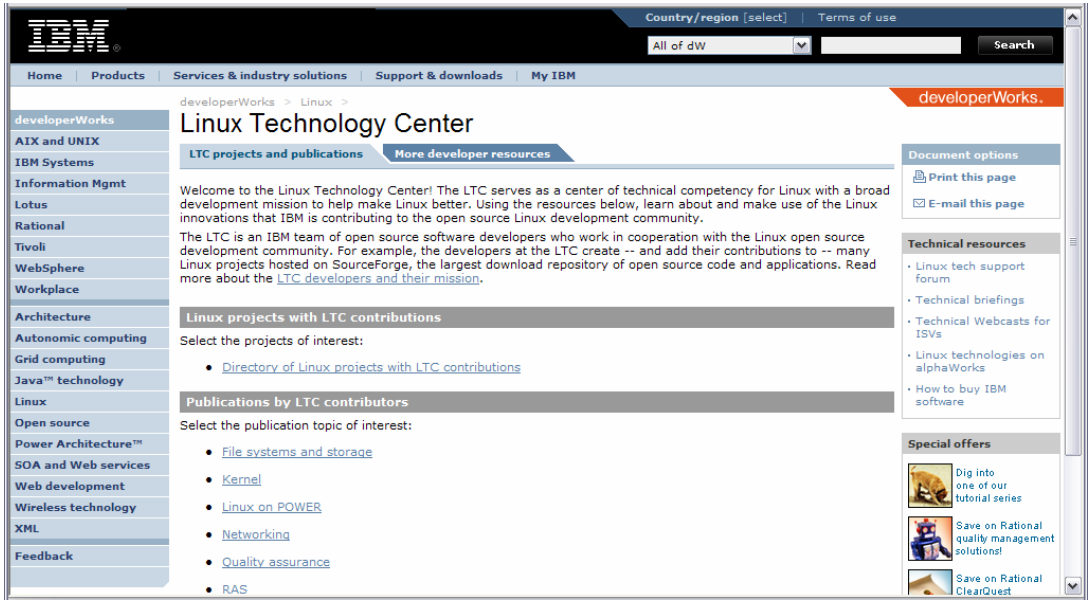
- Separation of policy from enforcement
- Most widely accepted mainstream implementation of MAC
- Supports type enforcement (strict and targeted), multi-level security, and role based access control policies



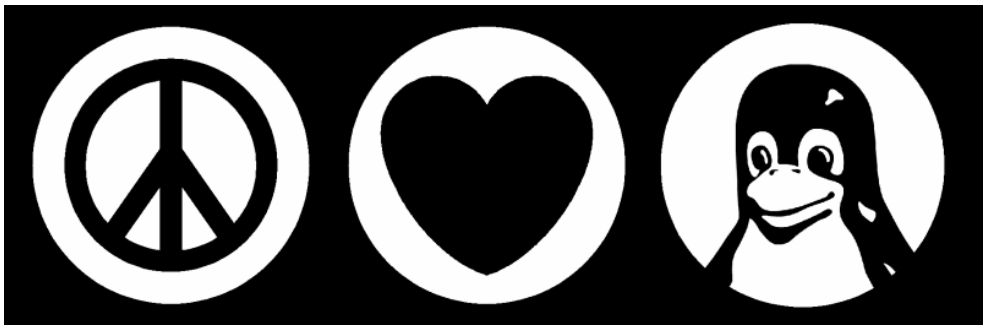
"The goals of this project are pretty specific. We are looking to incorporate flexible mandatory access control architecture into Linux."

Pete Loscocco, NSA
SELinux mailing list, 2001

What is the IBM Linux Technology Center ?
(www.ibm.com/linux/ltc)



- **The IBM participants in the Linux Open Source development community**
- **The Linux Operating System Development team for IBM**
  - All eServer platforms
  - All eServer software
  - Other key initiatives
- **The technical liaison to the Linux Distribution Partners**
- **The technical competency for IBM Servers, Software, Storage, Services and other key groups regarding Linux**



How do these 3 things fit together?

Community Driven

- Internet Enabled
- Worldwide Volunteers
- Security Unimportant

Maturation

- Open elements of IT industry join existing community
- Accelerate Linux into the Enterprise
- Security Adoption

Deployment

- IT Industry acknowledges Linux as a permanent presence
- OSS reluctant companies are compelled to engage
- Linux acknowledged as security leader

Few announced vulnerabilities

Call for Common Criteria
Can Linux be certified?

Please slow patch rate

Trusted Computing

Encrypted File system Bake-off

2008: IPv6

Flask Research Begins

New US crypto export rules

2.4 Released

FSF server hacked

RHEL4 GAs with SELinux support

OLPC Announces Security Architecture

0.01 Released

Stackguard

Ramen, Li0n & Adore

SELinux Upstreamed

Coverity Homeland Security Audits

Bliss

SELinux at Kernel Summit

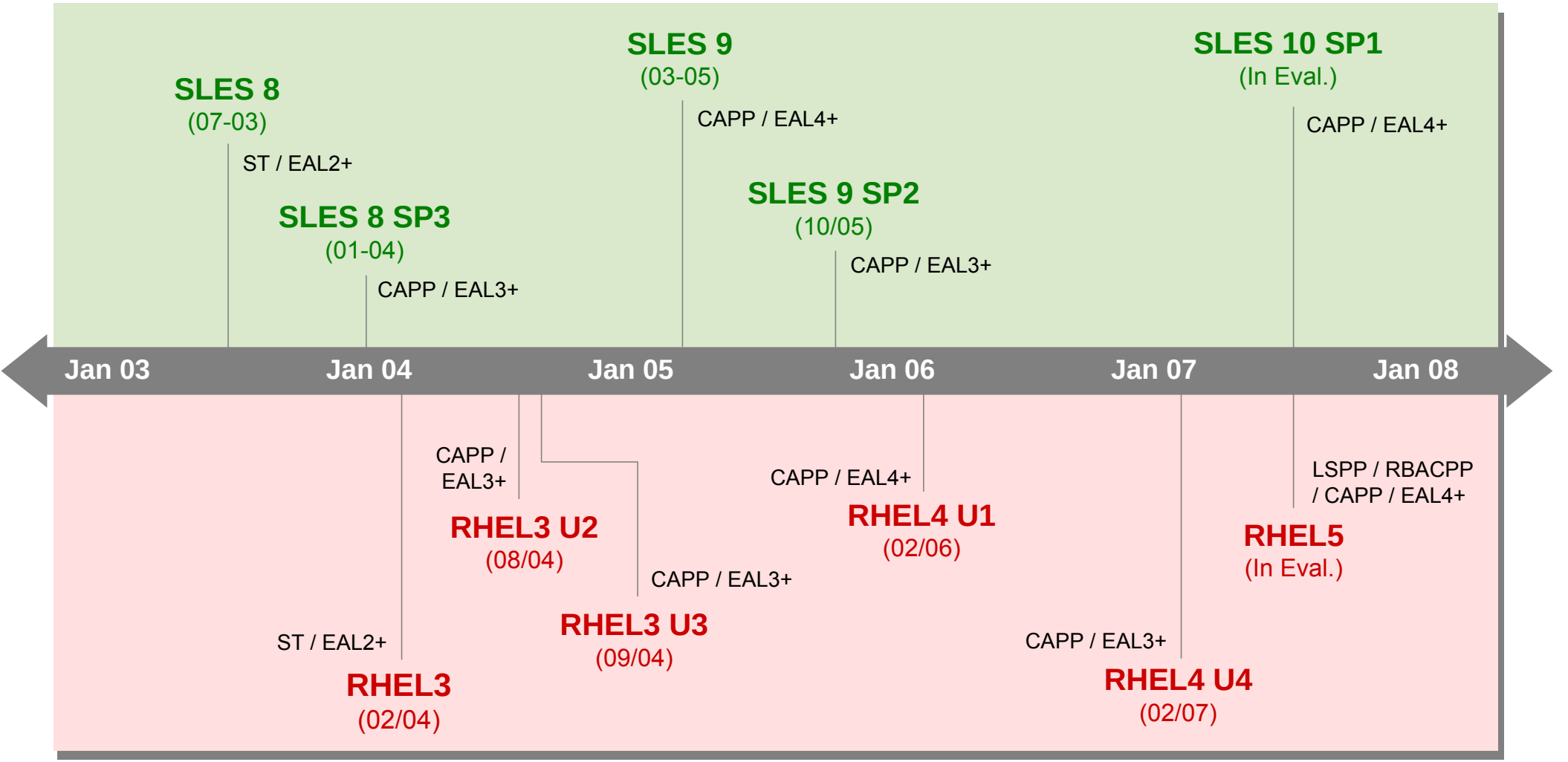
2.6 Released

Short History of Linux and Common Criteria

- **Linux has been evaluated at EAL2+, EAL3+, EAL4+ against CAPP, LSPP and RBACPP**
- **First evaluation completed July 2003**
- **Multiple enterprise providers: Red Hat and Novell**
- **CC Sponsors: HP, IBM, Oracle, SGI, and Unisys**
- **Linux is now the most evaluated operating system**
- **LSPP evaluation includes more HW platforms than have cumulatively been evaluated at LSPP for any operating system**
  - Scale up, scale out
- **Commoditization of government quality security**
  - Cost savings for government
  - Government style security widely available
- **Revalidation of open source development methodology**
- **IBM sponsored evaluations of CAPP at EAL2+, EAL3+, and EAL4+ of SLES & RHEL, now LSPP/RBACPP/CAPP at EAL4+**

Common Criteria Certification Dates

Novell SUSE Linux Enterprise Server

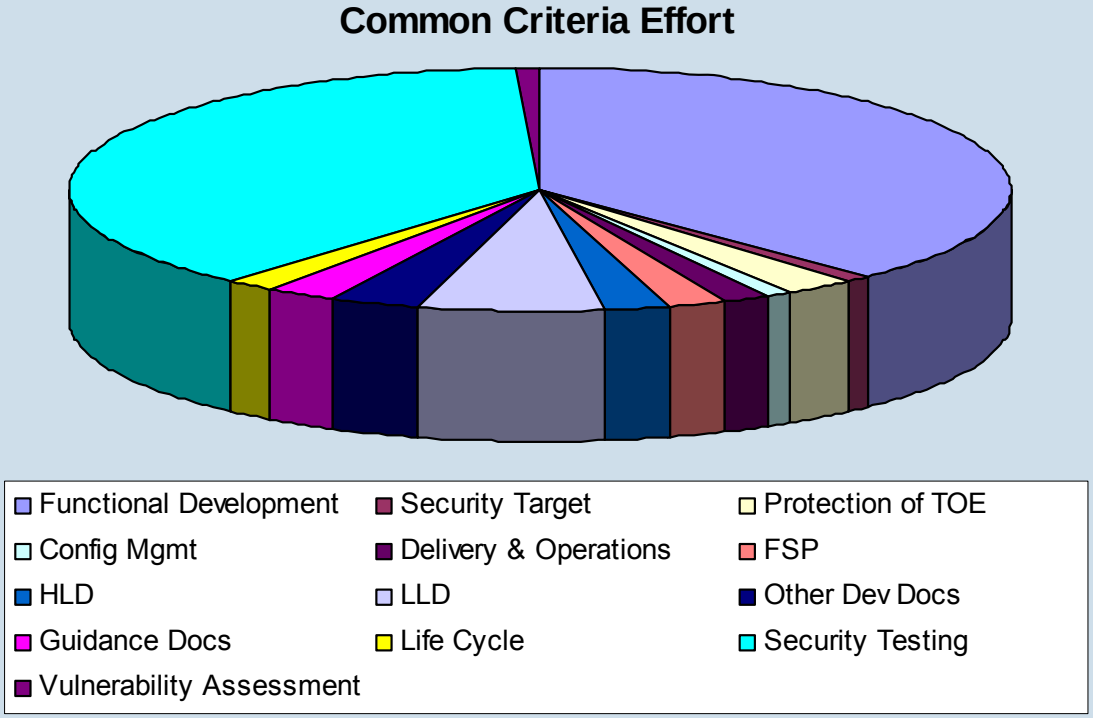


Red Hat Enterprise Linux

What does it take to get LSPP Certified at EAL4+?

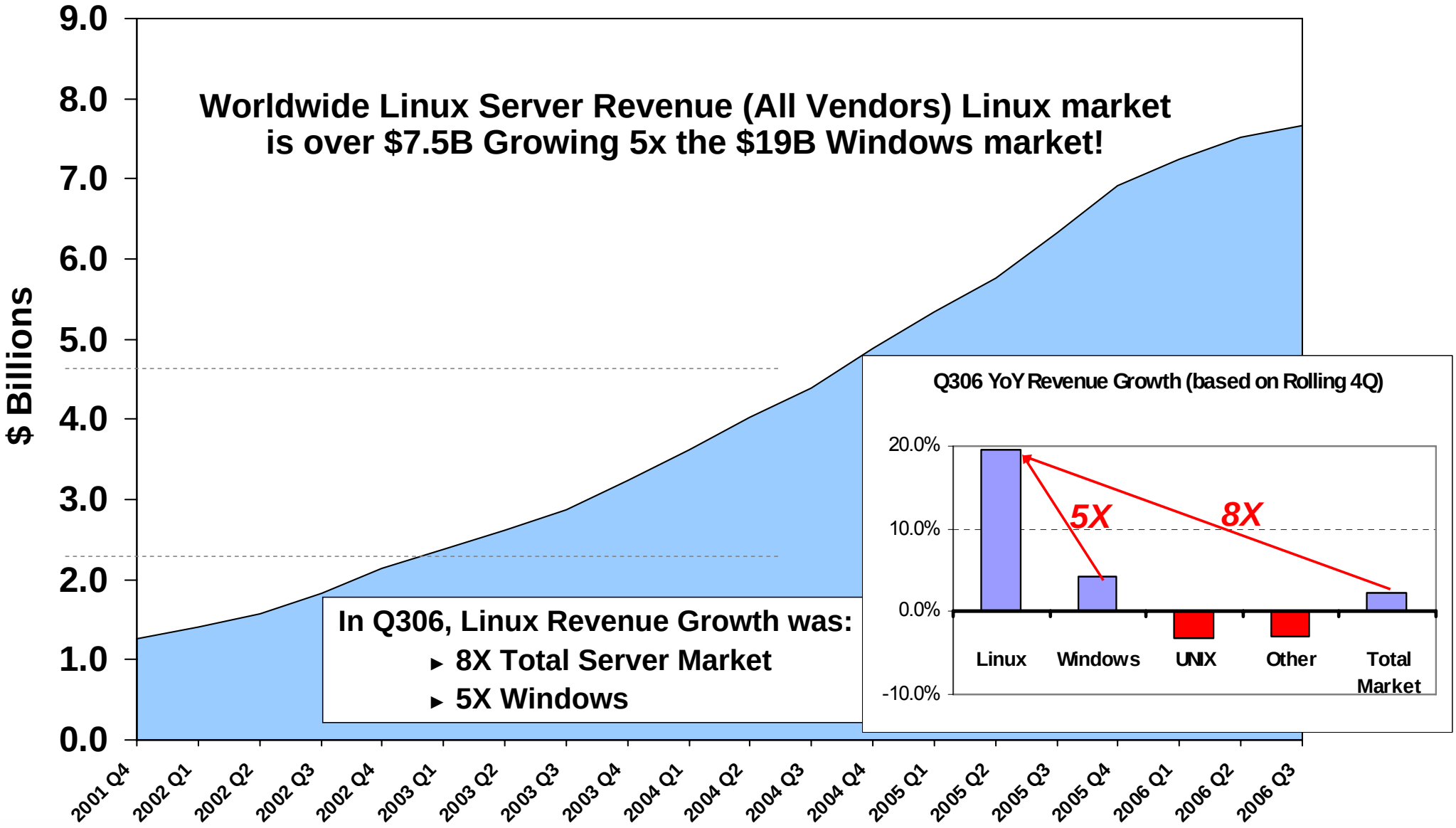
"*Methodically Designed, Tested, and Reviewed*"

- **Community Development**
  - MLS Policy
  - Labeled Networking
  - Labeled Printing
  - Audit Enhancements
  - Polyinstantiation



- **Assurance**
  - Security Target: 106 pages
  - Protection of TOE Security Functions (amtu)
  - Configuration Management (CVS)
  - Delivery & Operations: ~100 pages
    - Install & Configuration Manuals
  - Development Documents
    - Functional Specification: hundreds of man pages
    - High Level Design: 271 pages
    - Low Level Design: ~ 800 pages
    - Security Policy Model: 11 pages
  - Guidance Documentation: ~825 pages
    - User, Security & Admin Manuals
  - Life Cycle
    - Flaw remediation, security patch process
  - Testing
    - Test plan
    - 1200 test cases
  - Vulnerability Assessment: ~ 50 pages

Enterprises responded and demand for Linux is (Still) on Fire!



Source: Gartner Quarterly Statistics Rolling 4 Quarters 3Q06

Linux: UK Government Cabinet Office

Challenge

- ✓ Build a pilot of a secure Linux Operating System that allows cross department “Access to data Anywhere. Anytime. Anyhow.” and provides a common trust infrastructure for shared services and applications, primarily WebSphere and DB2.

Key Benefits*

- ✓ Server Process Confinement and Protection (sandboxing)
- ✓ Strongly enforced N-tier architecture
- ✓ Non intrusive enablement

Solution

- ✓ Tresys develops and tests policy (11/05 - 05/06)
- ✓ IBM tests pilot (05/06 - 07/06)
- ✓ Belmin test pilot integration (07/06 - 08/06)
- ✓ Pilot use (permissive mode) (08/06 - 10/06)
- ✓ **Pilot in production** (11/06)

* http://www.computerwire.com/industries/research/?pid=1C0B88FA-A04B-4A0E-862F-D51D898CBBC9

Linux: US Coast Guard

United States Coast Guard
U.S. Department of Homeland Security

Challenge

- ✓ Build a secure Linux Operating System that allows users to access multiple independent sessions at varying classification levels.

Key Benefits*

- ✓ Open Source Solution that provides a low cost alternative to multiple separate desktops or locked in proprietary solution
- ✓ Prevent cross domain contamination
- ✓ **Reduced Risk and Reduced Total Cost of Ownership**

Solution

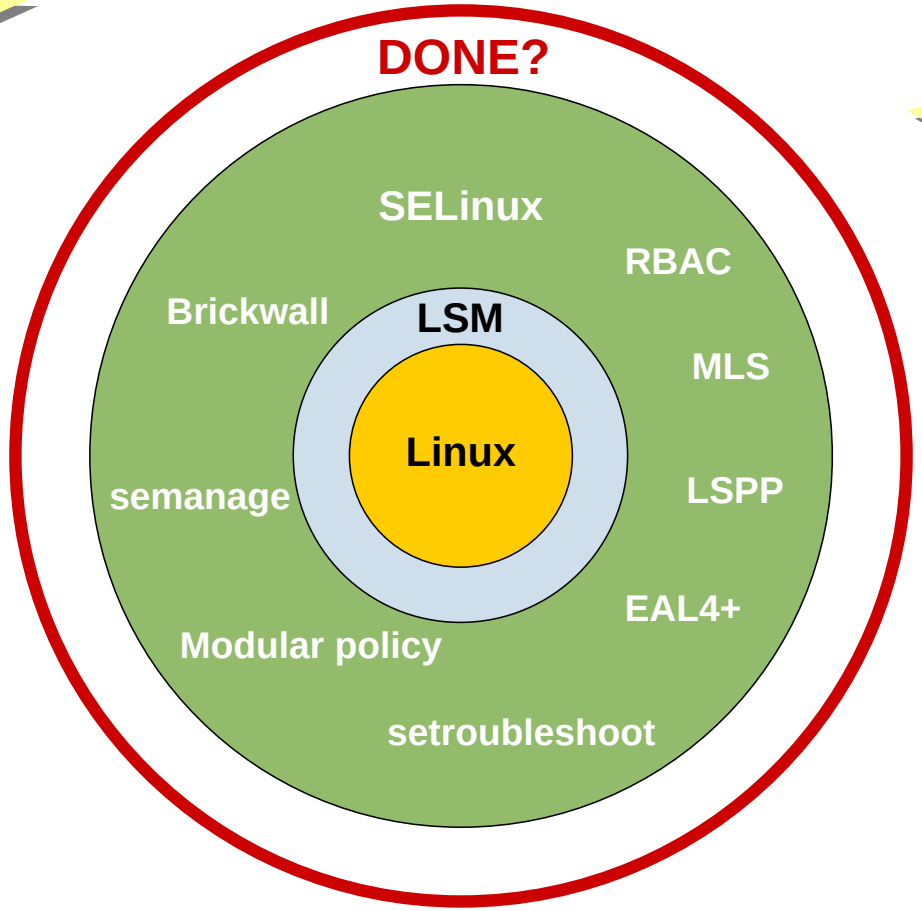
- ✓ TCS NetTop2 Thin Client
- ✓ SELinux –IBM Linux Technology Center, working with Red Hat, TCS and Linux Community
- ✓ IBM System x

* http://www.trustedcs.com/news/6news6_1_2j.htm

SELinux Today: Refinement and Productization Stage

Confine Damage from Hacked Programs

Precise Control Over Permissions

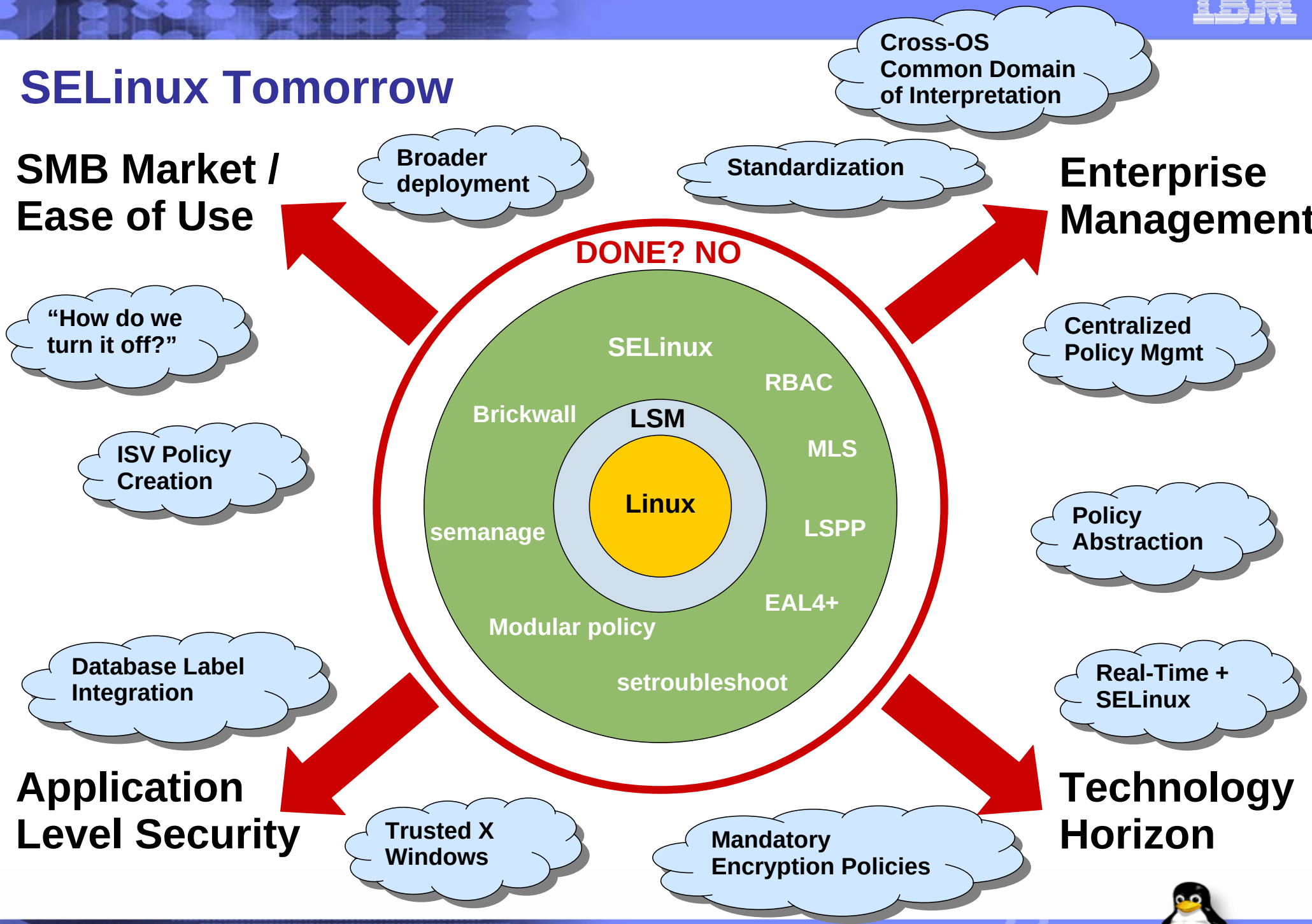


Remove Dependence on Root

Limit User and Application Privileges

Increasingly widespread deployment in public sector

SELinux Tomorrow



Thank You!

. . . Any Questions?

Trademarks and Presentation Notes

- The following are trademarks of the International Business Machines Corporation in the United States and/or other countries. For a complete list of IBM Trademarks, see www.ibm.com/legal/copytrade.shtml: eServer, System x, System p, System i, System z, IBM.

- The following are trademarks or registered trademarks of other companies:
- Java and all Java based trademarks and logos are trademarks of Sun Microsystems, Inc., in the United States and other countries or both
- Microsoft, Windows,Windows NT and the Windows logo are registered trademarks of Microsoft Corporation in the United States, other countries, or both.
- Linux is a trademark of Linus Torvalds in the United States, other countries, or both.
- Red Hat, Red Hat Linux are registered trademarks of Red Hat, Inc.
- SUSE is a registered trademark of Novell, Inc.
- Other company, product, or service names may be trademarks or service marks of others.

- Any statements about support or other commitments may be changed or cancelled at any time without notice. All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only Information is provided “AS IS” without warranty of any kind.

- This publication was produced in the United States. IBM may not offer the products, services or features discussed in this document in other countries, and the information may be subject to change without notice. Consult your local IBM business contact for information on the product or services available in your area.

- Information about non-IBM products is obtained from the manufacturers of those products or their published announcements. IBM has not tested those products and cannot confirm the performance, compatibility, or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

- The information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

- Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

- IBM makes no representation or warranty regarding third-party products or services including those designated as ServerProven, ClusterProven or BladeCenter Interoperability Program products. Support for these third-party (non-IBM) products is provided by non-IBM Manufacturers.

- IBM may have patents or pending patent applications covering subject matter in this document. The furnishing of this document does not give you any license to these patents. Send license inquires, in writing, to IBM Director of Licensing, IBM Corporation, New Castle Drive, Armonk, NY 10504-1785 USA.