

# Systems Evaluation Methods

❖ *DigitalSherlock.com | SafeHack.com*

❖ *Date: 2005/05/27*

❖ *Document Name: systems\_evaluation\_methods.pdf*

❖ *GNU Free Documentation License*

❖ *Version 1.00, 2005-05-27*

❖ *Copyright © 2005 Adonis, MSc, Eng, CISSP, Security+, CEH, GSec, MCSE, etc.*

❖ *Permission is granted to copy, distribute and/or modify this document under the terms of the GNU Free Documentation License, Version 1.2 or any later version published by the Free Software Foundation.*

## ❖ Orange Book TCSEC

### ➤ Introduction

- **Trusted Computer Security Evaluation Criteria TCSEC**
- **Used to implement a security policy**
- **TCSEC was developed in 1985 by National Computer Security Center (NCSC)**
- **Provide hardware/ firmware/ software security criteria**
- **The orange book address a SINGLE-SYSTEM security**
- **The orange Book looks specifically at the operating system and not other issues like networking and databases, etc..**
- **The orange book focus mainly on one attribute of security CONFIDENTIALITY and not integrity, availability or authenticity**
- **Orange Book Addresses Confidentiality**
- **Orange Book does NOT address Integrity**
- **Each division include the one above it. Example C2 must meet its criteria and all of the C1 criteria**
- **The orange book works with government classifications and not the protection classifications that commercial industries use**
- **The orange book has a relatively small number of ratings, which means many different aspects of security are not evaluated and rated**
- **The orange book Provide associated technical evaluation methodologies**
- **The orange book provide a standard to manufacturers as to what security features to build into their new and planned, commercial products**
- **The orange book provide DoD components with a metric with which to evaluate the degree of trust that can be placed in computer systems**
- **The orange book provide a basis for specifying security requirements in acquisition specifications**
- **The orange book provides a graded classification of systems that is divided into divisions of security levels A, B, C, D**
- **The classification A Represent the highest level of security**
- **Each Division can have one or more numbered classes**
- **The class with higher numbers indicate a greater degree of trust and security**
- **Example B2 is higher than B1, C2 is higher than C1**
- **The orange book looks at these items during evaluation**
  - **The functionality of a system**
  - **The effectiveness of a system**
  - **The assurance of a system**
  - **The functionality during its evaluation**

### ➤ D - Minimal Protection

- **Evaluated but fail to meet requirements**

- **Represent the lowest level of security**
- **Reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class**
- **C - Discretionary Protection (Access Control)**
  - **Does not require security labels**
  - **Deal with discretionary protection (need-to-know)**
  - **Class (C1): Discretionary Security Protection**
    - It requires a separation of users information
    - Is based on individuals and/or groups
    - Security Policy
      - ◆ Discretionary Access Control
    - Accountability
      - ◆ It requires identification and authentication of individual entities
      - ◆ Audit: Security relevant events are audited and these records must be protected from modification
    - Assurance
      - ◆ Operational Assurance
        - System Architecture
        - There must be specific ways of validating the system's operational integrity
      - ◆ Life-Cycle Assurance
        - Security Testing
    - Documentation
      - ◆ Security Features User's Guide
      - ◆ Trusted Facility Manual
      - ◆ Test Documentation
      - ◆ Design Documentation
  - **Class (C2): Controlled Access Protection**
    - Class (C2) systems require all the features required for class (C1).
    - C2 require object reuse protection and auditing
    - Make users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation
    - Security Policy
      - ◆ Discretionary Access Control
      - ◆ Object Reuse concept must be invoked
      - ◆ C2 Controlled access protection introduces the object reuse protection, meaning that any medium holding data must not contain any remnants of information after it is released for another subject to use.
    - Accountability
      - ◆ (C1) It requires identification and authentication of individual entities
      - ◆ Users need to be identified individually to provide more precise access control and auditing
      - ◆ Logical access control mechanisms are used to enforce authentication and the uniqueness of each individual's identification
      - ◆ Audit: Security relevant events are audited and these records must be protected from modification
    - Assurance
      - ◆ Operational Assurance
        - System Architecture
        - There must be specific ways of validating the system's operational integrity
      - ◆ Life-Cycle Assurance
        - Security Testing
    - Documentation
      - ◆ Security Features User's Guide

- ♦ Trusted Facility Manual
- ♦ Test Documentation
- ♦ Design Documentation

➤ **B - Mandatory Protection (Access Control)**

- **Is enforced by the use of Security Labels**
- **Deals with mandatory protection (Security Labels)**
- **It is based on the Bell-LaPadula security model**
- **Class (B1): Labeled Security Protection**
  - The security policy is based on an informal statement
  - It is the first rating that requires security labels
  - Each data object must contain a classification label
  - Each subject must have a clearance label
  - Data leaving the system must contain an accurate security label
  - Security Policy
    - ♦ Discretionary Access Control
    - ♦ Mandatory Access Control
    - ♦ Object Reuse concept must be invoked
  - Accountability
    - ♦ (C1) It requires identification and authentication of individual entities
    - ♦ Users need to be identified individually to provide more precise access control and auditing
    - ♦ Logical access control mechanisms are used to enforce authentication and the uniqueness of each individual's identification
    - ♦ Audit: Security relevant events are audited and these records must be protected from modification
  - Assurance
    - ♦ Operational Assurance
      - System Architecture
      - There must be specific ways of validating the system's operational integrity
    - ♦ Life-Cycle Assurance
      - Security Testing
      - Design Specification and Verification
  - Documentation
    - ♦ Security Features User's Guide
    - ♦ Trusted Facility Manual
    - ♦ Test Documentation
    - ♦ Design Documentation
- **Class (B2): Structured Protection**
  - Class (B2) systems require all the features required for class (B1).
  - Requires security labels on Subjects and devices
  - Data leaving the system must contain an accurate security label
  - Trusted Path: A trusted patch for authentication and logon processes must be in place
  - The system must protect against covert storage channels analysis not covert timing
  - Distinct address spaces must be provided to isolate processes
  - This class adds assurance by adding requirements to the design of the system
  - Trusted Facility Management
  - Configuration Management
  - Documentation
    - ♦ Security Features User's Guide
    - ♦ Trusted Facility Manual
    - ♦ Test Documentation
    - ♦ Design Documentation

- **Class (B3): Security Domains**
  - Class (B3) systems require all the features required for class (B2).
  - The design and implementation should not provide too much complexity
  - B3 requires security notifications to be sent
  - The reference monitor components must be small enough to be tested properly and be tamperproof
  - Protect against both covert storage and covert timing channels B3 and A1
- **A - Verified Design**
  - **Characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information**
  - **A means the system's design and level of protection is verifiable and provides the highest level of security**
  - **Protect against both covert storage and covert timing channels B3 and A1**
  - **Class (A1) are functionally equivalent to those in class (B3)**
  - **Trusted Facility Management - Identify Security Administrator Functions**
  - **Configuration Change Management - Entire System Lifecycle**
  - **Trusted Recovery Required**
  - **Class (A1): Verified Design**
    - Assurance
      - ♦ Operational Assurance
        - System Architecture
        - There must be specific ways of validating the system's operational integrity
      - ♦ Life-Cycle Assurance
        - Security Testing
        - Design Specification and Verification
    - Documentation
      - ♦ Security Features User's Guide
      - ♦ Trusted Facility Manual
      - ♦ Test Documentation
      - ♦ Design Documentation
- **Orange Book -- Criteria**
  - **Topic Security Policy**
    - The policy must be explicit and well defined and enforced by the mechanisms within the system
  - **Topic Identification**
    - Individual subjects must be uniquely identified
  - **Topic Assurance life Cycle**
    - Software, hardware, and firmware must be able to be tested individually to ensure that each each enforces the security policy in an effective manner
  - **Topic Accountability**
    - Audit data must be captured and protected to enforce accountability
  - **Topic Documentation**
    - This includes the test, design, specification documents, user guides and manuals
  - **Topic Continuous Protection**
    - The security mechanisms and the system as a whole must perform predictably and acceptably in different situations continuously

## ❖ **TNI Red Book**

- **Trusted Network Interpretation (TNI)**
- **Published by the U.S. Dept. of Defense to handle issues specific to maintaining a trusted computer network**
- **Address security evaluation topics for Networks and Network components**
- **Address security service that are not addressed in the orange book**
- **RedBook interprets the criteria described in the Orange Book**
- **The red book does not supply specific details about how to implement security mechanisms, instead, it provides a framework for securing different types of networks**
- **The red book rates confidentiality and integrity of data**
- **Data and Labels need to be protected from unauthorized modification**
- **Integrity of information as it is transferred needs to be ensured**
- **The source and destination mechanisms used for messages are evaluated and tested**
- **Encryption and protocols provide security within a network and need to be evaluated and tested**
- **Security Items addressed in the Red Book**
  - **Communication Integrity**
    - Authentication
      - ◆ Protect against masquerading and playback attacks
      - ◆ Mechanisms include Digital Signatures, Encryption, Timestamp, and passwords
    - Message Integrity
      - ◆ Protects protocol header, routing information, packet payload from being modified
      - ◆ Mechanisms include Message authentication and encryption
    - Non-Repudiation
      - ◆ Ensure that a sender cannot deny sending a message
      - ◆ Mechanisms include encryption, digital signatures, and notary
  - **Denial of Service Prevention**
    - Continuity of operations
    - Network Management
  - **Compromise Protection**
    - Data Confidentiality
    - Traffic Flow Confidentiality
    - Slective Routing
- **Classes**
  - **D: Minimal Protection**
  - **C: Dicretionary Protection**
  - **C1: Dicretionary security Protection**
  - **C2: Controlled Access Protection**
  - **B: Mandatory Protection**
  - **B1: Labeled security Protection**
  - **B2: Structured Protection**
  - **B3: Security Domains**

## ❖ **ITSEC**

- **Introduction**

- **Information Technology Security Evaluation Criteria (ITSEC)**
- **Created by Germany, France, UK, and Netherlands**
- **Version 1 published in June 1990**
- **It does not specify IT security requirements**
- **Provides a framework within which specific IT security requirements can be defined**
- **IT is only used in Europe not Internationally**
- **Under ITSEC approach the functionality is rated separately from the assurance**
- **ITSEC is a criteria for both security products and security systems and refers to both as the TARGET of EVALUATION (TOF)**

➤ **It defines 2 Main attribute**

- **Functionality**
  - When functionality is evaluated it is tested to see if the system delivers what it says it delivers
  - They are technical security features (referred to as "Security Enforcing Functions")
  - They are implemented in IT to support C.I.A
  - Examine and Evaluate
    - ♦ Access Control
    - ♦ Auditing
    - ♦ Authentication
    - ♦ So on...
  - ITSEC Functionality Classes
    - ♦ F1, F2, F3, F4, F5, F6, F7, F8, F9, F10
    - ♦ F1+E=C1
    - ♦ F2+F2=C2
    - ♦ F3+E3=B1
    - ♦ F4+E4=B2
    - ♦ F5+E6=A1
    - ♦ F6 = Systems that provide high integrity
    - ♦ F7 = Systems that provide high availability
    - ♦ F8 = Systems that provide data integrity during communication
    - ♦ F9 = Systems that provide high confidentiality
    - ♦ F10 = Networks with high demands on confidentiality and integrity
- **Assurance**
  - Provide confidence on how well the functionality has been implemented
  - Assurance is the degree of confidence in a security component and its effectiveness
  - Assurance is tested by examining development practices, documentation, configuration management and testing mechanisms
  - ITSEC considers assurance to be a combination of correctness & effectiveness
  - ITSEC Assurance Classes
    - ♦ E0, E1, E2, E3, E4, E5, E6
    - ♦ E0 is the lowest

## ❖ **The "Common Criteria"**

- **Derived from both the TCSEC and ITSEC efforts**
- **Framework for specifying new security requirements**
- **Enhance existing development and evaluation criteria while preserving their fundamental principles**
- **The Common Criteria was developed to address the shortcomings of other evaluation systems**

- Its rating is called the evaluation assurance level (EAL) and uses protection profiles to evaluate products
- A protection profile contains the following
  - Descriptive Elements - name of profile and a description of the security problem to be solved
  - Rationale - justification of the profile and a more detailed description of the protection problem to be solved
  - Functional Requirements - protection boundary is established, meaning that threats or compromises that were within this boundary could be countered
  - Development Assurance Requirements - the development phases from design to implementation have specific requirements that the product or system must meet
  - Evaluation Assurance Requirements - establishes the type and intensity of the evaluation

### ❖ Certification vs. Accreditation

- Certification - the technical evaluation of the security components and their compliance for the purpose of accreditation
- Accreditation - the formal acceptance of the adequacy of a system's overall security by management

### ❖ Open Systems vs. Closed Systems

- Open Systems - systems that have an architecture that has published specifications which enables third party vendors to develop add-on components and devices
- Closed Systems - systems that use an architecture that does not follow industry standards

### ❖ Threats to Security Models and Architecture

- Covert Channels
  - A way for an entity to receive information in an unauthorized manner
  - Information flow that is not controlled by a security mechanism
  - 2 Types
    - Covert timing channel - one process relays information to another by modulating its use of system resources
    - Covert storage channel - when a process writes data to a storage location and another process directly, or indirectly, reads it
- Back Doors
  - Also called maintenance hooks
  - Instructions within software that only the developer knows about and can invoke
- Timing Issues
  - Also called asynchronous attacks
  - Deals with the timing difference of the sequence of steps a system uses to complete a task
  - Race conditions
- Buffer Overflows
  - When programs do not check the length of data that is inputted into a program and then processed by the CPU

### ❖ Security Modes Of Operation

- **The mode of operation describes the security conditions under which the system functions**
- **Dedicated Security Mode**
  - All users have the clearance or authorization and need-to-know to all data processed within the system
  - The system can handle a SINGLE classification level of information
  - Many old military systems were designed to handle one level of security
- **System-High Security Mode**
  - All users have the clearance or authorization but not necessarily the need-to-know for all data processed within the system
  - This mode requires all users to have the highest level of clearance required by any and all data on the system
- **Compartmented Security Mode**
  - Enable the system to process data classified at different classification levels
  - This type of systems can support users with high and low clearances simultaneously
  - All users have the clearance but not necessarily the need-to-know for all data processed within the system
  - Compartmented Mode Workstation (CMW) enable users to process multiple compartments of data at the same time, if they have the necessary clearance
  - Information Lables contain more information than sensitivity Lables, but are not used by the reference monitor to determine access permissions
- **Multilevel Security Mode**
  - Enable the system to process data classified at different classification levels
  - It permits two or more classification levels of information to be processed at the same time when all users do not have clearance or formal approval to access all the information being processed
  - The Bell-Lapadula is an example

## ❖ **Trusted Computing Base**

- **The term originated from the Orange Book**
- **IT does not address the level of security a system provides, but the level of TRUST**
- **The TCB addresses hardware, software, components and firmware**
- **The trusted computing base is the total combination of protection mechanisms within a computer system, with the security perimeter being the boundary of the trusted computing base**
- **Not all system components fall under the TCB only those that enforce the security policy directly need to be**
- **The components that fall under the TCB are within the security perimeter**
- **TCB contains the security kernel and all other security protection mechanisms**
- **Trust means that a system uses all its protection mechanisms properly to process sensitive data for many type of users**
- **Assurance is the level of confidence you have in this trust and that the protection mechanisms behave properly in all circumstances**
- **Reference Monitor**

- **Reference monitor** - abstract machine which mediates all access subjects have to objects to ensure that the subjects have the necessary access rights and to protect the objects from unauthorized access and destructive modification
- **Example:** Law act like a reference monitor by enforcing rules
- **Example**
  - Individuals = Components
  - Society - Kernel
  - Laws = Reference monitor
- **Security Kernel**
  - **Security kernel** - made up of mechanisms that fall under the TCB and enforces the reference monitor concept
  - **The three requirements**
    - Must provide isolation for the processes carrying out the reference monitor concept and they must be tamperproof
    - The reference monitor must be invoked for every access attempt and must be impossible to circumvent
    - Must be small enough to be able to be tested and verified in a complete and comprehensive manner

## ❖ Other Components

- **Introduction**
  - **Security mechanisms can be placed at the hardware, kernel, operating system, services, or programs layers**
  - **If the protection is implemented at the hardware layer, the protection mechanisms will be simplistic**
  - **The more complex a security mechanism becomes, the less assurance it provides**
- **Security Perimeter**
  - **A security perimeter is an imaginary boundary that has trusted components within it and untrusted components on the outside of the boundary**
- **Resource Isolation**
  - **Processes need to be isolated which can be done through segmented memory addressing**
  - **Resource Isolation** - separating resources logically to prevent processes from accessing resources that are to be used for another process
  - **Hardware segmentation involves separating these resources physically instead of logically**
- **Security Policy**
  - **Security Policy** - set of rules, practices, and procedures dictating how sensitive information is managed, protected, and distributed
  - **A system can have the exact same hardware software but provide different levels of protection because of the different security policies and security Models**
  - **A security policy is a set of rules that dictate how sensitive data is to be managed protected and distributed**
  - **A multilevel security system processes data at different classifications, and users with different clearances can use the system**
  - **A multilevel security policy** - policies that prevent information from flowing from a high security level to a lower security level
- **Least Privilege**
  - **Processes should be assigned least privilege**

- **Least Privilege** - a subject has no more privilege than necessary to perform its function

➤ **Layering**

- Some systems provide functionality at different layers of the system, which is called layering
- Layering separates the processes and provides more protection for them individually
- Layering - separates processes at different levels and they can communicate only through detailed interfaces which uphold the security of the system

➤ **Data Hiding**

- Data Hiding - data in one "layer" is hidden so that processes in other layers do not even know it exists
- Data hiding provides more protection for the data

➤ **Abstraction**

- Abstraction - when a class of objects is assigned specific permissions and acceptable activities are defined