

# Orange Book

- ❖ *DigitalSherlock.com | SafeHack.com*
- ❖ *Date: 2005/05/27*
- ❖ *Document Name: orange\_book.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.*

## ❖ Introduction

### ➤ TCSEC

- **Trusted Computer System Evaluation Criteria (TCSEC) Orange Book**
- **Originally published in 1983 & revised in 1985**
- **"TCSEC was introduced in 1985 and retired in December 2000(...) TCSEC**
- **Was finally replaced with the Common Criteria"**
- **Address IT security issues within DoD**

### ➤ Purpose

- **Provide hardware/ firmware/ software security criteria**
- **Provide associated technical evaluation methodologies**
- **To provide a standard to manufacturers as to what security features to build into their new and planned, commercial products**
- **To provide DoD components with a metric with which to evaluate the degree of trust that can be placed in computer systems**
- **To provide a basis for specifying security requirements in acquisition specifications**

### ➤ Criteria are intended to be application-independent

### ➤ Two types of requirements are delineated for secure processing

- **Specific security feature requirements**
- **Assurance requirements**

### ➤ Fundamental Computer Security Requirements

- **Six fundamental requirements are derived from this basic statement of objective**
- **Four deal with what needs to be provided to control access to information**
  - SECURITY POLICY
  - MARKING
  - ACCOUNTABILITY
  - IDENTIFICATION
- **Two deal with how one can obtain credible assurances that this is accomplished in a trusted computer system**
  - ASSURANCE
  - CONTINUOUS PROTECTION

## ❖ Acronyms

- **Automatic Data Processing (ADP)**
- **The Trusted Computing Base (TCB)**
- **Formal top-level specification (FTLS)**

## ❖ PART I: THE CRITERIA

### ➤ Division D: MINIMAL

- **Reserved for those systems that have been evaluated but that fail to meet the**

requirements for a higher evaluation class

➤ **Division C: DISCRETIONARY**

• **Class (C1): Discretionary Security Protection**

- Providing separation of users and data
- Minimal requirements for systems class (C1)
- Security Policy
  - ♦ Discretionary Access Control
- Accountability
  - ♦ Identification and Authentication
- Assurance
  - ♦ Operational Assurance
    - System Architecture
    - System Integrity
  - ♦ Life-Cycle Assurance
    - Security Testing
- Documentation
  - ♦ Security Features User's Guide
  - ♦ Trusted Facility Manual
  - ♦ Test Documentation
  - ♦ Design Documentation

• **Class (C2): Controlled Access Protection**

- Security Policy
  - ♦ Discretionary Access Control
  - ♦ Object Reuse
- Accountability
  - ♦ Identification and Authentication
  - ♦ Audit
- Assurance
  - ♦ Operational Assurance
    - System Architecture
    - System Integrity
  - ♦ Life-Cycle Assurance
    - Security Testing
- Documentation
  - ♦ Security Features User's Guide
  - ♦ Trusted Facility Manual
  - ♦ Test Documentation
  - ♦ Design Documentation
- 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.

➤ **Division B: MANDATORY**

• **Class (B1): Labeled Security Protection**

- Class (B1) systems require all the features required for class (C2).
- Security Policy
  - ♦ Discretionary Access Control
  - ♦ Object Reuse
  - ♦ Labels
    - Exportation of Labeled Information
      - Exportation to Multilevel Devices
      - Exportation to Single-Level Devices

- Labeling Human-Readable Output
  - ♦ Mandatory Access Control
- Accountability
  - ♦ Identification and Authentication
  - ♦ Audit
- Assurance
  - ♦ Operational Assurance
    - System Architecture
    - System 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**
  - The system must protect against covert storage channels.
  - It must perform covert channel analysis for all covert storage channels
  - Requires the discretionary and mandatory access control enforcement found in class (B1)
  - Cover covert channels are addressed
  - Security Policy
    - ♦ Discretionary Access Control
    - ♦ Object Reuse
    - ♦ Labels
      - Label Integrity
      - Exportation of Labeled Information
        - Exportation to Single-Level Devices
        - Labeling Human-Readable Output
      - Subject Sensitivity Labels
      - Device Labels
    - ♦ Mandatory Access Control
  - Accountability
    - ♦ Identification and Authentication
      - Trusted Path
    - ♦ Audit
  - Assurance
    - ♦ Operational Assurance
      - System Architecture
      - System Integrity
      - Covert Channel Analysis
      - Trusted Facility Management
    - ♦ Life-Cycle Assurance
      - Security Testing
      - Design Specification and Verification
      - Configuration Management
  - Documentation
    - ♦ Security Features User's Guide
    - ♦ Trusted Facility Manual
    - ♦ Test Documentation

- ◆ Design Documentation
- **Class (B3): Security Domains**
  - All accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests
  - Security Policy
    - ◆ Discretionary Access Control
    - ◆ Object Reuse
    - ◆ Labels
      - Label Integrity
      - Exportation of Labeled Information
        - Exportation to Multilevel Devices
        - Exportation to Single-Level Devices
        - Labeling Human-Readable Output
      - Subject Sensitivity Labels
      - Device Labels
    - ◆ Mandatory Access Control
  - Accountability
    - ◆ Identification and Authentication
      - Trusted Path
    - ◆ Audit
  - Assurance
    - ◆ Operational Assurance
      - System Architecture
      - System Integrity
      - Covert Channel Analysis
      - Trusted Facility Management
      - Trusted Recovery
    - ◆ Life-Cycle Assurance
      - Security Testing
      - Design Specification and Verification
      - Configuration Management
  - Documentation
    - ◆ Security Features User's Guide
    - ◆ Trusted Facility Manual
    - ◆ Test Documentation
    - ◆ Design Documentation
  - Protect against both covert storage and convert timing channels B3 and A1
- **Division A: VERIFIED**
  - **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**
  - **Reserved for systems providing the most comprehensive security**
  - **Class (A1): Verified Design**
    - Protect against both covert storage and convert timing channels B3 and A1
    - Class (A1) are functionally equivalent to those in class (B3)
    - There are five important criteria for class (A1) design verification
    - Security Policy
      - ◆ Discretionary Access Control
      - ◆ Object Reuse
      - ◆ Labels
        - Label Integrity

- Exportation of Labeled Information
  - Exportation to Multilevel Devices
  - Exportation to Single-Level Devices
  - Labeling Human-Readable Output
- Subject Sensitivity Labels
- Device Labels
- ◆ Mandatory Access Control
- Accountability
  - ◆ Identification and Authentication
  - ◆ Audit
- Assurance
  - ◆ Operational Assurance
    - System Architecture
    - System Integrity
    - Covert Channel Analysis
    - Trusted Facility Management
    - Trusted Recovery
  - ◆ Life-Cycle Assurance
    - Security Testing
      - Design Specification and Verification
      - Configuration Management
      - Trusted Distribution
- Documentation
  - ◆ Security Features User's Guide
  - ◆ Trusted Facility Manual
  - ◆ Test Documentation
  - ◆ Design Documentation
- **Beyond Class (A1) Areas to be addressed**
  - System Architecture
  - Security Testing
  - Formal Specification and Verification
  - Trusted Design Environment

➤ **We Have 4 Divisions**

➤ **Within divisions C and B A we have Class**

➤ **Within each class, four major sets of criteria are addressed**

➤ **The first three cover Security Policy, Accountability, and Assurance**

➤ **The fourth set cover Documentation**

## ❖ **PART II: RATIONALE AND GUIDELINES**

➤ **CONTROL OBJECTIVES FOR TRUSTED COMPUTER SYSTEMS**

- **The criteria are divided within each class into groups of requirements**
- **These groupings were developed to assure that three basic control objectives for computer security are satisfied**
  - Security Policy
  - Accountability
  - Assurance
- **A Need for Consensus**
- **Definition and Usefulness**
  - Examples of control objectives include the three basic design requirements

- ♦ The reference validation mechanism must be tamperproof.
- ♦ The reference validation mechanism must always be invoked.
- ♦ The reference validation mechanism must be small enough to be subjected to analysis and tests

- **Criteria Control Objective**

- Security Policy
  - ♦ Mandatory Security Policy
  - ♦ Discretionary Security Policy
  - ♦ Marking
- Accountability
- Assurance

- **RATIONALE BEHIND THE EVALUATION CLASSES**

- **The Reference Monitor Concept**

- A. The reference validation mechanism must be tamper proof.
- B. The reference validation mechanism must always be invoked.
- C. The reference validation mechanism must be small enough to be subject to analysis and tests

- **A Formal Security Policy Model**

- **The Trusted Computing Base**

- **Assurance**

- **The Classes**

- **THE RELATIONSHIP BETWEEN POLICY AND THE CRITERIA**

- **Established Federal Policies**
- **DoD Policies**
- **Criteria Control Objective For Security Policy**
- **Criteria Control Objective for Accountability**
- **Criteria Control Objective for Assurance**

- **A GUIDELINE ON COVERT CHANNELS**

- **A GUIDELINE ON CONFIGURING MANDATORY ACCESS CONTROL FEATURES**

- **A GUIDELINE ON SECURITY TESTING**

- **Testing for Division A**
- **Testing for Division B**
- **Testing for Division C**