

Linux Common Operating Environment (COE) Integration

4 February 2004

John Chew

john.chew@ngc.com

- **Background**
- **Key focus areas**
- **What's available now**
- **What's coming soon**
- **Where to find it**

- **Prior to March 2003, the Defense Information Systems Agency (DISA) sponsored COE Kernel Platform Compliance testing**
- **COE conformance testing now performed by industry**
- **Two reference implementations provided to aid industry in meeting DISA COE conformance**
 - **POSIX (Solaris 8)**
 - **Linux (Red Hat Linux 8.0)**

- **Distributed user account management**
 - Ability to manage users, groups, and profiles within an administrative domain of various Linux distributions
- **Common packaging mechanism**
 - Software installation mechanism uniform across all distributions, automated for end-user ease
 - Examples are RPM Package Manager (RPM) and Java Based COE Installer (JBCI)
- **Common security lockdown**
 - Level of security uniform across the network

Goal: Vendor-agreed-upon solution that ensures cross-Linux interoperability

- Need not be the COE-provided solution
- The key is the function performed, not the particular implementation

What's Available Now

- **Available from DISA**
 - **COE Kernel and Toolkit Version 4.2.0.9**
 - **Based on Solaris COE Kernel & Toolkit version 4.2.0.9**
 - **Built on Red Hat Linux 8.0**
 - **Packaged as a Factory CD**
 - **If install OS, load CD-ROM, type `build_it_all` to build the COE Kernel and Toolkit**
 - **Includes executable 4.2.0.9 COE Kernel and Toolkit, source code, and documentation**
- **Available from the Free Standards Group (FSG)**
 - **Source Code for COE Kernel and Toolkit Version 4.2.0.9**

➤ **Software:**

- COE Kernel 4.2.0.9 on Red Hat Linux 8.0 including
 - Java Based COE Installer (JBCI)
 - Account and Profile Manager (APM)
 - Security Policy Configuration Tool (SPCFG) and SPCFG Data (SPCFGD)
- Java Based Developer's Toolkit (JBDT)
- Linux kickstart file (ks.cfg)
- Auditing tool (SNARE - System iNtrusion Analysis & Reporting Environment version 0.9.2 from InterSect Alliance)
- Red Hat 8.0 operating system (OS) Security Patches

➤ **Documentation:**

- New for Linux:
 - Red Hat Linux 8.0 and COE Kernel Installation Procedures (IP)
 - JBDT Installation Procedures (IP)
- Pre-existing Solaris:
 - System Administrator's Manual (SAM) (Solaris)
 - Security Administrator's Manual (SECAM) (Solaris/W2K)
 - Programmer's Guide and Reference Manual (PGRM) (Solaris/W2K)

➤ **Source Code:**

- “linux” CVS repository with COE kernel and toolkit source
- “Base” directory with COTS software:
 - JRE 1.4.2_01, Perl 5.8.0, SPCFG and SPCFGD 4.9.0.0,
 - Mozilla 3.4.2 (used when compiling Netscape Security Services),
 - SQLite 2.7.3 (replaces GDBM found in 4.2.0.6)
- JIFI Builder from Java Specification Request JSR-38; used when compiling JBCI and JBDT; information at <http://openchannelsoftware.org/projects/JIFI/>
- Source for 3 SPCFG binaries
- Compilers J2SDK 1.4.2_01, Apache Ant 1.5.2
- Build Procedure (BP) and build scripts

➤ **Validation Procedures, Test Data Segment**

➤ **Host-Oriented Security Test Suite (HOSTS)**

information at <http://www.openchannelfoundation.org/projects/hosts>

➤ **Pre-existing Security Documentation:**

- Security Features Developers Guide (SFDG) for Solaris/W2K
- Security Features User's Guide (SFUG) for Solaris/W2K

What's Coming Soon

- **Updated Validation Procedure**
 - Manual Security Test Procedure

- **Updated security lockdown software and documentation**
 - Security Policy Configuration Tool Data (SPCFGD)
 - Security Features Developers Guide (SFDG)
 - Security Features User's Guide (SFUG)

- **More software and documentation will be posted on the FSG web site**

- **DISA email address for requesting Factory CD:**
coeengr@ncr.disa.mil
- **Free Standards Group URL for downloading source code:**
<http://gforge.freestandards.org/projects/qp-coe/>
- **DISA newsgroup for Q & A**
Server: coenews.ncr.disa.mil
Newsgroup: coenews.clrp (COE Linux-Based Platform)

Questions ?

Backup

➤ **Key Differences between Solaris and Linux COE Kernels**

- **Group-ID**

	<u>Solaris 8</u>	<u>Red Hat Linux 8.0</u>
	other:1	bin:1, added other:1
	added key:37	rpm:37, added key:37
	added ftp:117	ftp:50
- **Display Manager** (CDE vs. GNOME)
- **NIS+ Support** (Only NIS is available on Red Hat 8.0)
- **Software Installation Tool** (COEInstaller vs. JBCI)
- **Audit Log File Manager** (Not ported to Red Hat)
- **Linux baseline was the Solaris 4.2.0.9 COE Kernel; Solaris 4.2.0.0P10 source code available from DISA**

Linux COE Integration

What's Available Now

Deltas from Previous Linux Delivery

- **Previous Linux baseline was the Solaris 4.2.0.6 COE Kernel**

- **Changes from 4.2.0.6 to 4.2.0.9 include:**
 - **115 COE Kernel and 18 Toolkit changes made in Solaris were ported to Linux**
 - **JBCI and JBDT source is integrated into main COE kernel source code tree**
 - **Updated Validation Procedures**
 - **All except SMTP, Print, WWW and Audit Log File Manager were ported to Linux**
 - **Updated automated security test (HOSTS)**