UNICOS/mp Common Criteria Evaluation

Janet Lebens,

Cray Inc.

Agenda

- Definitions
  - NIAP CCEVS
  - Common Criteria
  - CC vs TCSEC
- Why Evaluate?
- Steps of Evaluation
- Details of Steps for Cray / Progress
- What Have We Learned?
- References for Additional Information

What is NIAP CCEVS?

- National Information Assurance Partnership Common Criteria Evaluation and Validation Scheme
- Staffed by NIST and NSA personnel
- Establishes a national program for evaluation for conformance to the Common Criteria
- Approves testing laboratories (CCTLs)
- Validates results of evaluations performed by CCTLs
- Issues Common Criteria certificate

What is the Common Criteria?

- **“Common Criteria for Information Technology Security Evaluation”**
- **ISO standard 15408**
- **Common, multi-national, mutually-recognized set of criteria for evaluating the security of computer products and services**
- **Sources were:**
  - **ITSEC – Europe**
  - **CTCPEC – Canada**
  - **TCSEC – United States (“Orange Book”)**
- **Intended to satisfy governments’ desires to improve availability of evaluated products and to reduce duplication of effort**
- **CC certificate implies conformance to a specification, including assurance. Results are accepted by all CCRA members.**

CUG 2004

CC vs TCSEC

TCSEC evaluation

- TCSEC evaluation conducted by NSA
- TCSEC evaluation funded by NSA
- Concept of “ramping” kept the rating current
- USA only
- Security functionality specified by TCSEC

CC evaluation

- CC evaluation done by commercial, third-party testing lab
- CC evaluation funded by vendor
- Conformance certificate only valid for specific HW/SW release
- One evaluation, accepted everywhere (16 nations)
- Assurance level independent of functionality

CUG 2004

Why Evaluate?

- **Customer interest**
- **NSTISSP No. 11 (National Security Telecommunications and Information Systems Security Policy) requires evaluated, validated products for all systems used for national security information**
- **Opportunity for evaluation of our software processes for creating product**

Steps of Evaluation

1. Choosing a CCTL
2. CCTL performs an Initial Assessment
3. Writing a specification (Security Target) and choosing a Protection Profile (PP)
4. Choosing an Assurance Level
5. Collecting evaluation evidence:
   - Documenting processes
   - Reviewing user and internal documentation
   - Providing a security test suite
6. Independent testing done by CCTL
7. CCTL submits evidence and results to NIAP CCEVS

CCTL Choice

- Currently 8 CCTLs on NIAP approved list
- SAIC was our choice (Science Applications International Corporation)
- Only CCTL to have completed a NIAP evaluation of an operating system
- Had completed the evaluation of Irix for Silicon Graphics
- Contract with SAIC, including mutual NDAs, was signed in July 2003

Security Target/Protection Profile

- A Security Target is the set of security functionality and assurance level specific to a target of evaluation (TOE)
- TOE may be any hardware, firmware, software or other components of a product.
- What is a Protection Profile?
  - A common, approved set of security requirements for a key technology (eg, operating system)
  - Specifies functionality requirements and assurance requirements
  - 3 categories of robustness: basic, medium, high
- Security Target should specify a Protection Profile if one is available
- CC certificate specifies conformance to a Security Target

Security Target (ST) Choice

- No currently available PP exists for our evaluation (EAL2+ for an operating system)
- TOE (Target of Evaluation) chosen to balance timely completion of validation, cost, and usefulness of evaluation:
  - Cray X1 hardware
  - UNICOS/mp 2.4 operating system software
  - Related processes and procedures

Did not involve adding new security functionality

Security Target details

- **TOE Description (Target of Evaluation):**
  - **Cray X1 mainframe**
  - **RAID disk arrays**
  - **UNICOS/mp Operating System**
- **Security Functionality**
  - **User data protection (DAC policy, ACLs)**
  - **Identification & Authentication (user attributes)**
  - **Security Management (admin tools to manage user accounts and data)**
  - **Protection of the TOE (the OS protects itself)**
- **Security Assurance Requirements**
  - **EAL2 requirements from CC, augmented w/ flaw remediation (EAL2+)**

Evaluation Assurance Levels

- CC specifies levels EAL1 through EAL7
- Defines a scale for measuring assurance
- Assurance that a product meets its security objectives
- Increasing assurance level requires greater evaluation effort based upon:
  - Scope – a larger portion of the product is included
  - Depth – evaluated to a finer level of design and implementation detail
  - Rigor – applied in a more structured, formal manner

Assurance Level Choice

- Levels 1 through 4 for commercial products
- We chose EAL2+ to satisfy known customer requirements
- EAL2 provides for basic robustness
- We added an augmentation for “Flaw Remediation” (EAL2+)
- Not planning EAL3 at this time but will consider as customer requirements warrant

Cray Evaluation Evidence

- Touched many areas of the company
- Software Configuration Management processes
- Delivery and Operations processes, including installation
- Flaw remediation process
- Development documentation:
  - Functional specification
  - High level design
- Guidance documentation: User and Admin guides
- Tests:
  - Evidence of coverage
  - Security test suite from Cray
  - Independent testing by CCTL
- Vulnerability Assessment

Evaluation Progress

- Contract & NDA signed with SAIC in July 2003
- Initial Assessment conducted in August 2003
- Formally entered EAL2+ evaluation in Sept. 2003
- First evidence submitted in October 2003
- In the process of submitting evidence, receiving feedback/review from SAIC, and resubmitting evidence
- Expect SAIC independent testing this summer
- Expect validation by NIAP CCEVS before the end of the year
- The validation report will be published on NIAP's web site upon completion of the evaluation. It includes the Security Target.

What Have We Learned?

- Evaluation still in progress
- Our processes (new and inherited from Cray Research and SGI days) serve us well
- NIAP evaluations are a significant cost burden to a vendor
- EAL2+ evaluation is expected to cost close to $1 million
- The evaluation is for an “instant in time” (ie, Cray X1 running UNICOS/mp 2.4)
- Evaluation is of processes and procedures, as much as a specific product.

CUG 2004

More Information

- **NIAP website**
  - http://niap.nist.gov
- **Information Assurance Technical Framework Forum**
  - http://www.iatf.net
- **From**
  - **http://niap.nist.gov/cc-scheme/in_evaluation.html**

Product Name: Cray UNICOS/mp on Cray X1
Technology Type: Operating System
Entered into Evaluation: 22 September 2003
Conformance Claim: EAL 2 Augmented ALC_FLR.1
Sponsor: Cray Inc.
Point of Contact: Mr. Peter Rigsbee
Phone: 651.605.9167
Email Address: par@cray.com
CC Testing Lab: SAIC