Trusted Computer System Evaluation Criteria (TCSEC)

The Trusted Computer System Evaluation Criteria (1983-1999), better known as the *Orange Book*, was the first major computer security evaluation methodology. The Orange Book was part of a series of books developed by the Department of Defense in the 1980's and called the *Rainbow Series* because of the colorful report covers. The Rainbow Series documented security requirements for such contexts as networks, databases, audit systems, password guidance, and other system components. The emphasis was on confidentiality and the protection of government classified information.

6 Evaluation Classes: D, C1, C2, B1, B2, B3, A1

The TCSEC defines 6 evaluation classes identified by the rating scale from lowest to highest: D, C1, C2, B1, B2, B3, and A1. An evaluated computer product could use the appropriate rating based upon the TCSEC evaluation of that product. Such an evaluated product is called a *rated product*.

Functional Requirements

DAC – identifies an access control mechanism that allows for controlled sharing of names, objects by names, individuals, and/or groups. The requirements also address propagation of access rights, granularity of control, and access control lists.

MAC – embodies the simple security condition and the *-property from the Bell-LaPadula security model. MAC is not required until B1.

Object Reuse – addresses the threat of an attacker gathering information from reusable objects such as memory or disk memory. This also includes the revocation of access rights from a previous owner when the reusable object is released and the inability of a new user to read the previous contents of that reusable object.

Label – enables the enforcement of MAC. This also is not required until B1. Both subjects and objects have labels. Other issues address the accurate representation of classifications and clearances, exporting of labeled information, and labeling of human readable output and devices.

Identification and Authentication (I&A) – specifies that a user identify herself to the system and that the system authenticate that identity before allowing the user to use the system. It also addresses the granularity of the authentication data, protecting authentication data, and the associating identity with auditable actions.

Trusted Path – provides a communication path that is guaranteed to be between the user and the TCB. This is not required until B2.

Audit – addresses the existence of an audit mechanism as well as protection of the audit data. This define what audit records must contain and what events that must be audited.

Additional system architecture requirements and functional requirements are part of the model. Some of the additional requirements include tamperproof reference validation mechanism, process isolation, the principle of least privilege, and well-defined user interfaces. Trusted facility management requires separation of operator and administrator roles at the B2 level.

Assurance Requirements

Configuration Management – begins at B2 and increases for higher levels. This requirement addresses the identification of configuration items, consistent mappings among all documentation and code, and tools for generating the TCB.

Trusted Distribution – addresses the integrity of the mapping between masters and on-site versions of the software as well as acceptance procedures for the customer. This is unique to level A1.

System Architecture – mandates modularity, minimization of complexity, and other techniques for keeping the TCB as small and simple as possible. At level B3 the TCB must be a full reference validation mechanism.

Design Specification and Verification – addresses a large number of individual requirements, which vary among the evaluation classes.

Testing – addresses conformance with claims, resistance to penetration and correction of flaws followed by retesting. A requirement to search for covert channels includes the use of formal methods at higher evaluation levels.

Product Documentation – is divided into a Security Features User's Guide and an administrator guide called a Trusted Facility Manual. Internal documentation includes design and test documentation.

Evaluation Classes

D. Minimal Protection
- No security characteristics
- Evaluated at higher level and failed

C1. Discretionary Protection
- DAC
- Require identification & authentication
- Assurance minimal
- Nothing evaluated after 1986

C2. Controlled Access Protection
- C1 +
- Auditing capable of tracking each individuals access or attempt to each object
- More stringent security testing
- Most OSs at end of the TCSEC incorporated C2 requirements

B1. Labeled Security Protection
- C2 +
- MAC for specific sets of objects
- Each controlled object must be labeled for a security level & that labeling is used to control access
- Security testing requirements more stringent
- Informal security model for both hierarchical levels and non-hierarchical categories
- informal security model shown consistent with its axioms

Note: Most vendors offered B1 systems, but the systems often times fell behind technologically..

B2. Structured Protection
- B1 +
- MAC for all objects
- Labeling expanded
- Trusted path for login
- Requires use of principle of least privilege
- Covert channel analysis
- Configuration management
- Formal model of security policy proven consistent with its axioms

B3. Security Domains
- B2 +
- High-level design – simple
  - Layering
  - Abstraction
  - Information hiding
- Tamperproof security functions
- Increased trusted path requirements
- Significant assurance requirements
- Administrator's guide
- Design Documentation
- DTLS – Descriptive Top Level Specification

A1. Verified Protection
- B3 +
- Assurance
- Formal Methods
  - Covert channel analysis
  - Design specification & verification
- Trusted distribution
- Increased test and design documentation
- FTLS – Formal Top Level Specification

Issues

The TCSEC evaluation methodology had three fundamental problems. They are:

1. Criteria Creep

Gradual expansion of the requirements that define the TCSEC evaluation classes was inevitable. As new products were developed, the criteria needed to be interpreted to apply to those products.

2. Timeless of the Process

Process took too much time

misunderstanding of the depth of the evaluation and the required time

Interactions among the evaluation teams

scheduling problems and misunderstandings about the practice of the evaluation

Evaluation management

free evaluation lead to a lack of motivation

3. Focused on OS

Security issues had expanded beyond operating systems by the 90's