The Next Big Thing

Preparing a Legacy Infrastructure for a Paradigm Shift

Jane Medefesser
Sr. Manager, Security Certifications
Sun Microsystems, Inc.
September 24, 2008

Introduction

The Problem

- SUN's Evaluation docs need to be prepared for CEMv3.1R2

Scope

- Part 3 of the CEM
  - V3.1 CCMB-2007-09-003 V2.3 CCMB-2005-08-003
- Focus on Vendor provided deliverables
- Emphasis on maximized re-use of existing documentation whenever possible

Assumptions

Based on rumors and mis-information, we entered the study with the following expectations:

- Big changes were coming
- Assurance classes had changed significantly
- Understanding the new requirements would require re-learning portions of the CEM
- Documentation reuse would be minimal

We were apprehensive !!!

Study Approach

- Side by side comparison of CEM 2.3 vs 3.1 requirements
- Analysis of previous documentation requirements
  - Configuration List
  - ETR
- Map 3.1 assurance requirements to legacy documents
- Conclusions & recommendations

Assurance Requirements

Assurance Class	Assurance components
ACM: Configuration Management	ACM_AUT.1 Partial CM automation
	ACM_CAP.4 Generation support and acceptance procedures
	ACM_SCP.2 Problem tracking CM coverage
ADO: Delivery and support	ADO_DEL.2 Detection of modification
	ADO_IGS.1 Installation, generation, and start-up procedures
ADV: Development	ADV_FSP.2 Fully defined external interfaces
	ADV_HLD.2 Security enforcing high-level design
	ADV_IMP.1 Subset of the implementation of the TSF
	ADV_LLD.1 Descriptive low-level design
	ADV_RCR.1 Informal correspondence demonstration
	ADV_SPM.1 Informal TOE security policy model
AGD: Guidance documents	AGD_ADM.1 Administrator guidance
	AGD_USR.1 User guidance
ALC: Life cycle support	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target evaluation	ASE_DES.1 TOE Description
	ASE_ENV.1 Security environment
	ASE_INT.1 ST Introduction
	ASE_OBJ.1 Security objectives
	ASE_PPC.1 PP claims
	ASE_REQ.1 IT Security requirements
	ASE_SRE.1 Explicitly stated IT security requirements
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.1 Testing: high-level design
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability assessment	AVA_MSU.2 Validation of analysis
	AVA_SOF.1 Strength of TOE security function evaluation
	AVA_VLA.2 Independent vulnerability analysis

CEM 2.3 EAL4 Assurance Requirements

Assurance Class	Assurance components
ADV: Development	ADV_ARC.1 Security architecture description
	ADV_FSP.4 Complete functional specification
	ADV_IMP.1 Implementation representation of the TSF
	ADV_TDS.3 Basic modular design
AGD: Guidance documents	AGD_OPE.1 Operational user guidance
	AGD_PRE.1 Preparative procedures
ALC: Life-Cycle Support	ALC_CMC.4 Production support, acceptance procedures and automation
	ALC_CMS.4 Problem tracking CM coverage
	ALC_DEL.1 Delivery procedures
	ALC_DVS.1 Identification of security measures
	ALC_LCD.1 Developer defined life-cycle model
	ALC_TAT.1 Well-defined development tools
ASE: Security Target	ASE_CCL.1 Conformance claims
	ASE_ECD.1 Extended components definition
	ASE_INT.1 ST introduction
	ASE_OBJ.2 Security objectives
	ASE_REQ.2 Derived security requirements
	ASE_SPD.1 Security problem definition
	ASE_TSS.1 TOE summary specification
ATE: Tests	ATE_COV.2 Analysis of coverage
	ATE_DPT.2 Testing: security enforcing modules
	ATE_FUN.1 Functional testing
	ATE_IND.2 Independent testing - sample
AVA: Vulnerability Assessment	AVA_VAN.3 Focused vulnerability analysis

CEM 3.1 EAL4 Assurance Requirements

Legacy Collection

28 (CAPP/RBAC) or 33 (LSPP) docs consisting of ;

- Security Target
- Design Collection
  - HLD, FSP, SPM (3)
  - LLD (8-CAPP/RBAC 13-LSPP)
- Analysis Collection (6)
- Test Suites and Reports (8)
- Configuration Management (2)

Legacy Collection - Detail

- **Design Collection**
  - Functional Specification
  - Informal Security Policy Model
  - High Level Design
  - Low Level Design
    - Audit
    - File systems
    - Identification & Authentication
    - Kernel – Process Management
    - Kernel – System V IPC
    - Native LDAP
    - Administration Tools
    - Trusted Startup
    - *Trusted Windowing*
    - *Trusted Printing*
    - *Profile Shells*
    - *Trusted Networking*
    - *Trusted Devices*

- **Analysis Collection**
  - Misuse Analysis
  - Strength of Function Analysis
  - Operational Vulnerability Analysis
  - Construction Vulnerability Analysis
  - Change Analysis
  - Flaw Remediation Analysis

- **Test Suite and Report Collection**
  - Certification Test Suite
  - Developers Manual Tests
  - Security Test Plan
  - CC Test Coverage Plan
  - Test Installation Procedures
  - Test Report
  - Test Suite Design & Maintenance Guide

docs in italics are LSPP only

v2.3 classes ASE and AGD

Class ASE: Security Target evaluation

ASE_DES.1	TOE Description
T_101	ST, PP's
ASE_ENV.1	**Security Environment**
T_101	ST, PP's
ASE_INT.1	**ST Introduction**
T_101	ST, PP's
ASE_OBJ.1	**Security Objectives**
T_101	ST, PP's
ASE_PPC.1	**PP Claims**
T_101	ST, PP's
ASE_SRE.1	**IT Security Requirements**
T_101	ST, PP's
ASE_TSS.1	**TOE Summary Specifications**
T_101	ST, PP's

AGD_ADM.1	Administrator Guidance
T_101	Security Target
TOE	Administrator's Procedures
TOE	Reference Manual
c_fsp	Functional Specification
c_106	High Level Design

AGD_USR.1	User Guidance
T_101	Security Target
TOE	User's Guide
TOE	Reference Manual
c_fsp	Functional Specification
c_106	High Level Design

Class AGD: Guidance documents

v2.3 class ACM: Configuration Management

ACM_AUT.1	**Partial CM Automation**
s10_126	Delivery and Configuration Procedures
int	Software Development Framework
int	Sun Product Life Cycle
ACM_CAP.4	**CM Capabilities**
T_101	Security Target
s10_126	Delivery and Configuration Procedures
int	Software Development Framework
int	Sun Product Life Cycle
s_cfl	Configuration List
TOE	The TOE suitable for testing
src	SCCS Teamware Log
ACM_SCP.2	**CM Scope**
s_cfl	Configuration List

v2.3 class ADV: Development Environment

ADV_LLD.1	Description Low Level Design
c_107	LLD_Audit
c_106	LLD_Filesystems
c_109	LLD_Identification and Authentication
c_104	LLD_Kernel - Process Management
c_105	LLD_Kernel - System V IPC
c_111	LLD_Native LDAP
c_116	LLD_Trusted Admin Tools
c_114	LLD_Trusted Startup
t_115	LLD_Trusted Windowing
t_112	LLD_Trusted Printing
t_117	LLD_Profile Shells
t_110	LLD_Trusted Networking
t_118	LLD_Trusted Devices
sac	Source Code (DVD)

ADV_RCR.1	Representation Coorespondence
T_101	Security Target
c_106	High Level Design
c_fsp	Functional Specification
c_107	LLD_Audit
c_106	LLD_Filesystems
c_109	LLD_Identification and Authentication
c_104	LLD_Kernel - Process Management
c_105	LLD_Kernel - System V IPC
c_111	LLD_Native LDAP
c_116	LLD_Trusted Admin Tools
c_114	LLD_Trusted Startup
t_115	LLD_Trusted Windowing
t_112	LLD_Trusted Printing
t_117	LLD_Profile Shells
t_110	LLD_Trusted Networking
t_118	LLD_Trusted Devices

ADV_SPM.1	Informal TOE Security Policy Modeling
c_spm	Security Policy Model
T_101	Security Target
c_106	High Level Design
c_fsp	Functional Specification
c_107	LLD_Audit
c_106	LLD_Filesystems
c_109	LLD_Identification and Authentication
c_104	LLD_Kernel - Process Management
c_105	LLD_Kernel - System V IPC
c_111	LLD_Native LDAP
c_116	LLD_Trusted Admin Tools
c_114	LLD_Trusted Startup
t_115	LLD_Trusted Windowing
t_112	LLD_Trusted Printing
t_117	LLD_Profile Shells
t_110	LLD_Trusted Networking
t_118	LLD_Trusted Devices
src	Source Code (DVD)

ADV_FSP.2	Fully Defined External Interfaces
c_fsp	Functional Specification
T_101	Security Target

ADV_HLD.2	Security Enforcing High Level Design
c_106	High Level Design
c_fsp	Functional Specification
T_101	Security Target

ADV_IMP.1	Subset of the Implementation of the TSF
TOE	Reference Manual
T_101	Security Target

v2.3 class ALC: Life Cycle Support

ALC_DVS.1	Identification of security measures
T_101	Security Target
s10_126	Delivery and Configuration Procedures
int	Software Development Framework
int	Development Security
int	Access Control Policy
int	Misc Sun Internal Policies and Guidelines

ALC_LCD.1	Developer Defined Lifecycle Model
T_101	Security Target
int	Software Development Framework
s10_150	Flaw Remediation Analysis
int	ALC_FLR Supporting Documentation
int	Sun Product Life Cycle

ALC_TAT.1	Tools and Techniques
int	Software Development Framework
int	Sun Product Life Cycle
src	Subset of the source code (DVD)

ALC_FLR.3	Flaw Remediation
s10_150	Flaw Remediation Analysis
int	ALC_FLR Supporting Documentation

v2.3 class ATE: Tests

ATE_COV.2	Analysis of Test Coverage
T_101	Security Target
s_fsp	Functional Specification
s10_700	Security Test Plan
t10_dmt	Developers Manual Tests
s10_735	CC Test Coverage Plan
T152	Evaluation Test Suite – Design and Maintenance Guide

ATE_DPT.1	Testing: High Level Design
T_101	Security Target
s_fsp	Functional Specification
c_106	High Level Design
s10_700	Security Test Plan
t10_dmt	Developers Manual Tests
s10_735	CC Test Coverage Plan

ATE_FUN.1	Functional testing
T_101	Security Target
s_fsp	Functional Specification
c_106	High Level Design
s10_700	Security Test Plan
t10_dmt	Developers Manual Tests
s10_735	CC Test Coverage Plan
s10_702	Security Testing Report

ATE_IND.2	Independent Testing - sample
T_101	Security Target
s_fsp	Functional Specification
c_106	High Level Design
s10_700	Security Test Plan
t10_dmt	Developers Manual Tests
s10_735	CC Test Coverage Plan
s10_702	Security Testing Report
s10_701	Security Testing- Installation Procedure (TIP)
T152	Evaluation Test Suite – Design and Maintenance Guide
TOE	Toe Media Kit (CD's)
TOE	User Collection (DVD)
TOE	System Administrator Collection (DVD)
TOE	Installation Collection

v2.3 class AVA: Vulnerability Assessment

AVA_MSU.2	Validation of Analysis
T_101	Security Target
s_fsp	Functional Specification
c_106	High Level Design
c_spm	Informal Security Policy Model
s10_701	Security Testing Installation Procedure
s10_121	Misuse Analysis
s10_125	Security Release Notes
c_107	LLD_Audit
c_106	LLD_Filesystems
c_109	LLD_Identification and Authentication
c_104	LLD_Kernel - Process Management
c_105	LLD_Kernel - System V IPC
c_111	LLD_Native LDAP
c_116	LLD_Trusted Admin Tools
c_114	LLD_Trusted Startup
t_115	LLD_Trusted Windowing
t_112	LLD_Trusted Printing
t_117	LLD_Profile Shells
t_110	LLD_Trusted Networking
t_118	LLD_Trusted Devices
src	Source Code (DVD)

AVA_SOF.1	Strength of TOE Security Function
T_101	Security Target
t10_122	Strength of Function Analysis
s_fsp	Functional Specification
c_106	High Level Design
c_spm	Informal Security Policy Model
s10_701	Security Testing Installation Procedure
s10_125	Security Release Notes
c_107	LLD_Audit
c_106	LLD_Filesystems
c_109	LLD_Identification and Authentication
c_104	LLD_Kernel - Process Management
c_105	LLD_Kernel - System V IPC
c_111	LLD_Native LDAP
c_116	LLD_Trusted Admin Tools
c_114	LLD_Trusted Startup
t_115	LLD_Trusted Windowing
t_112	LLD_Trusted Printing
t_117	LLD_Profile Shells
t_110	LLD_Trusted Networking
t_118	LLD_Trusted Devices
src	Source Code (DVD)

AVA_VLA.2	Independent Vulnerability Analysis
t10_101	Operational Vulnerability
109_124	Construction Vulnerability

V3.1 EAL4 documentation requirements

Assurance components	Notes
ADV_ARC.1 Security architecture description	current HLD can be modified for re-use in this class
ADV_FSP.4 Complete functional specification	new FSP, requirement changes
ADV_IMP.1 Implementation representation of the TSF	code and tools delivery - no problem
ADV_TDS.3 Basic modular design	Describe the TOE in terms of subsystems mapped to the FSP - one doc per subsystem. This is the new LLD
AGD_OPE.1 Operational user guidance	combines requirements for all user roles, replacing AGD_ADM.1 and AGD_USR.1
AGD_PRE.1 Preparative procedures	Replaces ADO_DEL.2 and ADO_IGS.1
ALC_CMC.4 Production support, acceptance procedures and automation	replaces ACM_CAP.4, re-use existing documentation
ALC_CMS.4 Problem tracking CM coverage	CMS plan is now an EAL4 requirement
ALC_DEL.1 Delivery procedures	same as ADO_DEL..1
ALC_DVS.1 Identification of security measures	Unchanged from 2.3
ALC_LCD.1 Developer defined life-cycle model	Unchanged from 2.3
ALC_TAT.1 Well-defined development tools	Unchanged from 2.3
ASE_CCL.1 Conformance claims	changes in ASE class will result in changes to the ST, but no additions or subtractions to the documentation collection
ASE_ECD.1 Extended components definition	
ASE_INT.1 ST introduction	
ASE_OBJ.2 Security objectives	
ASE_REQ.2 Derived security requirements	
ASE_SPD.1 Security problem definition	
ASE_TSS.1 TOE summary specification	
ATE_COV.2 Analysis of coverage	essentially the same as 2.3
ATE_DPT.2 Testing: security enforcing modules	some additional documentation may be required for new additions ATE_DPT.2.2C and ATE_DPT.2.3C
ATE_FUN.1 Functional testing	essentially the same as 2.3
ATE_IND.2 Independent testing - sample	essentially the same as 2.3
AVA_VAN.3 Focused vulnerability analysis	Vulnerability Analysis docs no longer required. Evaluators perform analysis using TOE, ADV and AGO documentation as input

New Document Collection - Detail

- **Design Collection**
  - Functional Specification (enhanced)
  - Informal Security Policy Model
  - Security Architectural Design (ADV_ARC)
  - Basic Modular Design (ADV_TDS)
    - Audit
    - File systems
    - Identification & Authentication
    - Kernel – Process Management
    - Kernel – System V IPC
    - Native LDAP
    - Administration Tools
    - Trusted Startup
    - *Trusted Windowing*
    - *Trusted Printing*
    - *Profile Shells*
    - *Trusted Networking*
    - *Trusted Devices*

- **Analysis Collection**
  - Strength of Function Analysis
  - Change Analysis
  - Flaw Remediation Analysis

- **Test Suite and Report Collection**
  - Certification Test Suite
  - Developers Manual Tests
  - Security Test Plan
  - CC Test Coverage Plan
  - Test Installation Procedures
  - Test Report
  - Test Suite Design & Maintenance Guide

- **Configuration Management**
  - CM Plan (Life Cycle Support)

docs in italics are LSPP only

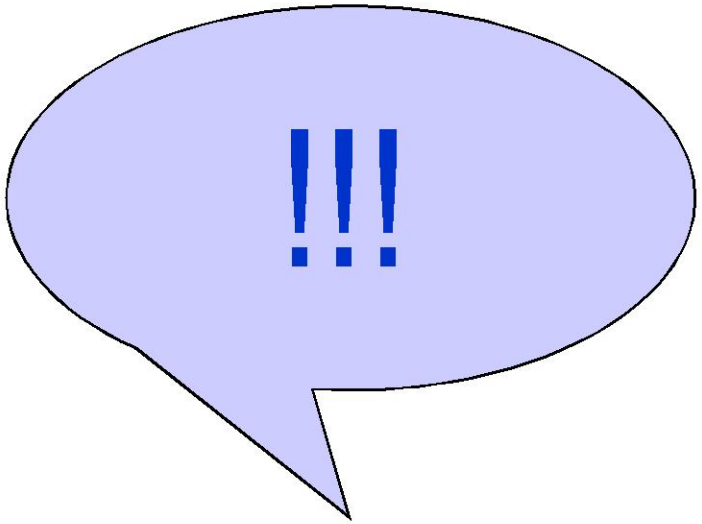
New Document Collection

26 (CAPP/RBAC) or 31 (LSPP) docs consisting of ;

- Security Target
- Design Collection
  - ARC, FSP, SPM (3)
  - TDS (8-CAPP/RBAC 13-LSPP)
- Analysis Collection (3)
- Test Suites and Reports (8)
- Configuration Management (3)

That's 2 fewer than the previous evaluation, *and* I don't have to perform a vulnerability analysis!!

Discussion



The Next Big Thing

Preparing a Legacy Infrastructure for a Paradigm Shift

Jane Medefesser
jane.medefesser@sun.com
http://www.sun.com/software/security/securitycert