A Comparison of Computer Security Evaluation Criteria

433-463 Software Engineering Thesis

Michael Papasimeon

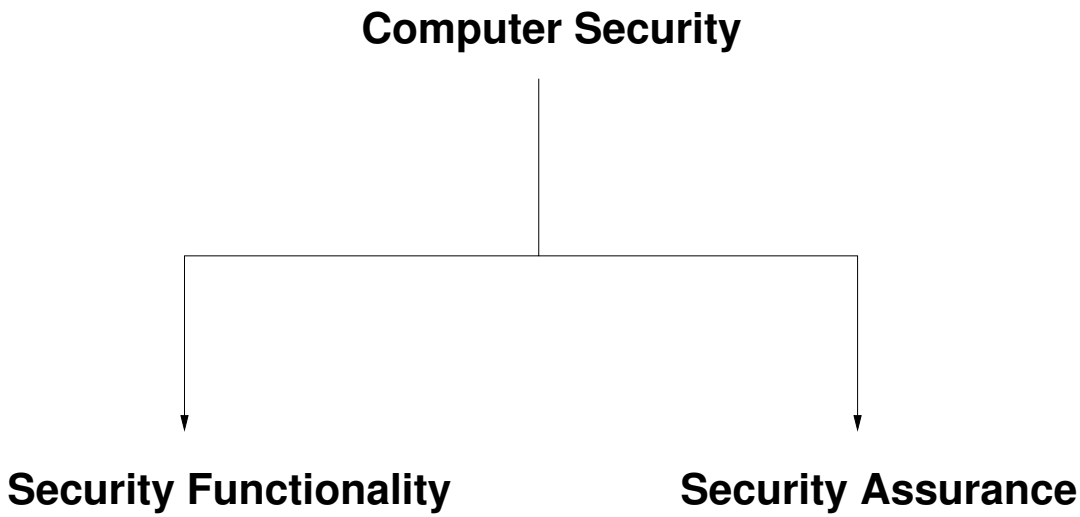
November 1997

Outline

- Computer Security and Evaluation Criteria
- Comparison Characteristics
- The Choice of Evaluation Criteria
- Description of TCSEC
- Description of ITSEC
- Description of CTCPEC
- Conclusions

Computer Security

- Security Functionality
- Security Assurance



Security Functionality

Examples include security features such as:

- Identification
- Authentication
- Discretionary and Mandatory Access Control
- Auditing
- Encryption

Security Assurance

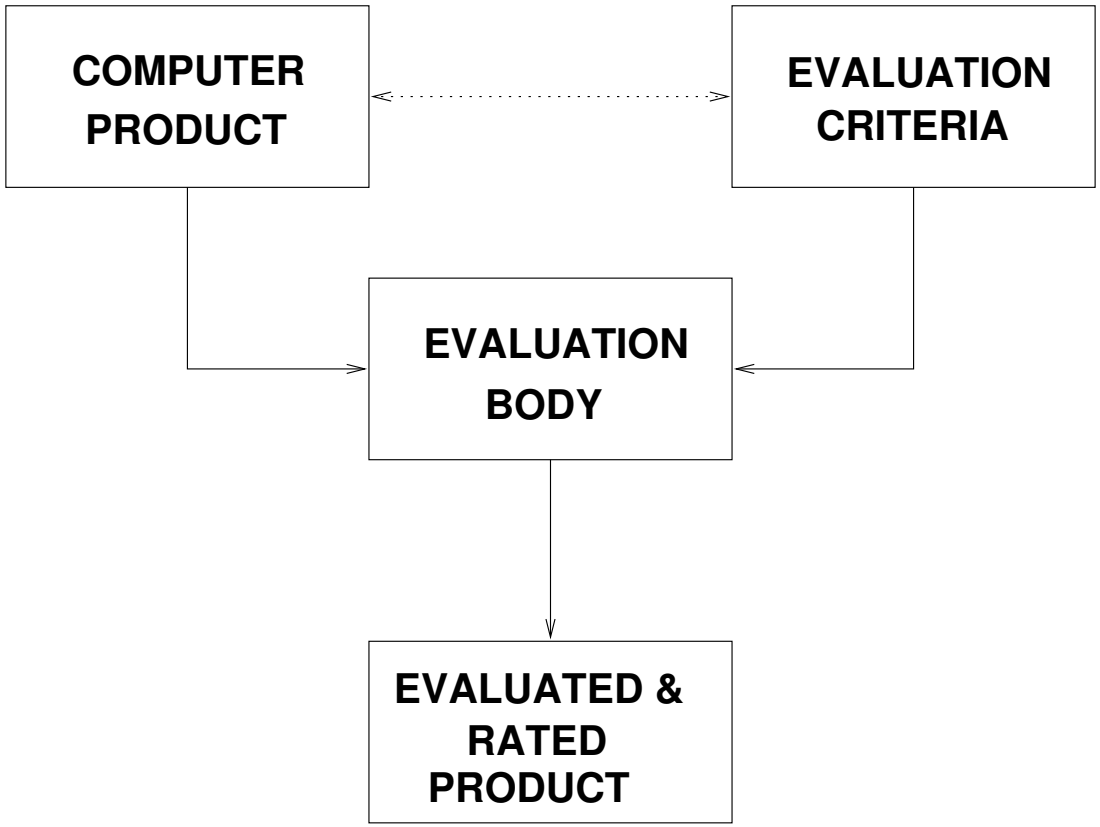
Typically involves the use of strict Software Engineering practices with an emphasis on assuring functionality.

- Security Policy and Security Policy Model Specification
- System Design
- Implementation
- Security Testing
- Security Documentation
- Configuration Management
- Verification and Validation of the development process

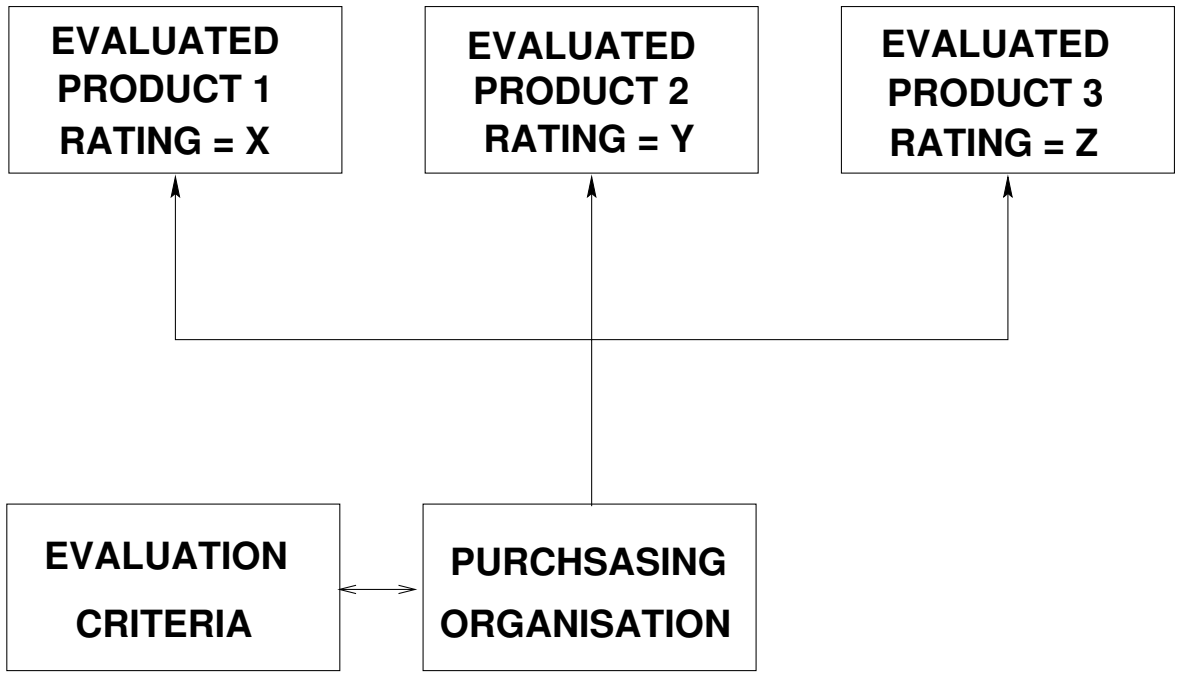
What are Computer Security Evaluation Criteria?

- General security standards
- Provide a set of criteria or requirements relating to security functionality and assurance
- Criteria are usually divided into “Levels of Trust” or ratings
- Computer systems are evaluated against a set of criteria and are given the rating or ”Level of Trust” of which they satisfy they have satisfied the requirements.
- A metric for measuring the level of security provided and confidence in that security provided by a system.

Typical Evaluation Process (1)



Typical Evaluation Process (2)



Comparison Characteristics

1. Organisation
   - Structure, Scope, Approach
   - Levels of Trust
2. Security Functionality
   - Accountability – Identification and Authentication
   - Access Control
   - Audit
3. Security Assurance
   - Security Policy
   - System Design
   - Implementation
   - Security Testing
   - Security Documentation
   - Configuration Management

Security Evaluation Criteria (1)

- United States
  - Trusted Computer System Evaluation Criteria (TCSEC)
    Also known as “Orange Book”
  - Federal Criteria
- Canada
  - Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

Security Evaluation Criteria (2)

- Europe
  - UK Systems Security Level
  - UK Commercial Computer Security Centre Evaluation Levels Manual
  - German Criteria for the Evaluation of Trustworthiness of Information Technology Systems
  - French “Blue-White-Red” Book
  - Information Technology Security Evaluation Criteria (ITSEC) [UK, France, Germany, the Netherlands]
- International
  - Common Criteria (CC)

Security Evaluation Criteria Selected for Comparison

The most influential and widely used evaluation criteria were selected for the comparison.

- Trusted Computer System Evaluation Criteria (TCSEC) [Orange Book]
- Information Technology Security Evaluation Criteria (ITSEC)
- Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

TCSEC (Orange Book)

- Classes contain both security functionality and security assurance requirements
- Scope is very high level
- Interpretation documents (The Rainbow Series) required for more specific cases. (eg: The Red Book is the Trusted Network Interpretation of the Orange Book).

TCSEC – Evaluation Criteria Classes

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

TCSEC Class Requirements

1. Security Policy
2. Accountability
3. Assurance
4. Documentation

CTCPEC

- Divides criteria into functionality criteria and asssurance criteria
- Does not require separate interpretation documents as it has more specific criteria

CTCPEC Assurance Levels

- Assurance Level T0
- Assurance Level T1
- Assurance Level T2
- Assurance Level T3
- Assurance Level T4
- Assurance Level T5
- Assurance Level T6
- Assurance Level T7

CTCPEC Assurance Levels – Areas of Evaluation

- Architecture
- Development Environment
- Development Evidence
- Operational Environment
- Security Documentation
- Security Testing

CTCPEC Functionality Criteria

1. Confidentiality Criteria
2. Integrity Criteria
3. Availability Criteria
4. Accountability Criteria

ITSEC

- Separation of assurance and functionality criteria
- Security functionality classes are not provided
- Only examples functionality classes and guidelines are provided
- Does not depend on external interpretation documents

ITSEC Assurance Levels

- Assurance Level E0
- Assurance Level E1
- Assurance Level E2
- Assurance Level E3
- Assurance Level E4
- Assurance Level E5
- Assurance Level E6

ITSEC Assurance Levels – Areas of Evaluation

1. Development Process
   - Requirements Specification
   - Architectural Design
   - Detailed Design
   - Implementation
2. Development Environment
   - Configuaration Control
   - Programming Languages and Compilers
   - Developer's Security
3. Operational Documentation
   - User Documentation
   - Administrator Documentation
4. Operational Environment
   - Delivery and Configuration
   - Start-up and Operation

ITSEC Example Functionality Classes

- Functionality Class F-C1
- Functionality Class F-C2
- Functionality Class F-B1
- Functionality Class F-B2
- Functionality Class F-B3
- Functionality Class F-IN
- Functionality Class F-AV
- Functionality Class F-DI
- Functionality Class F-DC
- Functionality Class F-DX

ITSEC Functionality Class Specification Guidelines

- Identification and Authentication
- Access Control
- Audit
- Object Reuse
- Accuracy
- Reliability of Service
- Data Exchange

Consequences

Summary