Lessons from the Orange Book

David Frier
RSS Oct 2, 2019

Agenda

Who is this guy?

What is he on about?

What are the lessons?

Who is this guy?

David C Frier, CISSP, CISM, CRISC, CCSK, AWS-CCP

Cybersecurity Dir. / Principal Consultant for Wipro at Xerox *...but I speak only for myself, not for Wipro!*

I’ve been doing Information Security for fourteen years* and IT of one sort or another for two score

Avid player of poker and Ingress, enthusiastic-if-slow rider of a Trek.

$FIRST.$LAST@{gmail|wipro|xerox}.com -- also now findable on LinkedIn

What is he on about

The Orange Book - History & Origins

Genealogy - ancestors & descendants

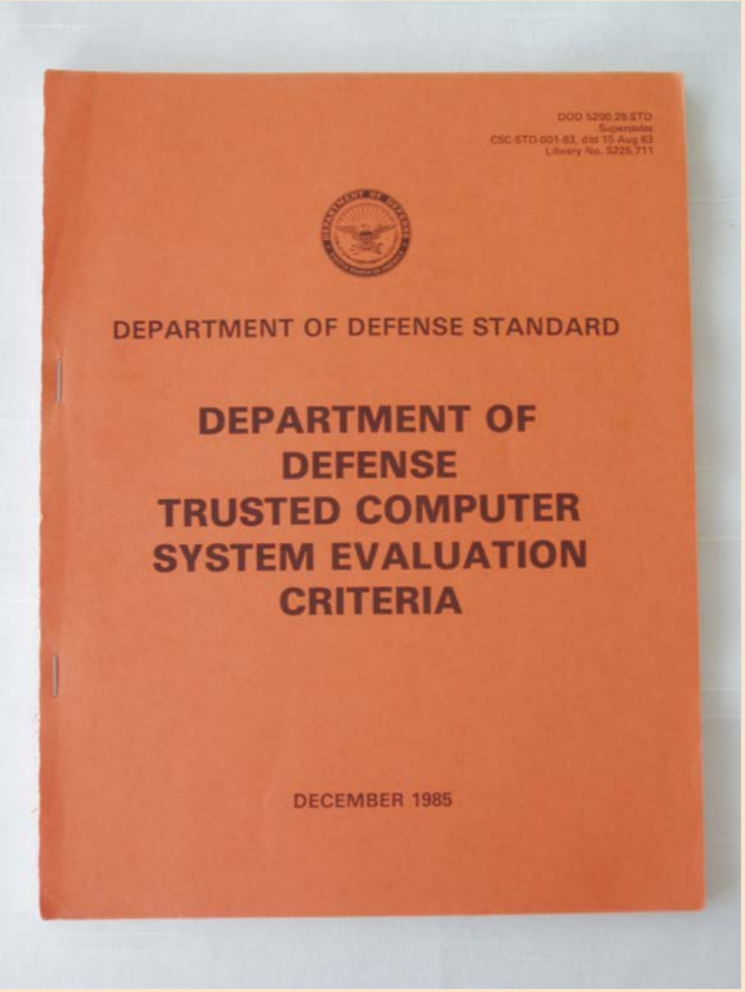
What it covers

What is the Orange Book?

Developed by the NSA

Intended to help DoD and others who needed it to purchase “ADP Systems” that would treat sensitive information properly

Originally part of the “Rainbow Series” put out by the National Computer Security Center



DOD 5200.28-STD
Supersedes
CSC-STD-001-83, dtd 15 Aug 83
Library No. S225,711

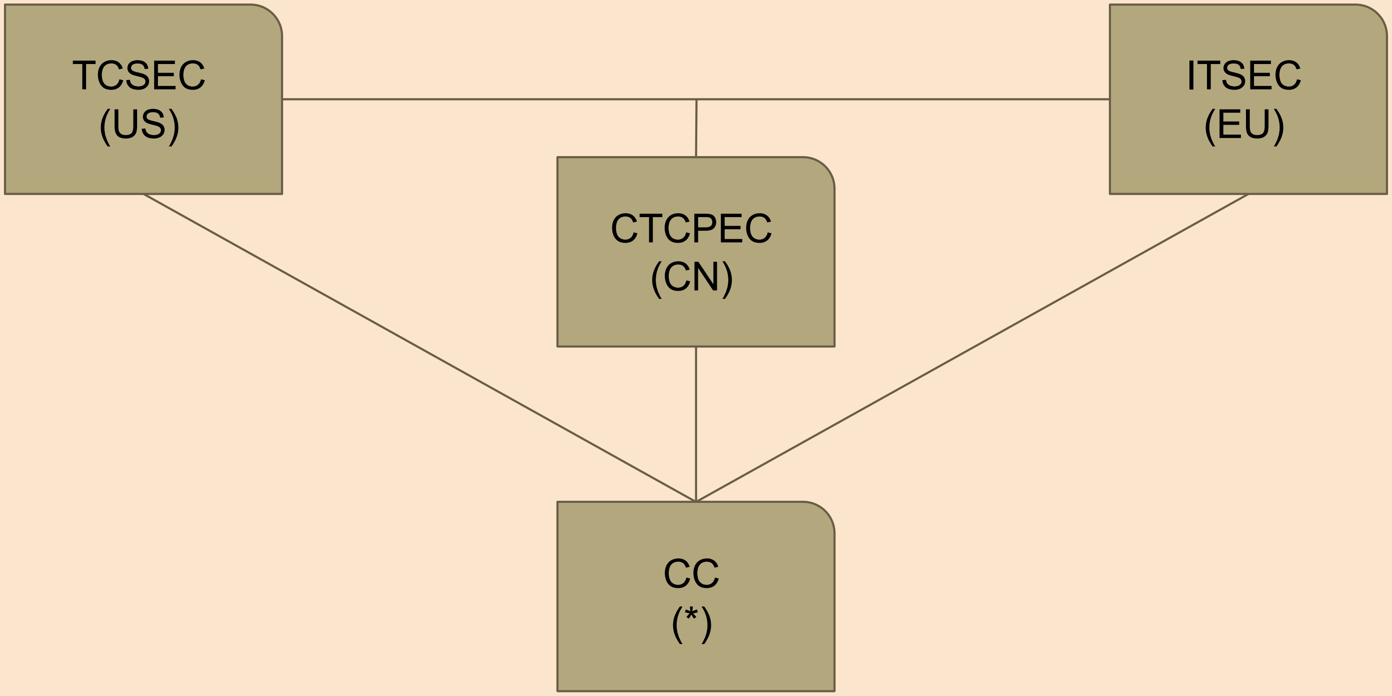
DEPARTMENT OF DEFENSE STANDARD

DEPARTMENT OF
DEFENSE
TRUSTED COMPUTER
SYSTEM EVALUATION
CRITERIA

DECEMBER 1985

DEPARTMENT OF DEFENSE STANDARD
DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA
DECEMBER 1985
DEPARTMENT OF DEFENSE
PASSWORD MANAGEMENT
GUIDELINE
COMPUTER SECURITY REQUIREMENTS
GUIDANCE FOR APPLYING THE DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA IN SPECIFIC ENVIRONMENTS
TECHNICAL RATIONALE BEHIND CSC-STD-003-85: COMPUTER SECURITY REQUIREMENTS
GUIDANCE FOR APPLYING THE DEPARTMENT OF DEFENSE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA IN SPECIFIC ENVIRONMENTS
NATIONAL COMPUTER SECURITY CENTER
NCSC-TG-011 VERSION-1
NCSC-TG-010 VERSION-1
NCSC-TG-009 VERSION-1
NCSC-TG-004 VERSION-1
NCSC-TG-003 VERSION-1
NCSC-TG-001 VERSION-2
NCSC-TG-006 VERSION-1
NCSC-TG-021 VERSION-1
NCSC-TG-020-A VERSION-1
NCSC-TG-019 VERSION-1
NCSC-TG-017 VERSION-1
NCSC-TG-016 VERSION-1
NCSC-TG-015 VERSION-1
NCSC-TG-027 VERSION-1
NCSC-TG-024 VOLUME 2/4 VERSION-1
A GUIDE TO UNDERSTANDING AUDIT IN TRUSTED SYSTEMS
1 June 1988
A GUIDE TO UNDERSTANDING CONFIGURATION MANAGEMENT IN TRUSTED SYSTEMS
Guidelines for Formal Verification Systems

Family Tree



What is covered?

Four Divisions:

- D - Minimal Protection
- C - Discretionary Protection
    - Classes: C1, C2
- B - Mandatory Protection
    - Classes: B1, B2, B3
- A - Verified Protection
    - Classes: A1, “Beyond A1”

What's in it for us?

- Discretionary Controls
  - Owner or anyone with permission to change permissions...
  - Assigns permissions to others...
  - Who can then change permissions...
  - *Ad breachium*

- Mandatory Controls
  - Every user has a "label" consisting of:
    - A classification level (hierarchical controls)
    - A set of categories (non-hierarchical controls)
  - Every file, channel or data item has the same type of label

What shall we do with the label?

- For reading:
  - A subject *(user or process)*'s label must "**dominate**" the label of the object they seek to read.
    - The classification level of the user must be ≥ the level of the object
    - Every category in the object's list must appear in the subject's

- For writing
  - A subject's label must **be dominated by** the label of the object they seek to write.
    - The classification level of the user must be ≤ the level of the object
    - Every category in the subject's list must appear in the object's

Every CISSP in here just groaned a little

Mandatory means Mandatory

- Labels are immutable
  - The subject cannot change their own label, nor the label of any object
  - Objects are created with the label of the subject creating them

- Labels are checked at every use
  - Subjects may reduce their level or drop categories during execution
  - …but lose access immediately to anything their new label does not allow

Progression - B1 Labeled Security

- Discretionary
  - Enforced by the TCB
  - No re-use of resources from system
- Mandatory
  - Labels maintained, enforced by TCB
  - Multiple Levels supported by one TCB
- Audit/Accountability
  - TCB to require Identification and to keep audit trail untampered
  -

- Assurance
  - TCB runs in separate execution domain
- Life Cycle
  - Testing results and
  - Informal statement of design principles
- Documentation
  - User and facility guides

Progression - B2 Structured Protection

- Discretionary:
  - Enforced by the TCB
  - No re-use of resources from system
- Mandatory
  - Labels maintained, enforced by TCB
  - Multiple Levels supported by one TCB
- Audit/Accountability
  - TCB to require Identification and to keep audit trail untampered
  - Audit to enable covert channel detection
  - Trusted communications path for login
- Assurance
  - TCB runs in separate execution domain
  - UI to TCB must be completely defined
- Life Cycle
  - Testing results
  - **F**ormal statement of design principles
- Documentation
  - User and facility guides
  - Full design documentation

Progression - B3 Security Domains

- Discretionary:
  - Enforced by the TCB
  - No re-use of resources from system
  - Ability to build “deny” list
- Mandatory
  - Labels maintained, enforced by TCB
  - Multiple Levels supported by one TCB
  - Immediate notification of level change
- Audit/Accountability
  - TCB to require Identification and to keep audit trail untampered
  - Audit to enable covert channel detection
  - Isolated, trusted communications path for login
- Assurance
  - TCB runs in separate execution domain
  - UI to TCB must be completely defined
  - Covert channel analysis
- Life Cycle
  - Testing results
  - **F**ormal statement of design principles
  - TCB tested against DoS and pen-tested
- Documentation
  - User and facility guides
  - Formal design specification
  - Bandwidth of residual covert channels

Lessons from the Orange Book

Control Objectives as Product Requirements

Formal Models as Design Principles

Security Policy as a Purchasing Criterion

Covert Channel Analysis as a Reporting Requirement

Mandatory Access Controls: where have they gone?

Testing as a Requirement

* Epilogue