

National Information Assurance Partnership

Partnership to meet the security testing needs of IT producers

COMP 6370 – Common Criteria and other Certifications

Common Criteria Evaluation and Validation Scheme (CCEVS)

- **Objective**
 - Test Security Properties of Commercial Products
- **Approach**
 - Tests performed by Accredited Commercial Laboratories
 - Validity/Integrity of results underwritten by NIAP
 - Results posted for public access
- **Evaluates conformance of the security features of IT products to the International Common Criteria (CC) for Information Technology Security Evaluation.**
- **Issues Certificates to vendors for successful completion of evaluations.**
 - Not an NSA or NIST endorsement
 - Not a statement about goodness of product

COMP 6370 – Common Criteria and other Certifications

The Common Criteria is a multipart standard used for evaluation of IT products and systems

- ❖ Common set of requirements for evaluating the security of IT products/systems
- ❖ Targets three groups that are considered to be principal users of the CC

Consumer
Allows for comparability between functions of products and systems.

Vendor
Provides security requirements to be satisfied by their products or systems.

Evaluator
Use criteria when determining if the product or system conforms to the security requirements for certification.

- ❖ **CC is presented in 3 distinct parts**
- ❖ **Part 1:** Introduction and general concepts / principles of IT security evaluation
- ❖ **Part 2:** Catalog of potential security functional requirements for Targets of Evaluations (TOEs)
- ❖ **Part 3:** Catalog of security assurance requirements
 - Establishes evaluation assurance levels (EALs) as a standard way of expressing the assurance requirements for TOEs;
 - Defines evaluation criteria for Protection Profiles (PPs) and Security Targets (STs)

COMP 6370 – Common Criteria and other Certifications

Scope of the Common Criteria

- **Within the scope of the CC:**
 - Specification of security properties of IT products and systems to address:
 - Confidentiality-Unauthorized disclosure
 - Integrity-Unauthorized modification
 - Availability- Loss of use
 - Applicable to IT security countermeasures implemented in HW, SW, and firmware
- **Outside the scope of the CC:**
 - "People-based" and physical security measures
 - Administration, Legal, Procedural Issues
 - Certification and Accreditation
 - Evaluation Methodology
 - Cryptographic "algorithm" definition (the CC evaluation only addresses use of crypto, not strength of crypto algorithm)

COMP 6370 – Common Criteria and other Certifications

NSTISSP No. 11

- National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology Products that protect national security information.
- Effective 1 July 2002, all COTS IA and IA-Enabled products must be evaluated by
 - International Common Criteria Mutual Recognition Arrangement
 - NIAP Evaluation and Validation Program (CCEVS)
 - NIST FIPS validation program
- The evaluation/validation of COTS IA and IA-enabled products will be conducted by accredited commercial laboratories, or the NIST.
- All GOTS IA or IA enabled products must be evaluated by NSA or an NSA approved process.

COMP 6370 – Common Criteria and other Certifications

NSTISSP #11 Guidance IA & IA-Enabled Products

Levels Of Robustness

7
6
5
4
3
2
1
0

High robustness products

Medium robustness products

Basic robustness products

| | Crypto Modules and Algorithms |
|--|--|
| NSA Involvement in Product Evaluation NSA Evaluated Product List | Type 1 Crypto for Classified |
| NIAP - Certified CCTL Evaluations Includes: <ul style="list-style-type: none"> <li style="width: 50%;">NIAP Labs <li style="width: 50%;">CSC <li style="width: 50%;">Booz Allen <li style="width: 50%;">Hamilton <li style="width: 50%;">Cable & Wireless <li style="width: 50%;">Cygnacom <li style="width: 50%;">CoACT <li style="width: 50%;">InfoCard <li style="width: 50%;">Criterion <li style="width: 50%;">SAIC | FIPS evaluated under CMVP (FIPS 140-1 or 140-2) Validated Product List http://csrc.nist.gov/cryptval CMVP Labs <ul style="list-style-type: none"> • Adas • Cygnacom (CEAL) • CoACT • EWA • Dromas • InfoCard |

COMP 6370 – Common Criteria and other Certifications

The COMMON CRITERIA EVALUATION AND CERTIFICATION SCHEME

July 23, 2002

The Big CCEVS Picture

By 1 July 2002, the acquisition of all COTS IA and IA-enabled IT products to be used on systems (including) NATIONAL SECURITY INFORMATION SHALL BE LIMITED ONLY TO THOSE WHICH HAVE BEEN EVALUATED AND VALIDATED AGAINST THE CC, NIAP CCEVS OR PFP.

... NISTISSP 11 POLICY LETTER, DATED JANUARY 2000

CCEVS Products

Available products to assist in making a more secure infrastructure.

Boosting consumer confidence through evaluation and testing of vendor products.

Policy that influences our adherence to the Common Criteria.

Help & Guidance

- CCEVS by Product Type
- CCEVS by Assurance Level
- CCEVS by Product Name
- CCEVS by Vendor
- Approved Evaluated Products
- Products in Evaluation
- Individual Protection Profiles
- Protection Profiles in Evaluation

Getting a Product Evaluated

- Finding a CCE
- Getting a CCEV Approved

NISTISSP #11 Fact Sheet

- NIST Spec Pub 800-23
- NIAP/CC
- NISTISAM Comparison 09
- NISTISAM Comparison 08
- NISTISAM Comparison 07
- NISTISAM Comparison 06
- NISTISAM Comparison 05
- NISTISAM Comparison 04
- NISTISAM Comparison 03
- NISTISAM Comparison 02
- NISTISAM Comparison 01
- For a comprehensive or falling other document (related documentation)

<http://niap.nist.gov/cc-scheme>

COMP 6370 – Common Criteria and other Certifications


DoD Policy and the Common Criteria

- **DOD Directive 8500.1 – 24 OCT 2002**
 - All IA or IA-enabled products incorporated into DoD Information systems must comply with NISTISSP 11
 - Products must be satisfactorily evaluated and validated either
 - prior to purchase or
 - if product has not been evaluated yet, as condition of purchase, vendor must commit to having their product evaluated.
 - Purchase contracts shall specify that product validation will be maintained for subsequent releases.
- **DOD Instruction 8500.2 – 12 FEB 2003**
 - Defines generic “robustness” levels of basic, medium, and high and assigns “baseline levels” of IA services dependent on value of information and environment
 - If Government Protection Profile (PP) exist for a specific technology area
 - products must get evaluated against PP.
 - If no Government PP exist for a specific technology area
 - as a condition of purchase, products must be submitted for evaluation at the appropriate EAL level as determined by ISSE and DAA.

COMP 6370 – Common Criteria and other Certifications

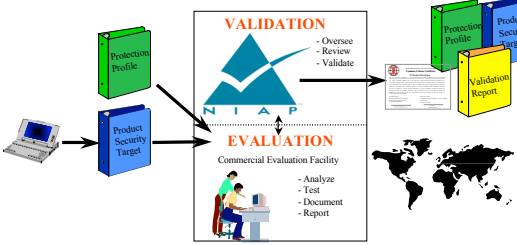
Use CC Language to Express Product Security Needs

- **CC Provides—**
 - Extensive, but not exhaustive, catalog of security requirements
 - Standardized format for communication among stakeholders and other players
- **Product Description and Environment**
 - Security Environment, Usage Assumptions, Organizational Security Policies, Threats, Objectives
- **Security Functional Requirements**
 - Desired security behavior
- **Security Assurance Requirements**
 - Functionality is effectively and correctly implemented
- **Rationale** (How requirements address security objectives)



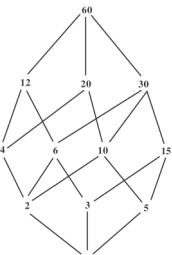
COMP 6370 – Common Criteria and other Certifications

Evaluation Process Summary



COMP 6370 – Common Criteria and other Certifications

Lattice Model of Access Security



- A lattice is a mathematical structure of elements organized by a relation among them represented by a relational operator.
- This is a partial ordering and therefore elements are:
 - Transitive
 - if $a < b$ and $b < c$, then $a < c$
 - Antisymmetric
 - if $a <= b$ and $b <= a$, then $a = b$

Lattice of all factors of the number 60

COMP 6370 – Common Criteria and other Certifications

Lattice Model of Security

- Marking contains name of level + name of compartment (e.g. TOP SECRET PETUNIA)
- Only those “read into” the compartment can read the information in that compartment, and then only at the level of their overall access
- A commercial security policy such as public, proprietary and internal with the natural ordering that public data are less sensitive than proprietary which is less sensitive than internal.

COMP 6370 – Common Criteria and other Certifications

Bell-LaPadula

- Is a state machine model
- Utilizes the machine state to check security
 - All permissions must be captured
 - All subjects accessing objects must be captured
 - These are machine states
- Complicated state set results
- *Defining state set is the major BLP problem*
- Mandatory security policies
- Simple security (ss) policy (no read up)
- Star (*) policy (no write down)
 - How to send messages from high to low?
 - Trusted subjects can violate policy
- Discretionary (ds) policy
- *If all three properties are satisfied, a state is secure*

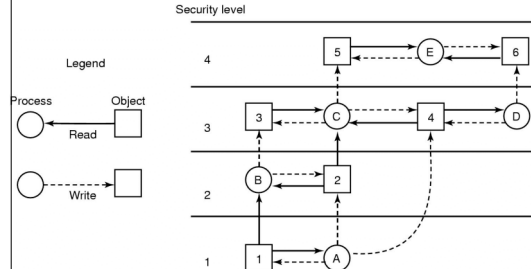


COMP 6370 – Common Criteria and other Certifications



Centralized vs Decentralized Security

- Example: Bell-LaPadula model
 - Processes can write up and read down



COMP 6370 – Common Criteria and other Certifications



BLP Advantages & Disadvantages

- **Advantages**
 - Descriptive capabilities of the model
 - Policies based on security levels -- easy to introduce other structures in their place
 - Actual security policies
 - Specific solution (e.g. Multics)
- **Disadvantages**
 - Deals only with confidentiality, not integrity
 - Does not address management of access control
 - Contains covert channels



COMP 6370 – Common Criteria and other Certifications



Rational for security evaluations

- Users of secure systems need assurance that products they use are secure.
- Users can:
 - trust manufacturer (not always a good idea!),
 - test system themselves (expertise not always available, and a very costly option),
 - rely on an impartial third party assessment (i.e. an *evaluation*).
- The Trusted Computer Security Evaluation Criteria (TCSEC), i.e. the *Orange Book*, were first generally accepted criteria for evaluating secure products.
- Orange Book provided method to *rate* security products on a simple scale.
- Other criteria developed since, but still relate their schemes back to Orange Book.



COMP 6370 – Common Criteria and other Certifications



'Target' of an evaluation

- Evaluation criteria cover **products**, e.g. operating systems & systems, i.e. collections of products for a specific use.
- **Product evaluation** needs a set of generic requirements - provided by classes of Orange Book and profiles of ITSEC, Common Criteria.
- **System evaluation** needs reqs. capture to be part of evaluation – covered by ITSEC (European Consortium -- (UK, France, Germany, Netherlands)).



COMP 6370 – Common Criteria and other Certifications



Structure of the evaluation criteria: ITSEC vs. Orange Book

- Evaluating security in a product relates to:
 - **Functionality**: security features of system, e.g. DAC, MAC, authentication, auditing,
 - **Effectiveness**: the appropriateness of the functionality for the security requirements,
 - **Assurance**: degree of certainty in the correctness of the implementation of the functionality.
- Orange Book classes cover all aspects at once.
- ITSEC more flexible.



COMP 6370 – Common Criteria and other Certifications



The Orange Book

- In 1985 the *Trusted Computer Security Evaluation Criteria* (Orange Book) was published - the first guideline for evaluating security products (in this case operating systems).
- Although Orange Book aimed at 'national security' sector, the authors intended to create more general document to provide:
 - yardstick for users to assess degree of trust in systems;
 - guidance for manufacturers of security systems;
 - basis for specifying security requirements for systems.



COMP 6370 – Common Criteria and other Certifications



19

Evaluation classes

- *Evaluation classes* are designed to address typical patterns of security requirements.
- Specific *security feature* and *assurance* requirements are combined in the definition of these evaluation classes.
- Main parts of evaluation class description:
 - **Security policy:** MAC and DAC policies.
 - **Marking of objects:** labels for object sensitivity.
 - **Identification of subjects:** users must be identified & authenticated.
 - **Accountability:** audit logs of security-relevant events.
 - **Assurance:** operational and life cycle assurance.
 - **Documentation:** use guidance and test/design documentation.
 - **Continuous protection:** ensure features cannot be tampered with.



COMP 6370 – Common Criteria and other Certifications



20

Security Divisions

- Orange Book uses criteria to define four secure divisions and seven security classes.
- Four security divisions are:
 - D - Minimal protection
 - Class for products that were submitted for evaluation but did not meet the requirements of any higher Orange Book class.
 - C - Discretionary protection ('need to know')
 - B - Mandatory protection (based on 'labels')
 - A - Verified protection
- The security classes of the Orange Book are defined incrementally.



COMP 6370 – Common Criteria and other Certifications



21

C1 - Discretionary Security Protection

- Intended for an environment where *co-operating users process data at the same level of integrity*.
- **Security policy:** DAC based on users and/or groups enables users to share access to objects in a controlled fashion.
- **Identification of subjects:** Users must identify themselves and their identity has to be authenticated.
- **Operational assurance:** TCB must have execution domain, and features needed for the periodic validation of correct operation of the TCB.
- **Life-cycle assurance:** security testing for 'obvious flaws'.
- **Documentation:** a user's guide, a Trusted Facility Manual (for the system administrator), test and design documentation needed.
- C1 systems aimed at friendly environment and do not give strong security.



COMP 6370 – Common Criteria and other Certifications



22

C2 - Controlled Access Protection

- C2 systems make users individually accountable for their actions.
- **Discretionary access control** enforced at the granularity of single users. The propagation of access rights has to be controlled.
- Subjects must not access objects containing information produced by a prior subject (*object reuse*).
- Audit trails of security-relevant events.
- Testing and documentation must cover the security features but assurance still limited. Testing for obvious flaws only.
- C2 is regarded as most reasonable for commercial applications although C2 systems are intrinsically rather weak.
- Most major vendors offer C2-evaluated versions of their operating systems or database management systems.



COMP 6370 – Common Criteria and other Certifications



23

B1 - Labelled Security Protection

- Division B intended for products handling classified data and enforcing mandatory Bell-LaPadula policies.
- **Labels** for each subject and object, constructed from hierarchical classification levels and non-hierarchical categories.
 - Label integrity must be protected.
- Identification and authentication help determine user's security label.
- If protection based on labels, need to consider handling of labelled objects when exported to another system, or to a printer.
- Communications channels can be single- or multi-level.
 - In multi-level channels, objects are exported with labels. In single-level channels, the TCB and authorised user designate label of exported information.
- Human-readable output must also be labelled, e.g. by label on each page.
- To achieve higher assurance, informal or formal model of security policy is required.
- Testing and documentation has to be much more thorough.
 - Design documentation, source and object code have to be analysed.
 - All flaws found in testing must be removed.
- However, class B1 is not very demanding with respect to TCB structure, and complex systems like multi-level-secure Unix systems & DBMSs have obtained class B1 certificates.



COMP 6370 – Common Criteria and other Certifications



24

B2 - Structured Protection

- B2 increases assurance, mainly by adding requirements on the design of the system.
- MAC governs access to physical devices.
- Users must be notified about changes of their security levels.
- There has to be a *Trusted Path* for login and initial authentication.
- Formal model of security policy and a *descriptive top level specification (DTLS)* of system needed.
- Distinct address spaces to isolate processes.
- Hardware support for memory management.
- *Covert channel analysis* must be conducted and events potentially creating a covert channel must be audited.
- Security tests must be performed on resistance of TCB to penetration.



COMP 6370 – Common Criteria and other Certifications



25

B3 - Security Domains

- Many of B3 elements cover security management:
 - A security administrator is supported.
 - Auditing mechanisms monitor occurrence or accumulation of security-relevant events and issue automatic warnings.
 - *Trusted recovery* facilitated after system failure.
- TCB complexity to be minimised, and must exclude non security-relevant parts.
- Convincing argument needed to establish consistency between formal policy model and informal DTLS.



COMP 6370 – Common Criteria and other Certifications



26

A1 - Verified Design

- Functionally equivalent to B3.
- Achieves highest assurance level through use of formal methods.
- Formal specification of policy and system, and consistency proofs show with a high degree of assurance that the TCB is correctly implemented.
- Evaluation for class A1 requires:
 - formal model of the security policy;
 - a formal top level specification (FTLS), including abstract definitions of TCB functions;
 - consistency proofs between model and FTLS (formal, where possible);
 - TCB implementation informally shown to be consistent with FTLS;
 - formal covert channel analysis (informal for timing channels);
 - continued existence of covert channels must be justified and bandwidth limited.



COMP 6370 – Common Criteria and other Certifications



27

Class A1 (continued)

- More stringent configuration management and distribution control (site security acceptance testing) to ensure that version installed is same as (evaluated) master copy.
- Very few products have been evaluated to class A1.
 - Only two network components appear in the list of A1-rated products although there also exist classified products.



COMP 6370 – Common Criteria and other Certifications



28

Interpretations of Orange Book

- Orange Book specifically aimed at Operating Systems.
- Recognised early that evaluations needed for other types of product.
- Hence a series of 'interpretations' of Orange Book produced, showing how to apply Orange Book methodology to other types of product (e.g. databases, networks, ...).



COMP 6370 – Common Criteria and other Certifications



29

Trusted Network Interpretation

- The *Trusted Network Interpretation* ('Red Book') addresses network security using Orange Book concepts and terminology.
- The Red Book is restricted to a limited class of networks, has to address issues which are not present in the Orange Book, and competes to some extent with the OSI Security Architecture (ISO 7498-2).
- Red Book may be viewed as link between Orange Book and newer criteria e.g. ITSEC.
- The Red Book distinguishes between two types of network.
 - Networks of independent components (*interconnected accredited automated information systems*). Enforcing security in such a network is a very difficult problem.
 - Centralised networks (*single trusted systems*) with single accreditation authority, policy, and *network trusted computing base* (NTCB). Only this type of network is covered by Red Book.



COMP 6370 – Common Criteria and other Certifications





30

ITSEC



(Information Technology Security Evaluation Criteria)

- The harmonised European ITSEC were the result of Dutch, English, French & German national security evaluation criteria.
- First draft published in 1990 and ITSEC formally endorsed as Recommendation by the Council of the EU in April 1995.
- ITSEC exists in a number of translations, which adds to the difficulties of interpreting the criteria uniformly.
- ITSEC is logical progression from lessons of various Orange Book interpretations.
- Orange Book too rigid and ITSEC aims to provide a framework for security evaluation that can deal with new sets of security requirements when they arise.
- Functionality and assurance link is broken.
- ITSEC refers to *effectiveness & correctness*.

 COMP 6370 – Common Criteria and other Certifications  31



Security Functionality

- In definition of Orange Book classes there are few indications of rationale for protection mechanisms, their function, and the way they should be implemented.
- ITSEC rectifies this lack. When describing security functionality, you must state:
 - **Security objectives:** Why functionality wanted?
 - **Security functions:** What is actually done?
 - **Security mechanisms:** How is it done?

 COMP 6370 – Common Criteria and other Certifications  32



Assurance of correctness

- Assurance of correctness expressed using seven incremental *evaluation levels*, E0-E6.
- Levels refer to:
 - construction and operation of the TOE,
 - specify documents to be provided by sponsor,
 - actions to be performed by the evaluator.
- Documents and actions refer to:
 - **Development Process:** using a top-down methodology, the security requirements, architectural design, detailed design, and implementation are considered.
 - **Development Environment:** includes configuration control and, from class E2 upwards, developer security, e.g. the confidentiality of evaluation documents.
 - **Operation:** refers to operational documentation for users and administrators, and to the operational environment, including delivery, configuration, start-up, and operation.

 COMP 6370 – Common Criteria and other Certifications  33



Main Features of the evaluation classes

- E0: Inadequate assurance: TOE fails evaluation.
- E1: A security target and informal description of TOE. Testing shows TOE meets security target.
- E2: An informal description of the detailed design. Evidence of testing. Configuration control and controlled distribution process.
- E3: A detailed design and source code for security functions shall be provided.
- E4: Formal model of the security policy required. Rigorous approach and notation for architectural and detailed design needed. Vulnerability analysis based on rigorous approach needed.
- E5: Close correspondence between detailed design and source code have to be established. The vulnerability analysis uses the source code.
- E6: A formal description of the security architecture of the TOE, consistent with the formal model of the security policy, is required. It must be possible to relate portions of the executable form of the TOE to the source code.

 COMP 6370 – Common Criteria and other Certifications  34



Evaluation classes (continued)

- Today, E3 is the most popular evaluation level for commercial security products.
- Secure operating systems or database management systems typically aim for the combination F2+E3.
- DAC is deemed sufficient but higher assurance than given by class C2 is desired.
- Most evaluations done with functionality classes similar to Orange Book classes.

 COMP 6370 – Common Criteria and other Certifications  35

Orange Book - ITSEC correspondence

| Orange Book | ITSEC |
|-------------|-------|
| D | E0 |
| C1 | F1+E1 |
| C2 | F2+E2 |
| B1 | F3+E3 |
| B2 | F4+E4 |
| B3 | F5+E5 |
| A1 | F5+E6 |

 COMP 6370 – Common Criteria and other Certifications  36

Evaluation Assurance Levels

Common Criteria vs. ITSEC vs. Orange Book

| Common Criteria | ITSEC | TCSEC |
|-----------------|-------|-------|
| EAL0 | E0 | D |
| EAL1 | | |
| EAL2 | E1 | C1 |
| EAL3 | E2 | C2 |
| EAL4 | E3 | B1 |
| EAL5 | E4 | B2 |
| EAL6 | E5 | B3 |
| EAL7 | E6 | A |



COMP 6370 – Common Criteria and other Certifications



37