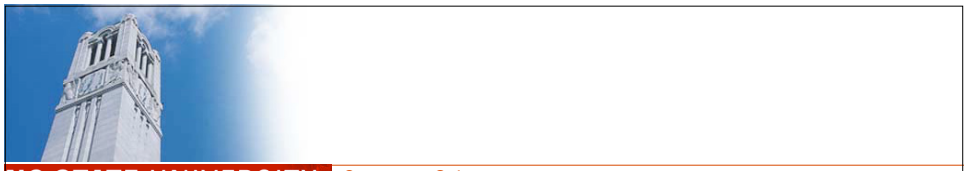


NC STATE UNIVERSITY Computer Science

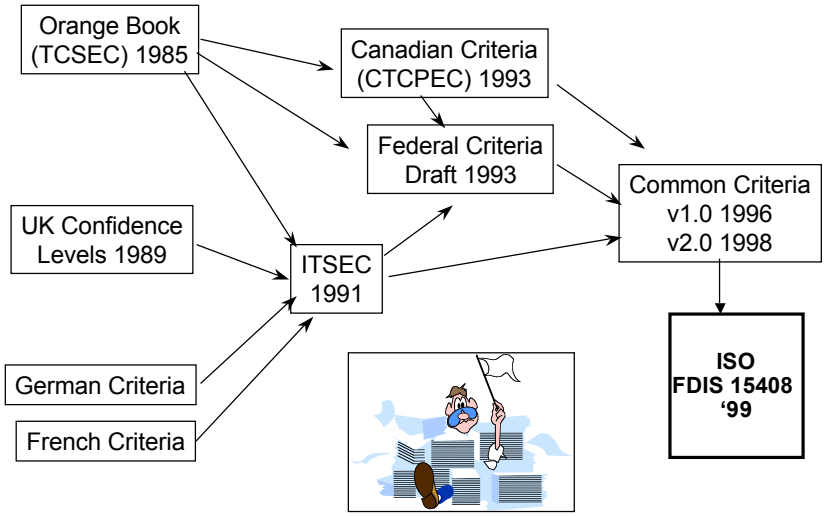
CSC 474/574
Information Systems Security

Topic 6.3: Evaluation of Secure Information Systems

What are Security Criteria?

- (User view) A way to define Information Technology (IT) security requirements for some IT products:
  - Hardware
  - Software
  - Combinations of above
- (Developer view) A way to describe security capabilities of their specific product
- (Evaluator view) A tool to measure the confidence we may place in the security of a product.

History of IT Security Criteria



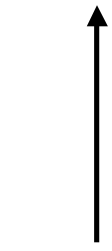
Trusted Computer System Evaluation Criterion ("The Orange Book")

- Issued under authority of an in accordance with DoD Directive 5200.28, Security Requirements for Automatic Data Processing (ADP) Systems
- Purpose is to provide technical hardware/firmware/software security criteria and associated technical evaluation methodologies in support of overall ADP system security policy, evaluation and approval/accreditation responsibilities promulgated by DoD

Fundamental Computer Security Requirements

- What it really means to call a computer system "secure"
- Secure systems control access to information
  - Only properly authorized individuals, or processes operating on their behalf may:
    - Read
    - Write
    - Create
    - Delete
- Two sets of requirements:
  - Four deal with what needs to be provided to control access to information
  - Two deal with how one can obtain credible assurances that this is accomplished in a trusted computer system

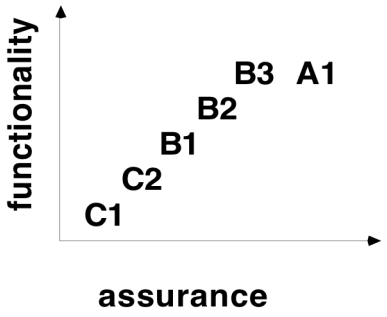
Orange Book Classes



- A1 Verified Design
- B3 Security Domains
- B2 Structured Protection
- B1 Labeled Security Protection
- C2 Controlled Access Protection
- C1 Discretionary Security Protection
- D Minimal Protection

Functionality v. Assurance

- **functionality is multi-dimensional**
- **assurance has a linear progression**



Orange Book Classes — Unofficial View

- C1, C2 Simple enhancement of existing systems. No breakage of applications
- B1 Relatively simple enhancement of existing systems. Will break some applications.
- B2 Relatively major enhancement of existing systems. Will break many applications.
- B3 Failed A1
- A1 Top down design and implementation of a new system from scratch

NCSC Rainbow Series — Selected Titles

- Orange Trusted Computer System Evaluation Criteria
- Yellow Guidance for Applying the Orange Book
- Red Trusted Network Interpretation
- Lavender Trusted Database Interpretation

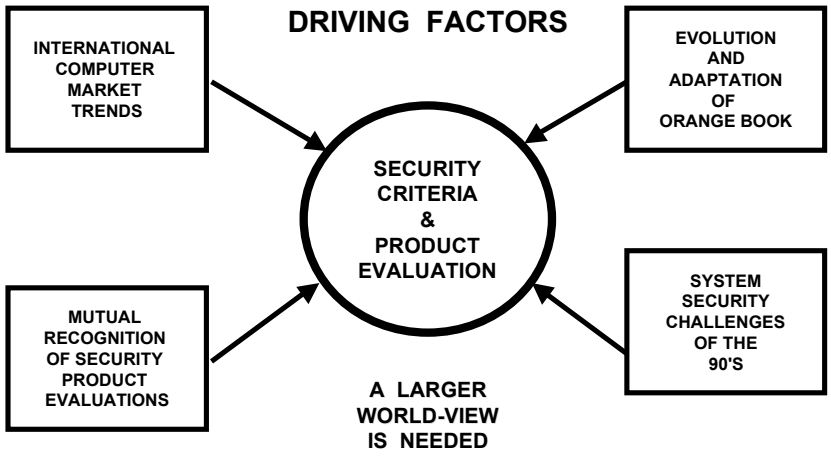
Orange Book Criticisms

- Mixes various levels of abstraction in a single document
- Does not address integrity of data
- Combines functionality and assurance in a single linear rating scale
  - They are indeed other combinations.

International Criteria

ORANGE BOOK	More Flexibility in Application to Non-Military Use Broader Functionality Broader Assurance
ITSEC	Address Functionality Directly Broader Assurance
CTCPEC	Broader Functionality Broader Assurance

Why New International Criteria?



CC Project

- In Spring 1993, the following governments agreed to develop a "Common Information Technology Security Criteria"
  - Canada
  - France
  - Germany
  - Netherlands
  - UK
  - USA - NIST and NSA
- Objectives
  - Common evaluation methodology
  - Mutual recognition

CC

- Three major drafts
  - v0.6 - circulated for comments by a limited audience in 4/94
  - v0.9 - Published in 11/94 for public review
  - v0.1 - More definitive version in 2/96 for trial use
- CC Version 2.0
  - Accepted as an International Standards Organization (ISO) security standard in 5/98 (ISO International Standard 15408)
  - US, Canada, France, Germany, and UK officially agreed on mutual recognition in 10/98

Common Criteria (CC)

- Part 1: Introduction and General Model
  - Terminology, derivation of requirements and specifications, PP & ST Normative
- Part 2: Security Functional Requirements
  - Desired information technology security behavior
- Part 3: Security Assurance Requirements
  - Measures providing confidence that the security functionality is effectively and correctly implemented.

Within Scope of CC

- Basis for evaluation of security properties of IT products and systems
- Allows independent evaluations to be compared
- Addresses protection of information from
  - unauthorized disclose (confidentiality)
  - modification (integrity),
  - loss of use (availability)
- Applicable to IT security measures implemented in HW, SW, and firmware.

Outside Scope of CC

- Administrative and legal application of CC
- Administrative security measures
- Physical aspects of IT security
- Evaluation methodology
- Mutual recognition arrangements
- Cryptographic algorithms
- Accreditation & certification processes

Terminology

- Protection profile (PP)
- Security target (ST)
- Target of evaluation (TOE)

Protection Profile

- Answer the question:
  - "This is what I want or need."
- Implementation independent
- Protection profile authors:
  - Anyone who wants to state IT security needs (e.g., commercial consumer, consumer groups)
  - Anyone who supplies products which support IT security needs
  - Others (security officers, auditors, accreditors, etc.)

Security Target

- Answer the question:
  - "This is what I have."
- Implementation dependent
- Security target authors
  - Product vendors
  - Product developers
  - Product integrators

PP and ST Examples

- PP makes a statement of implementation independent security needs
  - A *generic* OS with DAC, audit, identification and authentication
- ST defines the implementation dependent capabilities of a *specific* product
  - Microsoft NT 4.0.02 (TOE)
  - Sun OS 4.7.4 (TOE)

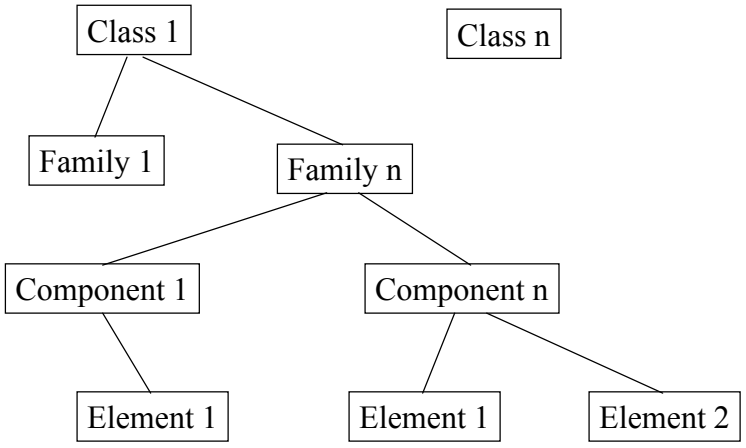
Security Functional Requirements

- Security functional requirements describe the security behavior expected of a TOE and they meet the security objectives as stated in a PP or ST
- Their behavior can generally be observed.

Functional Requirement Classes

- Security Audit (FAU)
- Communication (FCO)
- Cryptographic Support (FCS)
- User Data Protection (FDP)
- Identification & Authentication (FIA)
- Security Management (FMT)
- Privacy (FPR)
- Protection of the TOE Security Functions (FPT)
- Resource Utilization (FRU)
- TOE Access (FTA)
- Trusted Path (FTP)

Security Functional Requirements Organization



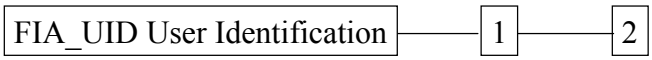
Definitions

- Class – for organizational purposes; all members share a common focus
  - e.g., audit
- Family – for organizational purposes; all members share security objectives but may differ in emphasis
  - e.g., audit event definition, audit event review
- Component – contains a set of security requirements.
  - A component is the smallest selectable requirement set.
- Element – members of a component.
  - Elements cannot be selected individually.

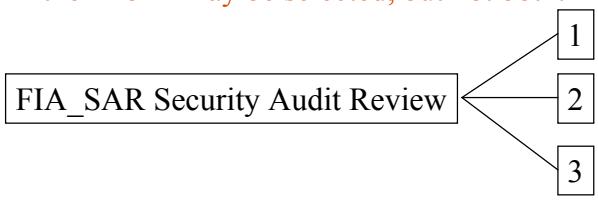
Component Hierarchy

- Each family contains one or more components
- The relationship between components can be either
  - No relationship, or
  - A hierarchical relationship
- A hierarchical component
  - Can satisfy a dependency on the component it is hierarchical to
  - May provide more security than a component it is hierarchical to
- Hierarchical components are not selected together.

Component Hierarchy Examples



Component 2 is hierarchical to component 1. Either 1 or 2 may be selected, but not both.



There are no hierarchical relationship between components 1, 2, and 3. Any combination of them may be selected.

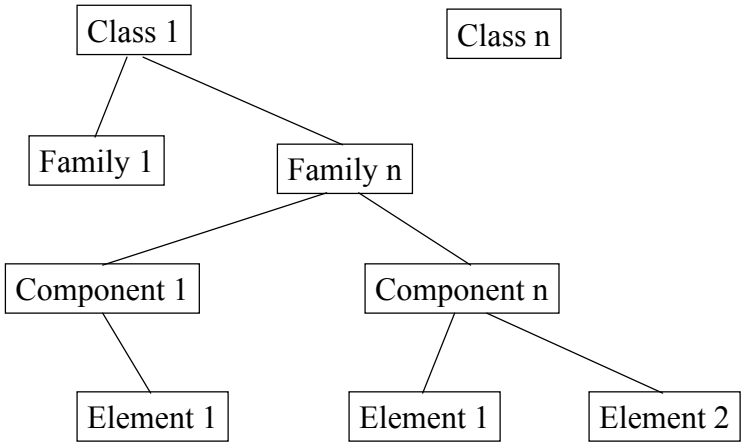
Security Assurance Requirements

- Grounds for confidence that an IT product or system meets its security objectives.

Assurance Requirement Classes

- Configuration Management (ACM)
- Delivery and operation (ADO)
- Development (ADV)
- Guidance documents (AGD)
- Life cycle support (ALC)
- Tests (ATE)
- Vulnerability assessment (AVA)
- Maintenance of assurance (AMA)
- Evaluation criteria of PP and ST (APE, ASE)

Security Assurance Requirements Organization



Assurance Packages

- Reusable set of functional or assurance components combined together to satisfy a set of identified security objectives
- Currently, there are 7 assurance packages called Evaluation Assurance Levels (EAL1 – EAL7)

Evaluation Assurance Levels

- EAL0 - Inadequate assurance
- EAL1 - Functionally tested
- EAL2 - Structurally tested
- EAL3 - Methodically tested and checked
- EAL4 - Methodically designed, tested and reviewed
- EAL5 - Semiformally designed and tested
- EAL6 - Semiformally verified designed and tested
- EAL7 - Formally verified designed and tested

Relationship to TCSEC

- With respect to assurance, roughly
  - EAL0 and EAL1 ~ D
  - EAL2 ~ C1
  - EAL3 ~ C2
  - EAL4 ~ B1
  - EAL5 ~ B2
  - EAL6 ~ B3
  - EAL7 ~ A1

TCSEC Status and Migration to CC

- Kenneth A. Minihan, Director of NSA, signed an Advisory Memorandum in April 1999
  - By the end of 2001, all products which were formerly evaluated against the TCSEC will have either become obsolete or, if they have maintained their TCSEC rating and are still in use, will be transitioned to a CC rating.

Mutual Recognition

- As of 18 October 1999
  - US
  - Canada
  - France
  - Germany
  - Australia
  - New Zealand
  - UK