A Comparison of Computer Security Evaluation Criteria

Michael Papasimeon

433-463 THESIS
FINAL YEAR SOFTWARE ENGINEERING THESIS
DEPARTMENT OF COMPUTER SCIENCE
THE UNIVERSITY OF MELBOURNE
OCTOBER 1997

Abstract

This document describes the results of a comparison of the three most important and widely used computer security evaluation criteria; the US Trusted Computer Systems Evaluation Criteria, the Canadian Trusted Computer Product Evaluation Criteria and the European Information Technology Security Evaluation Criteria.

Table of Contents

List of Tables

Section 1

Introduction

Computer systems have been used to store and process security critical information for decades. Secure computing systems, once solely used by the military, are required in an ever increasing range of applications. Such systems are being used in government, industry, in financial applications such as banking, and over the last couple of years in many Internet applications such as electronic commerce. Secure systems are required almost anywhere sensitive information is stored, processed and where protection of this information is required.

It is therefore of great importance that the systems used in security critical applications conform to certain security standards. We must be able to evaluate systems against a computer security standard and determine, firstly what are the security features that the system provides, and secondly what level of assurance do we have that the system securely provides these features. Considerable effort has been expended by many countries to develop information technology security standards. In particular, over the past decade the concepts and criteria used to evaluated secure computer systems have matured in the United States, Europe and Canada.

A computer security standard provides a set of criteria which a product, such as an operating system, can be compared against to show the level of security which the product provides. However, there are number of security standards currently in use. The choice of standard affects how widely the evaluation of a product is accepted by potential customers around the world, especially in countries where different standards are in use.

Hence, there is justification in looking at and comparing a number of security standards. This not only involves looking at the similarities and differences in security criteria which each standard specifies, but also comparing the different levels of trust at which products are evaluated against. Computer security standards dealing with the evaluation of complete systems are known as computer security evaluation criteria.

This paper presents the results of a comparison between comparing a number of the most important, widely and currently used computer security standards. The purpose of the comparison was to determine what the consequences were for choosing a particular standard from the perspective of the developer, the development organisation and the end user. The comparison was made against a number of relevant characteristics. These include general characteristics such as levels of trust provided by the standards as well as more specific characteristics relating to security functionality and assurance.

In this paper we describe the selected characteristics and justify their choice. This is followed by a description of the security standards selected for the comparison and why they were chosen. The general and specific comparisons based on the selected characteristics are then described, followed by an evaluation of the consequences of using the standards and then a summary of the conclusions of the comparison.

Section 2

Comparison Characteristics

2.1 Method

The method followed in this comparison is as follows:

- A number of computer security standards relating to the evaluation of trusted systems were chosen.
- A list of evaluation characteristics were selected to form the basis of the comparison.
- The chosen documents were then summarised against the comparison characteristics.

This method was chosen because by evaluating the standards against a number of characteristics, then provided we can extract some useful information from the characteristics, we can also draw conclusions about the standards. The comparison of the security standards was based on the general characteristics discussed in this section. The criteria are divided into three general categories:

General Comparison: A general comparison provides us with information regarding the scope of each of the documents, the types of criteria specified, the types of computer systems targeted, the criteria for the different levels of trust and information on the reliance on separate interpretations of the standards.

Security Functionality: This is a comparison of the standards based on the different aspects of functional security criteria. This allows us to look at how the standards address different issues relating to security functionality.

Functionality Assurance: A comparison of the security standards based on various system engineering practices which must be put in place to assure that the security functionality has been successfully implemented and in fact provide operational security at the required level of trust. This tells us the type of issues which the developer must consider when designing and building a system which needs to be evaluated against one of the standards.

Each category is further divided up into a number of characteristics. A description of each the characteristics is given in this section.

The choice of the the characteristics on which the comparison is made is not meant to be extensive. Rather, the characteristics were chosen as general areas in which organisations developing trusted systems need to be aware of and then a comparison of how each of the documents deals with these characteristics is made.

2.2 Organisation

2.2.1 Structure

The overall structure of the security evaluation criteria documents is compared, including the purpose and intended audience of each document. The comparison on structure is an overall general description of the similarities and differences between the documents.

This characteristic was chosen because it provides us with information regarding the scope of the documents and type of security issues that are addressed. This information is relevant to both developers and those involved in evaluating systems.

2.2.2 Levels of Trust

A level of trust is a measure of the security functionality that a system provides, and the assurance of security that the system gives. Each standard specifies a number of levels of trust [1]. A computer product which is evaluated against a set of evaluation criteria is given a rating corresponding to a level of trust of satisfying the requirements of that level.

This characteristic was chosen because levels of trust are the primary indicator that establish what level of security a system provides. Organisations make decisions on what evaluated systems should be purchased according the level at which the system is evaluated at. This allows the organisation to look at the standards and see what level of trust corresponds to their requirements.

This characteristic allows us too look at what is specified for each level of trust in each of the security evaluation criteria, and what security issues are addressed at each level.

2.3 Security Functionality

The three characteristics of accountability, access control and audit were chosen as a basis for comparing the security functionality criteria of the three security standards. Although this is far from being a complete list of all the security functions which a system can provide, the purpose was to select only a few of the most important security functions. By looking at three of the most important and widely implemented security functions, we are able to assess how each of the security evaluation criteria addresses security functionality at a general level.

2.3.1 Accountability — Identification and Authentication

Accountability in computer security consists of two main areas:

- Identification
- Authentication

Identification deals with identifying a user, and the files, processes, actions and access to system resources associated with the user. Authentication involves verifying the identity of a user or process so that it can be decided which resources may be accessed by the user.

[1] Also known as assurance levels, evaluation levels and classes

2.3.2 Access Control

Discretionary Access Control (DAC), refers to information in a computer system which is by default not freely available, but access may be granted to other users at the discretion of the owner of the information.

Mandatory Access Control (MAC) refers to the access of information through classification and labeling and different levels, accessed by users with authorisation at those classifications.

2.3.3 Audit

Auditing in secure computer systems serves two main purposes. Firstly it allows the monitoring of a system's operation (through mechanisms such as audit logs), to identify security breaches and to facilitate corrective action. Secondly it is used in functionality assurance (see section 2.4) by certifying that a system meets certain security requirements.

2.4 Security Functionality Assurance

Security functionality assurance deals with the practices which must be put in place by a developer for a system to be evaluated at a particular assurance level. Therefore all the characteristics chosen in this category for the comparison deal with the different system engineering practices associated with the system development life cycle.

The characteristics selected are security policy, system design, implementation, security testing, security documentation, and configuration control. The information provided by the comparison is of importance to developers as it indicates the kind of engineering practices which have to be put in place when developing systems to be evaluated against one the standards.

2.4.1 Security Policy

A security policy is a set of requirements with respect to the security function that a system provides. From the security policy a security policy model is developed, which contains detailed descriptions of a system's security functions. The security policy model may be described using a informal, semi-formal or formal specification style.

2.4.2 System Design

Systems requiring high levels of trust must be designed to ensure that the the system's security policy is adequately enforced. The system design characteristic will look at what the each of the evaluation criteria specify as requirements for the design of a secure system to assure the system's security functionality;

This includes the requirements for formal designs at both the architectural and detailed level, the design methodologies used, and traceability and mapping between the design and the requirements specification.

2.4.3 Implementation

The implementation requirements for a system in each of the evaluation criteria look at issues such as the choice and use of well defined programming languages, coding standards and compliance with these standards, the choice of development tools such as compilers, the provision of source code for evaluation, the mapping between the source code and the detailed design, and the specification of implementation specific options.

2.4.4 Security Testing

Although some form of testing is present in all system engineering processes, when developing trusted and secure systems it is of very important to ensure that the system is tested adequately so that the user of the system has some level of confidence that the system's security policy is being satisfied.

Issues such as the type of testing required for different levels of trust, test documentation such as test plans, test results, and justification that the testing is sufficient.

2.4.5 Security Documentation

Trusted systems must be delivered with documentation to adequately inform both the user and system administrator about the security features of the system and the secure operation and administration of the system.

2.4.6 Configuration Management

Trusted systems must be developed under approved and reliable configuration management system, so that all source code, object code, and all documentation (requirements, design, testing, user and security) are under revision control and are consistent.

Section 3

Computer Security Evaluation Criteria

3.1 Choice of Computer Security Evaluation Criteria

The are many computer security evaluation criteria from countries all around the world. Only a subset of the many available ones have be chosen to be compared.

Although many of the security evaluation criteria in use are aimed at evaluating products for military and intelligence systems, they are usually have a broad scope and are just as applicable in many other areas as well.

The three most influential and widely used security evaluation criteria were chosen for the comparison. These documents are the specified security standards of the United States, Europe and Canada. The three standards are shown below.

- Trusted Computer Security Evaluation Criteria (TCSEC) [USA]
- Information Technology Computer Security Evaluation Criteria (ITSEC) [Europe]
- Canadian Trusted Computer Product Evaluation Criteria (CTCPEC) [Canada]

The following sections contain more detailed information on why these standards were chosen and other standards were omitted.

3.2 United States Security Evaluation Criteria

The most widely used and best known security evaluation criteria is the US Department of Defense “Trusted Computer System Evaluation Criteria (TCSEC)” [1], also known as the “Orange Book”. The latest version of this document is dated 1985 and it was included in the comparison.

In 1992 a draft document of a new set of security criteria known as the “Federal Criteria” [2] which was intended to eventually replace the TCSEC, was developed . The “Federal Criteria” did not get beyond draft stage and are not widely used, and therefore were not included in the comparison.

3.3 European Security Evaluation Criteria

There are a number of European security standards in existence.

- UK Systems Security Confidence Levels, CESG Memorandum Number 3 [3].
- UK Commercial Computer Security Centre Evaluation Levels Manual [4] (Also known as “The Green Book”).
- Criteria for the Evaluation of Trustworthiness of Information Technology Systems [5] (German Information Security Agency).
- The French “Catalogue de Crit res Destin s valuer le Degt de Confiance des Syst mes d’Information” [6]. (Also known as the ‘Blue-White-Red” book).

It was decided that work being done in Europe should be combined into a harmonised set of security evaluation criteria. This led to the development by the United Kingdom, Germany, the Netherlands, and France of the “Information Technology Security Evaluation Criteria (ITSEC)” [7]. As the ITSEC document replaced all the other European security evaluation criteria mentioned above, it is the only European document selected for the comparison.

3.4 Canadian Security Evaluation Criteria

The most important security criteria currently in use in Canada was developed by the Canadian government and is known as the “Canadian Trusted Computer Product Evaluation Criteria” [8] and was included in the comparison.

3.5 Common Criteria

The “Common Criteria for Information Technology Security Evaluation” [9] also known as “CC” are an international effort to combine the TCSEC, ITSEC, and CTCPEC into one common set of security evaluation criteria. The Common Criteria are at version 1.0, and are currently undergoing trial evaluations and review and hence were not considered in this comparison.

Section 4

Comparison of the Computer Security Evaluation Criteria

4.1 Comparing Organisational Structure

Table 4.1 shows the document structure for each of the security evaluation criteria being compared.

The first part of the TCSEC describes the criteria used to evaluate computer systems. The criteria are divided into four divisions which are given the following names.

- Division D – Minimal Protection
- Division C – Discretionary Protection
- Division B – Mandatory Protection
- Division A – Verified Protection

Each division consists of one or more classes. Each class contains a list of security functionality and security assurance requirements which a system must satisfy to be evaluated at that class. There are seven classes in the TCSEC — A1, B3, B2, B1, C2, C1, and D, in decreasing order of features and assurances. The requirements for a higher class are always a superset of the lower class.

The second part of the TCSEC contains some information regarding the rationale behind the development of the evaluation classes. It also contains some guidelines on various security issues which are specified in the evaluation classes such as security testing.

The second column of table 4.1 shows the document structure for the ITSEC. The ITSEC describes it's approach to functionality criteria in chapter 2, and effectiveness assurance in chapter 3. This is followed by a chapter on the the security assurance levels. There are seven levels of assurance in the ITSEC — E6, E5, E4, E3, E2, E1, and E0 in decreasing order of features and assurances similar to the TCSEC.

Example functionality classes are contained in Annex A of the ITSEC, and are not part of the main criteria. Unlike the TCSEC and the CTCPEC, the ITSEC does not define it's own security functionality criteria. It provides guidelines, recommendations and examples for selecting functionality criteria for a system.

TCSEC	ITSEC	CTCPEC
1. Introduction 2. Part I : The Criteria • Division D – Class D • Division C – Class C1 – Class C2 • Division B – Class B1 – Class B2 – Class B3 • Division A – Class A1 3. Part II : Rationale and Guidelines • Control objectives for trusted computer systems • Rationale behind the evaluation classes • The relationship between policy and the criteria • A guideline on covert channels • A guideline on configuring mandatory access control features • A guideline on security testing 4. Appendices • A. Commercial Product Evaluation Process • B. Summary of Evaluation Criteria Divisions • C. Summary of Evaluation Criteria Classes • D. Requirement Directory 5. Glossary 6. References	1. Introduction 2. Functionality 3. Assurance – Effectiveness 4. Assurance – Correctness • Level E0 • Level E1 • Level E2 • Level E3 • Level E4 • Level E5 • Level E6 5. Results of Evaluation 6. Glossary and References 7. Annex A – Example Functionality Classes • F-C1 • F-C2 • F-B1 • F-B2 • F-B3 • F-IN • F-AV • F-DI • F-DC • F-DX 8. Annex B – The Claims Language	1. Introduction 2. Confidentiality Criteria 3. Integrity Criteria 4. Availability Criteria 5. Accountability Criteria 6. Assurance Criteria • T0 – non-compliant • Level T-1 • Level T-2 • Level T-3 • Level T-4 • Level T-5 • Level T-6 • Level T-7 7. Definitions 8. Bibliography 9. Appendices • A. Technical Rationale • B. Constraints • C. Fundamentals • D. Concepts • E. Guide to Object Mediation • F. Guide to Confidentiality • G. Guide to Integrity • H. Guide to Availability • I. Guide to Accountability • J. Guide to Assurance • K. Implementing Services via Cryptography • L. Government Security Policy and Standards • M. Security Functionality Profiles

Table 4.1: Document Structure of Computer Security Evaluation Criteria

The evaluation criteria of the CTCPEC are divided into those dealing with security functionality and those dealing with security assurance. The CTCPEC contains individual chapters describing confidentiality criteria, integrity criteria, availability criteria, accountability criteria and assurance criteria. There are eight levels of assurance in the ITSEC — T7, T6, T5, T4, RT, T2, T1, and T0 in decreasing order of assurance.

4.2 Comparing Levels of Trust

This section looks at the different levels of trust specified by each of the documents. A level of trust is metric used to measure the level of security features and assurance a system provides.

4.2.1 Classes of the TCSEC

Table 4.2 summarises the requirements for each of the classes of the TCSEC. Each class in the TCSEC addresses four different areas.

Security Policy

All the classes above class D, in the TCSEC require the description of a system security policy. The security policy covers functionality such discretionary and mandatory access control and labelling. The specification of a security policy model is required in some of the classes, with the higher classes requiring use of semi-formal or formal methodologies, for the specification of the model and for the verification of the system design.

Accountability

The accountability requirements of the TCSEC classes deal with issues such as identification, authentication, trusted path and auditing. The higher the class, the stricter the requirements for identification, authentication, and auditing.

Assurance

The TCSEC classes address operational assurance (covert channels, trusted recovery) and life cycle assurance (requirements, design, implementation, testing, formal specification and verification).

Documentation

All TCSEC classes require the provision of security documentation for the user and the system administrator. The higher classes require the provision of test and design documentation.

TCSEC	
Level	**Description**
D	Minimal Protection Inadequate assurance
C1	Discretionary Security Protection Separation between users and data, enforcement of access limitations for individual users. Use of discretionary access control, design documentation, identification and authentication, secure system architecture and integrity, security testing, security documentation for users and administrators and test documentation.
C2	Controlled Access Protection C1 requirements and stricter discretionary access control. Accountability of all users through procedures such as auditing.
B1	Labelled Security Protection C2 requirements, and informal security policy model specification, data labelling according to specification, and mandatory access control. Formal or informal design specification and verification.
B2	Structured Protection B1 requirements and a formal security policy model, extended discretionary and mandatory access control enforcement. Addressing of covert channels, separation of security critical components, strict configuration management and strong authentication mechanisms.
B3	Security Domains B2 requirements and significant engineering to minimize system's complexity, expanded audit and security administration mechanisms, and system recovery procedures.
A1	Verified Design B3 requirements and use of formal design specification and verification techniques throughout whole life of the system, starting from a formal security policy model, a formal top level specification of the design and a formal detailed design. Support for strict configuration management controls and secure distribution of the system.

Table 4.2: Summary of the TCSEC assurance levels

4.2.2 Assurance Levels of the ITSEC

Table 4.3 summarises the requirements for the different levels of assurance of the ITSEC. The requirements for the ITSEC assurance levels are divided into a number clearly defined areas. There are four areas dealing with the development and the operation of the system. Each area is divided into smaller categories. At each level of assurance each category has a number of requirements which a system must satisfy for it to be evaluated at that level.

Development Process

- Requirements Specification
- Architectural Design
- Detailed Design
- Implementation

Development Environment

- Configuration Control
- Programming Languages and Compilers
- Developer's Security

Operational Documentation

- User Documentation
- Administrator Documentation

Operational Environment

- Delivery and Configuration
- Start-up and Operation

ITSEC	
Level	**Description**
E0	Inadequate Assurance
E1	Provision of a security policy, informal architectural design, and security testing to show the system satisfies it's security policy.
E2	E1 requirements and an informal detailed design, evidence of functional testing, use of a configuration control system, and use of an approved distribution procedure.
E3	E2 requirements and the provision of source code and/or hardware corresponding to the security mechanisms. Evidence of testing those security mechanisms.
E4	E3 requirements and formal security policy model supporting the system's security policy. Security enforcing functions, architectural design and detailed design specified in a semi-formal style.
E5	E4 requirements and a close correspondence between the detailed design and source code and/or hardware.
E6	E5 requirements and formal specification of the of security enforcing functions and architectural design, consistent with the formal security policy model.

Table 4.3: Summary of the ITSEC assurance levels

Security Functionality Criteria

Unlike the TCSEC and the CTCPEC, the ITSEC does not specify any functionality criteria. It is the responsibility of the developer to provide a specification of the security enforcing functions which the system provides. Annex A of the ITSEC contains example functionality classes which the developer can use as a guide. Although the selection of arbitrary security functionality in a system is allowed by the ITSEC, it is recommended that the system's security functions are grouped into eight generic categories.

- Identification and Authentication
- Access Control
- Audit

- Object Reuse
- Accuracy
- Reliability of Service
- Data Exchange

4.2.3 Assurance Levels and Security Ratings of the CTCPEC

Table 4.4 summarises the requirements for the assurance levels of the CTCPEC. As can be seen from the table, there is an emphasis on semi-formal and formal specifications at the higher classes for the security policy model, and the architectural and detailed design. There is also an emphasis on verification, through the requirements that there is a mapping or tracing between the different phases of the system development. Each assurance level in the CTCPEC addresses six different areas.

Architecture

This area covers requirements relating to a system's overall architecture and the enforcement of a system's security policy.

Development Environment

This area covers requirements such as the choice of development process, and configuration management.

Development Evidence

This area covers the requirements which show evidence of the product being developed. This includes requirements for a functional specification, architectural and detailed design and implementation.

Operational Environment

The operational environment requirements include the secure distribution, installation, startup and operation of a trusted system.

Security Documentation

The security documentation requirements include the requirements for both user and administrator documentation.

Security Testing

The security testing requirements cover issues such as security test planning, security test procedures, justification as to why the test coverage is sufficient, and evidence of security testing through the provision of test results.

CTCPEC	
Level	**Description**
T0	Inadequate level of assurance
T1	Informal security policy, informal architectural design, informal detailed design of security critical components.
T2	Informal security policy, informal security policy model informal architectural design, informal detailed design,
T3	Informal security policy semi-formal security policy model, semi-formal architectural design, informal detailed design, provide subset of source code for evaluation.
T4	Informal security policy, formal security policy model, semi-formal architectural design, semi-formal detailed design, provide subset of source code for evaluation.
T5	Informal security policy, formal security policy model, semi-formal architectural design, semi-formal detailed design, provide source code of entire product for evaluation.
T6	Informal security policy, formal security policy model, formal architectural design, semi-formal detailed design, provide source code of entire product for evaluation.
T7	Informal security policy, formal security policy model, formal architectural design, formal detailed design, provide source code of entire product for evaluation.

Table 4.4: Summary of the CTCPEC assurance levels

Security Functionality Criteria

Unlike the TCSEC, the CTCPEC separates the functionality criteria from the assurance criteria. Also, unlike ITSEC, the CTCPEC does not leave the decision for the choice of security functionality to the developer. The CTCPEC clearly defines a large number of security functionality criteria. Table 4.5 summarises the functionality criteria of the CTCPEC.

As can be seen from the table, the CTCPEC contains four types of security functionality criteria.

- Confidentiality Criteria
- Integrity Criteria
- Availability Criteria
- Accountability Criteria

Each of these criteria types contain a number of specific criteria, each with a number of ratings. For example, “Audit” is one of the accountability criteria.

Functionality Criteria	**Levels**
Confidentiality Criteria	
Covert Channels	CC-0, CC-1, CC-2, CC-3
Discretionary Confidentiality	CD-0, CD-1, CD-2, CD-3, CD-4
Mandatory Confidentiality	CM-0, CM-1, CM-2
Object Reuse	CR-0, CR-1
Integrity Criteria	
Domain Integrity	IB-0, IB-1, IB-2
Discretionary Integrity	ID-0, ID-1, ID-2, ID-4
Mandatory Integrity	IM-0, IM-1, IM-2, IM-4
Physical Integrity	IP-0, IP-1, IP-2, IP-3, IP-4
Rollback	IR-0, IR-1, IR-2
Separation of Duties	IS-0, IS-1, IS-2
Self Testing	IT-0, IT-1, IT-3
Availability Criteria	
Containment	AC-0, AC-1, AC-2, AC-3
Fault Tolerance	AF-0, AF-1, AF-2
Robustness	AR-0, AR-1, AR-2, AR-3
Recovery	AY-0, AY-1, AY-2, AY-3
Accountability Criteria	
Audit	WA-0, WA-1, WA-2, WA-3, WA-4, WA-5
Identification and Authentication	WI-0, WI-1, WI-2, WI-3
Trusted Path	WT-0, WT-1, WT-3

Table 4.5: Summary of the CTCPEC's functionality criteria and available security ratings

4.2.4 Summary of Evaluation Areas

When evaluating systems for assurance, the evaluation occurs against a group of general criteria. Table 4.6 summarises the areas in which requirements are specified for each of the levels of trust in each of the documents.

TCSEC	**ITSEC**	**CTCPEC**
Security Policy Accountability Assurance Documentation	Development Process Development Environment Operational Documentation Operational Environment	Architecture Development Environment Development Evidence Operational Environment Security Documentation Security Testing

Table 4.6: Areas of Evaluation

4.2.5 Equivalent Levels of Trust

Table 4.7 shows the approximate correspondence between levels of assurance for the three documents. The relationship between the TCSEC classes and the ITSEC assurance levels are specified in the ITSEC [7]. The relationship between the ITSEC and the CTCPEC assurance levels, are obtained from the results of an international collaboration to develop a common approach to security standards described in *Foundations for the Harmonization of Information Technology Security Standards* [10].

TCSEC	ITSEC	CTCPEC
A1	E6	T7
B3	E5	T6
B2	E4	T5
B1	E3	T4
C2	E2	T3
C1	E1	T2
		T1
D	E0	T0

Table 4.7: Comparison of Assurance Levels

4.3 Summary of General Characteristics

Characteristic	TCSEC	ITSEC	CTCPEC
Structure			
Introduction	YES	YES	YES
Assurance Criteria	YES	YES	YES
Separation of Functionality Criteria	NO	YES	YES
Additional Guidelines for Criteria	YES	NO	YES
Rationale behind Criteria	YES	NO	YES
Glossary/Definitions	YES	YES	YES
References/Bibliography	YES	YES	YES
Levels of Trust			
Separation of assurance criteria from security functionality criteria (confidentiality, integrity, availability, accountability)	NO	YES	YES
Security Functionality			
Specification of Functionality Criteria	YES	NO	YES
Criteria Interpretations			
Reliance on separate interpretation documents to cover wider range of systems	YES	NO	NO

Table 4.8: Summary of General Characteristics

Table 4.8 gives a summary of some of the general characteristics of the three sets of security evaluation criteria.

Both the ITSEC and the CTCPEC target a greater range of systems than does the TCSEC, are more explicit about the requirements at each assurance level and therefore do not require separate interpretation documents. The requirements in the TCSEC are more general and hence it is often the case that there are several ways to read a given statement [1]. As a result, a number of official interpretations of the TCSEC have been developed. The interpretations are official statements articulating which of a number of possible ways to read a security requirement for different applications. For example, the Trusted Network Interpretation (TNI) [12] of the TCSEC, also referred to as “The Red Book”. The official interpretations of the TCSEC are collectively know as the “The Rainbow Series” [13].

[1] Stated in the NSA’s TPEP FAQ [11]

4.4 Comparing Security Functionality

This section compares the three sets of security evaluation criteria with respect to specific areas of security functionality. The comparison is made on three important areas of security functionality.

- Accountability
- Access Control
- Audit

4.4.1 Accountability — Identification and Authentication

Table 4.9 summarises the requirements for identification and authentication.

Accountability is one of four major criteria in which requirements are specified for each class of the TCSEC. Requirements for identification and authentication are addressed in this area. The issue of "trusted paths" are addressed in this area for the higher classes.

The ITSEC does not specify any criteria regarding accountability through identification and authentication, as it allows the developer to select arbitrary security functions for a product. The ITSEC recommends that ”Identification and Authentication” is one of the categories which the developer should use when specifying functionality. The ITSEC provides example functionality classes, which the developer can use a guide. Identification and authentication requirements are present in all the example classes. A set of four levels (WI-0 to WI-3) are defined, indicating increasing security in terms of identifying and authenticating users.

TCSEC	
Levels	Identification: C1, C2, B1, B2, B3, A1 Authentication: C1, C2, B1, B2, B3, A1 Trusted Path: B2, B3, A1
ITSEC	
Levels	F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-DI, F-DC, F-DX
CTCPEC	
Levels	WI-0, WI-1, WI-2, WI-3

Table 4.9: Comparison of Accountability Criteria — Identification and Authentication

4.4.2 Access Control

Table 4.10 summarises the requirements for access control mechanisms. In the TCSEC, access control is addressed under the area of security policy. The TCSEC classes look at discretionary access control and mandatory access control. As mentioned previously the ITSEC does not specify any security functionality. The ITSEC specifies that "Access Control" is one of the categories which the developer should use when specifying security functionality, and it is included in the ITSEC example functionality classes. The CTCPEC looks at access control from the perspective of Confidentiality Criteria (including discretionary and mandatory confidentiality) and Integrity Criteria (including discretionary and mandatory integrity).

<table>
<tr><th colspan="2">TCSEC</th></tr>
<tr><td>Levels</td><td>Discretionary Access Control: C1, C2, B1, B2, B3, A1
Mandatory Access Control: B1, B2, B3, A1</td></tr>
<tr><th colspan="2">ITSEC</th></tr>
<tr><td>Levels</td><td>F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-DI, F-DC, F-DX</td></tr>
<tr><th colspan="2">CTCPEC</th></tr>
<tr><td>Levels</td><td>Discretionary Confidentiality: CD-0, CD-1, CD-2, CD-3 CD-4
Mandatory Confidentiality: CM-0, CM-1, CM-2
Discretionary Integrity: ID-0, ID-1, ID-2, ID-4
Mandatory Integrity: IM-0, IM-1, IM-2, IM-4</td></tr>
</table>

Table 4.10: Comparison of Access Control Criteria

4.4.3 Audit

Table 4.11 summarises the requirements for auditing. Audit requirements in the TCSEC are covered under accountability criteria and are present in classes above class D. The ITSEC recommends that "Audit" be one of the categories when specifying security functionality. Like the TCSEC, the CTCPEC addresses audit under accountability criteria but specifies a number of audit levels.

<table>
<tr><th colspan="2">TCSEC</th></tr>
<tr><td>Levels</td><td>C2, B1, B2, B3, A1</td></tr>
<tr><th colspan="2">ITSEC</th></tr>
<tr><td>Levels</td><td>F-C1, F-C2, F-B1, F-B2, F-B3, F-IN, F-AV, F-DI, F-DC, F-DX</td></tr>
<tr><th colspan="2">CTCPEC</th></tr>
<tr><td>Levels</td><td>WA-0, WA-1, WA-2, WA-3, WA-4, WA-5</td></tr>
</table>

Table 4.11: Comparison of Audit Criteria

4.5 Comparing Security Functionality Assurance

This section compares the security evaluation criteria on the basis of functionality assurance. The comparison is made against seven system engineering characteristics which are important in assuring that a system is secure. The characteristic are:

- Security Policy
- System Design
- Implementation
- Security Testing
- Security Documentation
- Configuration Management

4.5.1 Security Policy

A system's security policy is a set of security requirements which a system must satisfy. A detailed description of a system's security policy is known as the security policy model. The TCSEC, the ITSEC and the CTCPEC all address the issues of security policies and security policy models very similarly.

<table>
<tr><th colspan="2">TCSEC</th></tr>
<tr><td>Approach</td><td>Security Policy is one of the four major criteria addressed for each class of the TCSEC</td></tr>
<tr><td>Levels</td><td>C1, C2, B1, B2, B3, A1</td></tr>
<tr><th colspan="2">ITSEC</th></tr>
<tr><td>Approach</td><td>For each assurance level in the ITSEC, security policy is assessed under the area of “Development Process - Requirements”</td></tr>
<tr><td>Levels</td><td>E1, E2, E3, E4, E5, E6, E7</td></tr>
<tr><th colspan="2">CTCPEC</th></tr>
<tr><td>Approach</td><td>For each assurance level, the CTCPEC addresses the issue of security policy under the area of the system’s “Architecture”</td></tr>
<tr><td>Levels</td><td>T1, T2, T3, T4, T5, T6, T7</td></tr>
</table>

Table 4.12: Comparison of Security Policy Criteria

Table 4.12 summarises the requirements for security policy for each of the documents. In general for the lower level of assurances in the TCSEC, the ITSEC and the CTCPEC, the requirements include:

- Informal security policy
- Informal or semi-formal security policy model
- Tracing between the security policy and the security policy model
- Tracing between the security policy model and the architectural design

At the higher levels of assurance, the requirements are stricter and include:

- Informal security policy
- Formal security policy model
- Demonstration of security policy mapping to security policy model
- Formal verification that the security policy model maps to the architectural design

4.5.2 System Design

Table 4.13 shows which assurance levels of the three documents require assurance through the provision of a system design. As can be seen from the table, evidence for system design is a requirement for all classes of the TCSEC above class D, all assurance levels of the ITSEC above E0, and all assurance levels of the CTCPEC above T0.

<table>
<tr><th colspan="2">TCSEC</th></tr>
<tr><td>Levels</td><td>C1, C2, B1, B2, B3, A1</td></tr>
<tr><th colspan="2">ITSEC</th></tr>
<tr><td>Levels</td><td>E1, E2, E3, E4, E5, E6</td></tr>
<tr><th colspan="2">CTCPEC</th></tr>
<tr><td>Levels</td><td>T1, T2, T3, T4, T5, T6, T7</td></tr>
</table>

Table 4.13: Comparison of System Design Criteria

System design in the TCSEC is addressed under the "Assurance" category for each class. In the ITSEC, the system design is addressed under the "Development Process Criteria" in the areas of "Architectural Design" and "Detailed Design". The CTCPEC addresses system design under the criteria for "Development Evidence".

The requirements for system design across the three sets of security evaluation criteria are very similar. All the documents have requirements for:

- Architectural design
- Detailed design
- Mapping between security policy model and architectural design
- Mapping between the architectural design and the detailed design
- Mapping between the detailed design and the implementation

At the higher levels of assurance, there is a greater emphasis on formal design and verification techniques.

4.5.3 Implementation

Implementation issues in the TCSEC are addressed under the Assurance Criteria, in the areas dealing with operational assurance and development life-cycle assurance. However, the TCSEC does not go into much detail regarding implementation, focusing more on verification and testing techniques to show that the system satisfies it's security policy. The TCSEC relies on the the interpretation documents, the "Rainbow Series" [13], for specific requirements regarding implementation for different types of systems.

The ITSEC and the CTCPEC on the other hand, have more specific implementation requirements, at each level of assurance. In each assurance level, the ITSEC addresses implementation requirements in the following criteria groups.

- Construction — The Development Process
  - Implementation
- Construction — The Development Environment
  - Programming Languages and Compilers
  - Developer's Security

The CTCPEC addresses implementation requirements, in the following criteria groups.

- Development Environment
- Development Evidence
- Operational Environment

In all the security evaluation criteria being compared, in the higher assurance levels, there is an emphasis on semi-formal and formal verification techniques to show the mapping between the detailed design and the requirement. Also common in the higher assurance levels, is the requirement that security critical source code or all the source code be provided when the system is being evaluated.

4.5.4 Security Testing

The TCSEC, the ITSEC and the CTCPEC have very similar requirements for security testing. All assurance levels (above the non-compliant levels) in all the documents address the issue of security testing. The emphasis is on:

- Test Plan Documentation
- Test Results Documentation
- Evidence of Testing
- Justification that coverage of testing is sufficient
- Evidence using test reports to show that the system satisfies it's security policy.

4.5.5 Security Documentation

The requirements for security documentation are very similar in the TCSEC, the ITSEC, and the CTCPEC. All documents require that the system is provided with security documentation for the user and for the system administrator at all levels of assurance. This is summarised in table 4.14.

Requirement	TCSEC	ITSEC	CTCPEC
Security Features User's Guide (User Documentation)	C1, C2, B1, B2, B3, A1	E1, E2, E3, E4, E5, E6	T1, T2, T4, T4, T5, T6, T7
Trusted Facility Manual (Administrator's Documentation)	C1, C2, B1, B2, B3, A1	E1, E2, E3, E4, E5, E6	T1, T2, T3, T4, T5, T6, T7

Table 4.14: Comparison of ecurity Documentation Criteria

Security documentation requirements are addressed in the "Documentation" criteria for each class in the TCSEC, in the "Operational Documentation" criteria of the ITSEC, and in the "Security Documentation" criteria of the CTCPEC.

4.5.6 Configuration Management

The use of a configuration control system throughout all phases of the system's development is requirement at all levels of assurance for the TCSEC, the ITSEC and the CTCPEC. This is summarised in table 4.15.

Requirement	TCSEC	ITSEC	CTCPEC
Configuration Control System	C1, C2, B1, B2, B3, A1	E1, E2, E3, E4, E5, E6	T1, T2, T3, T4, T5, T6, T7

Table 4.15: Comparison of Configuration Management Criteria

Configuration management is addressed under "Assurance" in the TCSEC, and under "Development Environment" in the both the ITSEC and the CTCPEC.

Section 5

General Evaluation

This section looks at the consequences of getting a system evaluated against one of the sets of security evaluation criteria – TCSEC, ITSEC and CTCPEC from the perspective of the developer, the procurer and the end user.

5.1 Consequences for the developer

Developers need to be aware of technical security issues, protocols and standards specific to the system being built, in some cases interpretations of the criteria, and should be aware of security guidelines or requirements which are not specified in the criteria but have being identified by a client or other stakeholder in the development of the system.

All the assurance levels of the three security evaluation criteria require that the developer employ standard software engineering practices, such as system requirements (formal) specification, design, implementation, testing, documentation, configuration management, and (formal) verification and validation. In addition to these general software engineering requirements, there are many requirements specifically relating to security, such as the development of the security policy model.

If the system is being evaluated against the TCSEC, the developer should be aware that the interpretations of the TCSEC, the "Rainbow Series", need to be consulted for specific application type. Interpretations are not required for the ITSEC or the CTCPEC, as all these criteria were developed to target a greater range of trusted systems. If the system being evaluated against the ITSEC, the developer should be aware that functionality criteria are not specified in the standard and it is up to the developer to define the security functions of the system.

5.2 Consequences for the development organisation

The organisation developing a trusted system must be familiar with the assurance levels of the criteria and must notify the organisation conducting the evaluation to which assurance level the system is being targeted at. This means that the evaluation will only attempt to determine if the system provides that level of trust or assurance.

The evaluation body usually also places other requirements on the development organisation. For example, in the United States, if a system is being submitted to the Trusted Product Evaluation Program (TPEP) [1] for evaluation against the TCSEC, the organisation must provide evidence that the system has a legitimate

[1] The TPEP is part of the National Security Agency (NSA), which is part of the US Department of Defense

market in the United States.

Although evaluation organisation such as TPEP do not charge the development organisation a fee for an evaluation, there should be an awareness that developing a system which satisfies any of the assurance levels of criteria such as TCSEC, ITSEC and CTCPEC results in very high development costs, especially at the higher levels of assurance.

5.3 Consequences for the end user

A user or a purchaser of a secure system needs to aware of a number of issues.

- What are the security requirements?
- Is there familiarity with the security requirements of the evaluation criteria which the product being considered has being evaluated against?
- With what level of assurance in the relevant evaluation criteria does the user's security requirement correspond to?

The user must also be aware of the secure installation, startup and operation of the system in order for the security requirements to be fulfilled.

In general, a system which has been successfully evaluated against one of the evaluation criteria provides the user with a high degree of confidence that their is assurance that the system provides the level of assurance which it has been awarded.

Section 6

Conclusions

The choice of which security evaluation criteria will be targeted by a developer depends on a number of different factors. Since conformance to a standard is important, the choice of criteria is likely to be limited to the TCSEC from the USA, the ITSEC from Europe or the CTCPEC from Canada, as these are the most widely used and accepted security evaluation criteria.

The factor most influencing the choice of a target set of security evaluation criteria for a trusted product is the product's intended market.

For example If a product is being developed with government or military customers in mind, it is in the the best interest of the developer to choose the evaluation criteria which has been specified by the government of the nation which the product is targeted at. In the United States, the National Security Agency requires conformance to the TCSEC, the ITSEC in Europe and the CTCPEC in Canada. Countries which do not have their own evaluation criteria usually adopt either the TCSEC, the ITSEC or the CTCPEC. For example in Australia, the Defence Signals Directorate (DSD) [14] has adopted the ITSEC for use by the Australian government.

Choosing a set of security evaluation criteria as a developer is usually an easier job than a government or commercial organisation choosing a particular evaluation criteria for which products which they use must conform to. This is simply because it is often the case for the developer that the choice has already been made by the client.

From a security functionality and security assurance perspective the three sets of evaluation criteria compared, specify very similar requirements. Regardless of the whether the choice is the TCPEC, the ITSEC or the CTCPEC, building a trusted system does require important security issues to be taken into account. These include accountability, access control, audit and the development of security policy models, as well as the use of well defined and rigid software engineering practices such as security requirements specification, architectural and detailed design, secure implementation, security testing, the production of security documentation, configuration management, and at the higher levels of assurance, the use of formal verification techniques to ensure that the system being built satisfies the security policy model throughout all the phases of the development process.

The many similarities between the TCSEC, the ITSEC and the CTCPEC is to be expected because the European and Canadian documents were originally based on the US experience with the TCSEC, which has been in use since 1983.

Based on the comparison of the three sets of security evaluation criteria, from an operational perspective the ITSEC and the CTCPEC are to be preferred over the TCSEC. The main reason for this is that the criteria in the ITSEC and the CTCPEC are more wide reaching, take more cases into account and allow the targeting of a more diverse range of systems without the reliance on separate interpretation documents as is the case with the TCSEC.

Selecting between the ITSEC and the CTCPEC depends on the requirements of the particular organisation. Both the ITSEC and the CTCPEC separate functionality criteria from assurance criteria. The CTCPEC contains detailed and very specific security functionality criteria. On the other hand, the ITSEC allows a system to have any security function which the developer defines.

Therefore, if a choice was to be made between the three compared documents, (not taking external requirements such as those of a client or the wide spread use of a document into account), it would have to be the ITSEC or the CTCPEC. Both standards do not require external interpretations, they separate functionality and assurance criteria, and both apply to wide range of systems. A choice between them depends on the developer. It is up to the developer to choose the flexibility of the ITSEC in specifying security functionality or the rigidness of the CTCPEC, where security functions are explicitly defined and have their own level of trust separate from the assurance levels.

The increase in the use of computer systems for all sorts of applications, has resulted in the requirement for the existence of secure systems which have been evaluated against a set of well defined criteria and can be rated to provide a specific level of trust. Trusted systems, once only required by the military now are in wide spread use in government, industry, commerce, education and many other areas. Hence, the application of security evaluation criteria to evaluate systems is becoming increasingly important, and is very much an active area of research and development in the large domain of computer security. This world wide effort has resulted in the current development of the Common Criteria combining the TCSEC, the ITSEC and CTCPEC into one standard set of security evaluation criteria, which will in the future will provide a common base from which a trusted system can be evaluated.

Appendix A

Background Information on Selected Computer Security Evaluation Criteria

A.1 Trusted Computer System Evaluation Criteria (TCSEC)

Full Title	Department of Defense Trusted Computer System Evaluation Criteria
Identification	DoD 5200.28-STD
Abbreviation	TCSEC
Known As	Orange Book
Country	United States
Organisation	US Department of Defense
Date	December, 1985

Table A.1: TCSEC Background Information

A.2 Information Technology Computer Security Evaluation Criteria (ITSEC)

Full Title	Information Technology Computer Security Evaluation Criteria (ITSEC) Harmonised Criteria of France – Germany – the Netherlands – the United Kingdom
Abbreviation	ITSEC
Countries	France, Germany, the Netherlands, the United Kingdom
Organisation	Department of Trade and Industry, London, United Kingdom
Date	June, 1991

Table A.2: ITSEC Background Information

A.3 Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

Full Title	The Canadian Trusted Computer Product Evaluation Criteria
Abbreviation	CTCPEC
Country	Canada
Organisation	Canadian System Security Centre, Communications Security Establishment, Government of Canada
Date	January, 1993

Table A.3: CTCPEC Background Information

References

[1] US Department of Defence. *Trusted Computer System Evaluation Criteria*, December 1995.

[2] United States Government. *Federal Criteria for Information Technology Security, Version 1.0*, December 1992.

[3] Communications-Electronics Security Group. *UK Systems Security Confidence Levels, CESG, Memorandum No. 3*, January 1989.

[4] Department of Trade and United Kingdom Industry. *DTI Commercial Computer Security Centre Evaluation Levels Manual, V22*, February 1989.

[5] German Information Technology Security Agency. *Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems*, January 1989.

[6] France Service Central de la S curit des Syst mes d'Information. *Catalogue de Crit res Destin s valuer le Degr de Confiance des Syst mes d'Information*, July 1989.

[7] Commission of the European Communities. *Information Technology Security Evaluation Criteria*, June 1991.

[8] Government of Canada Canadian System Security Centre, Communications Security Establishment. *Canadian Trusted Computer Product Evaluation Criteria*, January 1993.

[9] NIST NSA. *Common Criteria for Information Technology Security Evaluation*, January 1996.

[10] Cooperation on Security of Information Systems Joint Task 01. *Foundations for the Harmonization of Information Technology Security Standards*, April 1993.

[11] Trusted Product Evaluation Program (TPEP). *The Computer Security Evaluation Criteria Frequently Asked Questions (V2.1)*.
`http://www.radium.ncsc.mil/tpep/process/faq.html`.

[12] US Department of Defence. *Trusted Network Interpretation*, April 1985. CSC-STD-002-85
`http://www.radium.ncsc.mil/tpep/library/rainbow/NCSG-TG-021.html`.

[13] US Department of Defence. *The Rainbow Series*.
`http://www.radium.ncsc.mil/tpep/library/rainbow/`.

[14] Commonwealth of Australia Department of Defence. *Defence Signals Directorate*.
`http://www.dsd.gov.au/`.

References Used but not Cited

[1] Simson Garfinkel and Gene Spafford, *Practical UNIX and Internet Security*, O'Reilly and Associates, Inc, 1996

[2] B. Clifford Neuman, *Protection and Security Issues for Futire Systems*, Department of Computer Science and Engineering, University of Washington

[3] CT Sennet, *Computer Security*, Royal Signals and Radar Establishment

[4] Charles P. Pfleeger, *The Fundamentals of Information Security*, IEEE Software, January, 1997

[5] COAST Security Archive, Purdue University, `http://www.cs.purdue.edu/coast/archive/index.html`

[6] Mark Joseph Edwards, *The Handy Security Toolkit*, Windows NT Magazine, July, 1997

[7] Joint Task 1 (JT01), *Relating Functionality Class and Security Sub-profile Specification*, EC/US Joint Workplan for cooperation on Security of Information Systems