NISTIR 4774

A Review of U.S. and European Security Evaluation Criteria

Charles R. Dinkel

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Systems Laboratory
Computer Security Division
Gaithersburg, MD 20899

U.S. DEPARTMENT OF COMMERCE
Rockwell A. Schnabel, Acting Secretary
NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director

NIST

NISTIR 4774

A Review of U.S. and European Security Evaluation Criteria

Charles R. Dinkel

U.S. DEPARTMENT OF COMMERCE
Technology Administration
National Institute of Standards
and Technology
Computer Systems Laboratory
Computer Security Division
Gaithersburg, MD 20899

March 1992

U.S. DEPARTMENT OF COMMERCE
Rockwell A. Schnabel, Acting Secretary

NATIONAL INSTITUTE OF STANDARDS
AND TECHNOLOGY
John W. Lyons, Director

TABLE OF CONTENTS

A Review of U.S. and European Security Evaluation Criteria

Charles Dinkel
National Institute of Standards and Technology
Computer Systems Laboratory
Computer Security Division

ABSTRACT

Several United States and European documents describing criteria for specifying and evaluating the trust of computer products and systems have been written. This report reviews five of these documents and discusses the approach each one uses to provide criteria for specifying and evaluating the trust of computer products and systems.

KEY WORDS

Computers, computer security, ITSEC, Orange Book, Red Book, security evaluation criteria, trust, trusted computer system

1.0 INTRODUCTION

Users of systems need confidence in the security of the system they are using. They also need a metric to compare the security capabilities of products they are thinking of purchasing. Users have several options for dealing with this issue: they could trust the word of the manufacturers or vendors of the systems and products in question; they could test the systems themselves; they could rely on the results of some impartial assessment by an independent body. Evaluating a system or product using the latter approach requires objective and well defined security evaluation criteria.

Several United States and European documents describing criteria for specifying and evaluating the trust of computer products and systems have been written. Among these are the following:

1. **Department of Defense Trusted Computer System Evaluation Criteria** (TCSEC); DoD 5200.28-STD; December 1985; also known as the Orange Book.[1]

[1] The term "Rainbow Series" refers to the publications of the National Computer Security Center (NCSC). Each book is printed with a different color cover.

2. **Trusted Network Interpretation** (TNI); NCSC-TG-005; July 1987; also known as the Red Book.[1]

3. **Trusted Database Management System Interpretation** (TDI); NCSC-TG-021; August 1990.

4. **IT Security Criteria - Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems**; German Information Security Agency (GISA); 1st Version 1989. (Included in the ITSEC; see #5 below)

5. **Draft Information Technology Security Evaluation Criteria**, (ITSEC); Harmonized Criteria of France - Germany - the Netherlands - the United Kingdom; May 1990.

This report reviews and provides NIST's views on each of these documents and discusses the approach each uses to provide criteria for specifying and evaluating the trust of computer products and systems.

2.0 TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

The trusted computer system evaluation criteria defined in the Orange Book classify operating systems into four broad divisions of security protection: A,B,C,D. These divisions form a hierarchy with the highest division (A) reserved for systems providing the most comprehensive security. Each division represents a major improvement in the overall confidence that can be placed in the system for the protection of sensitive information. It is important to note that this guide does not apply to networks or components. The Orange Book defines security levels as follows:

* **Division D: *Minimal Protection*** - This division contains only one class. It is reserved for those systems that have been evaluated but that fail to meet the requirements for a higher evaluation class.

* **Division C: *Discretionary Protection*** - Classes in this division provide discretionary (need-to-know) protection and, through the inclusion of audit capabilities, accountability of subjects and the actions they initiate.

* **Division B: *Mandatory Protection*** - The concept of a security relevant or *Trusted Computing Base* (TCB) that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules

is a major requirement of this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor, an access control concept that refers to an abstract machine that mediates all accesses to objects by subjects, has been implemented. The security kernel, the hardware, software and firmware elements of a TCB, must mediate all accesses to data, be protected from modification, and be verifiable as correct.

* **Division A: *Verified Protection*** - This division is characterized by the use of formal verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect classified or other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development and implementation.

The four divisions of criteria provide a basis for the evaluation of effectiveness of security controls built into trusted, commercially available automatic data processing (ADP) system products. They are also applicable to the evaluation of existing systems and to the specification of security requirements for ADP system acquisition.

Within divisions C and B there are a number of subdivisions known as classes. The classes are also arranged in an hierarchical order. Assurance of correct and complete design and implementation of division C and lower classes of division B is gained mostly through testing of the security relevant portions or TCB of the systems.

Higher classes in division B and division A derive their security attributes more from their design and implementation structure than the set of security mechanisms they possess. Rigorous analysis during the design stages provides increased assurance that the required security features are operative, correct and tamperproof.

Within each class, four major sets of criteria are addressed. The first three represent features necessary to satisfy the broad objectives of Security Policy, Accountability, and Assurance. The fourth set, Documentation, describes the type of written evidence in the form of user guides, manuals, and the test and design documentation required for each class.

The criteria described in the Orange Book were developed with three objectives in mind:

1. To provide a standard to manufacturers as to what security features to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements (with particular emphasis on preventing the disclosure of data) for sensitive applications.

2. To provide DoD organizations with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information.

3. To provide a basis for specifying security requirements in acquisition specifications.

Two types of requirements are delineated for secure processing: (1) specific security feature requirements and; (2) assurance requirements. The latter enable evaluation personnel to determine if the required features are present and functioning as intended.

The Orange Book criteria are applied to the set of security relevant software modules comprising a trusted computing base (TCB). For upper end secure systems (B2-A1), the TCB is a subset of the entire operating system; ie. the TCB is made up of the hardware and software that is security relevant and responsible for enforcing a security policy. For C1-B1 level systems the operating system interface and the TCB are one and the same.

It is not necessary to apply the Orange Book criteria to each system module individually. Thus some modules of a system may be completely untrusted, while others may be individually evaluated to a higher or lower evaluation class than the trusted product considered as a whole system.

In trusted products at the high end of the range, the strength of the reference monitor is such that most of the system modules can be completely untrusted. At the B3 level the reference monitor concept results in a security kernel that controls the access of users to information. The kernel must mediate all accesses, be protected from modification, and be verifiable as correct.