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.

The criteria in the Orange Book are intended to be application independent. Specific security requirements, however, may have to be interpreted when applying the criteria to systems with their own functional requirements, applications or special environments (e.g., communications processors, process control computers, and embedded systems in general).

The Orange Book addresses two types of access control - discretionary and mandatory. Discretionary access control (DAC) is the weaker of the two. It provides a means of restricting access to objects based on the identity of subjects and/or groups to which they belong. The controls are discretionary in the sense that a subject with a certain access permission is capable of passing that permission, directly or indirectly, to any other subject. The TCB of Division C systems includes provisions for DAC. This type of access protection is vulnerable to Trojan horse attack and can result in security problems related to inappropriate or unauthorized sharing of objects.

In Division B and higher systems mandatory access control (MAC) is required. The TCB restricts access to objects based on the sensitivity (as represented by a label) of the information contained in the objects and the formal authorization of subjects to access information of such sensitivity. Uses can specify and control sharing of objects and limit the propagation of access rights.

The Orange Book forms the basis upon which the National Computer Security Center (NCSC) conducts its commercial computer security evaluation process. This process is focused on commercially produced and supported general-purpose operating system products that meet the needs of government departments and agencies. The evaluation is aimed at off-the-shelf products and is completely separate from any considerations of overall system performance, potential applications, or processing environments. The evaluation can provide a key input to a computer system security approval/accreditation. However, it does not constitute a complete computer system security study. A complete study must consider additional factors dealing with the system in its unique environment, such as its proposed security mode of operation, specific users, applications, data sensitivity, physical and personnel security, administrative security and communications security.

3.0 TRUSTED NETWORK INTERPRETATION

The Red Book consists of two main sections and several appendices. Part I of the document provides interpretations of the Orange Book criteria for trusted computer/communications network systems. The specific security features, assurance requirements, and rating structure of the Orange Book are extended to networks of computers ranging from isolated local area networks to wide-area internetwork systems.

Part II describes a number of additional security services (e.g., communications integrity, denial of service, transmissions security) that arise in conjunction with networks. The full range of physical and administrative security measures appropriate to the highest sensitivity level of information on the network must be in place in order to operate a trusted network as described in the Red Book.

In the Red Book a network system is defined as the entire collection of hardware, firmware, and software necessary to provide a desired functionality. A component is any part of the system that, taken by itself, provides all or a portion of the total functionality required of a system.

The Red Book does not describe all the security requirements that may be imposed on a network. Depending upon the particular environment, there may be communications security, physical security, and other measures required.

One of the major objectives of the Red Book is to provide a metric by which to evaluate the degree of trust that can be placed in a given network system for processing sensitive information. This closely maps to a similar Orange Book objective for establishing a level of trust for operating systems. The evaluations for networks, however, are divided into two types: (1) an evaluation on a network product from a perspective that excludes the application environment; (2) an evaluation to assess whether appropriate security measures have been taken to permit the system to be used operationally in a specific environment (also known as a certification evaluation).

The completion of a formal product evaluation by the National Computer Security Center does not constitute certification for the system to be used in any specific environment. The evaluation report only provides a trusted network system's evaluation rating along with supporting data describing the product's strengths and weaknesses from a computer security point of view. The system

security certification procedure must still be followed before a network can be approved for use in processing or handling classified information.

The term integrity as used in the Red Book requires some explanation. In Part I integrity refers to the correct operation of the network trusted computer base hardware/firmware, and protection against unauthorized modification of labels and data. Division A and B networks must protect the labels that represent the sensitivity of information and the corresponding authorizations of users.

In Part II of the Red Book the term integrity relates to the mechanisms for information transfer between distinct components. This communications integrity includes the issues for correctness of message transmission, authentication of source/destination, data/control/protocol communication field correctness and related areas.

Depending upon the operational and technical characteristics of the environment in which a network exists, two different approaches for evaluation and certification are used in the Red Book. The first views the network as a collection of two or more interconnected separately accredited systems. The second, the "single trusted system" view point, establishes a single authority that has responsibility for security accreditation.

The former approach is a perspective that recognizes that parts of the network may be independently created, managed, and accredited. A joint approval process that describes the handling practices and classification levels that will be exchanged between the components involved is required. The range of sensitive information that may be exchanged between two activities must be agreed upon by each system's approving authorities. The range, however, cannot exceed the maximum sensitivity level in common between the two systems.

A "single trusted system" network implements a reference monitor to enforce the access of subjects to objects in accordance with an explicit and well defined network security policy. The network has a single trusted computing base that is partitioned among the network components in a manner that ensures the overall network security policy is enforced by the network as a whole. Every component that is trusted must enforce a component-level security policy that may contain elements of the overall network security policy. The sum of all component-level security policies must be shown to enforce the overall network security policy.

4.0 TRUSTED DATABASE MANAGEMENT SYSTEM INTERPRETATION

The **Trusted Database Management System Interpretation** (TDI) was prepared by the National Computer Security Center using inputs provided by the database vendor community, research community, and the community of commercial and governmental users. It is designed to be used in conjunction with the TCSEC and applies primarily to trusted, commercially available database management systems (DBMSs). The criteria can also be used to evaluate existing non-commercial DBMSs and for the specification of security requirements for DBMS acquisitions.

The interpretations in the TDI are a conservative application of TCSEC requirements and principles in a DBMS context. NCSC identifies several DBMS security issues that are not covered by the TDI. Included are:

1. Inference problems where derived information may be classified at a level above that of the provided information;

2. Aggregation problems in which the sensitivity level of a collection of data may exceed the sensitivity level of any individual datum in that collection;

3. Database integrity

NCSC anticipates that some of these issues will be dealt with in later versions of the TDI. The absence of these topics from the TDI reflects the lack of community consensus on solutions to these problems that are precise enough to be included within the evaluation process.

Appendix B of the TDI provides several example DBMS architectures and discusses the evaluation approach appropriate for each. The selected architectures include:

1. A trusted DBMS installed as an application on an evaluated trusted operating system, the DBMS providing only discretionary access control on specified DBMS objects;

2. A trusted DBMS that uses an underlying trusted operating systems's mandatory access control facilities to support isolation and tamper resistance arguments, while providing both mandatory and discretionary access control on its objects;

3. A partitioned system architecture with a database server;

4. A database architecture using trusted computing base augmentation;

5. An untrusted server architecture.

Each of the examples are described and then analyzed with respect to the definition of trusted computing base and other conditions identified in the TDI.

5.0 IT SECURITY CRITERIA - CRITERIA FOR THE EVALUATION OF THE TRUSTWORTHINESS OF INFORMATION TECHNOLOGY (IT) SYSTEMS

This document, often referred to as the German Green Book, was developed as a standard to be used to assess the trustworthiness of information technology (IT) systems. It should be noted that many of the ideas developed in the Green Book have been incorporated into the draft harmonized European ITSEC and superseded by that reference. Today the information in the Green Book is primarily historic in nature. It is discussed in this section of the report in order to illustrate the relationship between these two documents.

The Green Book states that the "criteria are a further development of the Orange Book." The objective is to provide a common set of evaluation criteria acceptable to manufacturers and users of IT systems. This position is not universally accepted. Some detractors argue that the functionality and assurance requirements described in the Green Book (and the ITSEC) do not compare closely enough to those in the Orange Book to be considered "common".

The Green Book employs a step-by-step approach to IT security. It begins by addressing the three basic threats:

1. Loss of confidentiality
2. Loss of integrity
3. Loss of availability

From these the document develops the concept of the security policy that the user of a system wants to enforce.

Eight basic security functions are described in the Green Book. These are:

1. Identification and authentication
2. Access control

3. Accountability
4. Audit
5. Object reuse
6. Accuracy
7. Reliability of service
8. Data exchange

The Green Book recognizes the fact that in the case of data communications it is not always possible to completely protect the communication channels by access control. Additional protection mechanisms are, therefore, introduced. For this purpose the protection mechanisms defined in **Security Addendum to OSI-Model ISO 7498-2-1988** were selected. Included are peer entity authentication, access control, data confidentiality, data integrity, data origin authentication, and non-repudiation.

The eight security functions are sufficient to enforce a very broad spectrum of security policies. In some circumstances not all of the functions will be necessary to enforce a policy. The Green Book identifies a series of topics that might be relevant for each of the eight security functions when defining a security policy. Users can employ a threat analysis method to analyze the topics and determine if any are useful to counter threats to the system.

In order to implement a security policy, mechanisms and/or algorithms are used. The mechanisms are rated according to their effectiveness in enforcing the security policy.

Ten classes of functionality are developed in the Green Book. The first five, F1 through F5, map closely to criteria of the Orange Book (C1, C2, B1, B2, B3/A1). Class F6 is for systems with high integrity requirements for data and programs such as would be the case with databases. Class F7 sets high requirements for the availability of a complete system or special functions of a system. An example would be process control systems. Functionality class F8 sets high requirements with regard to the safeguarding of data integrity during data communications. Systems with high demands on confidentiality of data during data communication, such as a crypto box, fall into class F9. Class F10 is intended for networks with high demands on the confidentiality and integrity of the information to be communicated. Sensitive information sent via insecure (e.g. public) networks are an example.

The final section of the Green Book contains a detailed list of criteria that permits one to rate the degree to which a system can be trusted. Eight hierarchical assurance levels, Q0 through Q7, are described. The principal elements considered in assigning a

trust rating are:

1. Quality of the security policy
2. Quality of the specifications of the system components to be evaluated
3. Quality of the mechanisms used
4. Quality of the separation from system components not to be evaluated
5. Quality of the software development process
6. Quality of the operational behavior
7. Quality of the user documentation

The Green Book clearly points out that using the criteria developed in the document only allows statements about the degree of trust with which a system enforces its security policy to be made. The IT security criteria are not meant to be used for evaluating the complete functionality of an IT system.

6.0 DRAFT INFORMATION TECHNOLOGY SECURITY EVALUATION CRITERIA

The Draft Information Technology Security Evaluation Criteria (ITSEC) of May, 1990 is an attempt on the part of four European nations, Germany, France, the Netherlands, and the United Kingdom, to build on and harmonize information technology (IT) security criteria. These four countries recognized that much work had already been done on the development of IT security evaluation criteria, although for slightly different objectives according to the specific requirements of the countries involved. They identified three major reasons for harmonization:

1. To combine and build on the experience of each of the countries in the area of IT;

2. Industry did not want different security in the different countries;

3. The basic concepts and approaches were the same, across countries and even across commercial, government, and defense applications.

The approach adopted by the four countries included taking the best features of what had already been developed and putting them in a consistent, structured perspective, and ensuring maximum compatibility with existing work, most notably the Orange Book. As noted earlier in the discussion of the Green Book this compatibility remains an unresolved issue.

In the ITSEC, security refers to confidentiality, integrity and availability. The ITSEC recognizes that security of an IT system can often be achieved through non-technical measures, such as organizational and administrative controls. Technical security measures are used to counter remaining threats.

The document makes a distinction between products and systems. An IT product is a hardware and/or software package that can be bought off-the-shelf and used in a variety of operational environments. An IT system is designed and built for the needs of a specific user; it has a unique operational environment. Both products and systems can be considered to be made up of components.

A system has a real world environment that can be defined and observed in detail. Security threats are real world threats. On the other hand, only general assumptions can be made about the operational environment of an IT product. It is up to the user, when incorporating the product into a real world system, to make certain these assumptions are consistent with the actual environment of the system.

The ITSEC uses the same criteria to deal with the security evaluation of both IT products and IT systems. The document uses the term Target of Evaluation (TOE) to refer to the product or system to be evaluated. Some components of a system or product will be relevant to security and others will not.

The functionality of a TOE consists of the security features of the TOE that contribute to security. In the ITSEC functionality is defined at three levels:

1. Security objectives - why the functionality is wanted

2. Security functions - what is actually done

3. Security mechanisms - how it is done

Security functions consist of features such as access control and audit. These functions are in turn implemented by a specific algorithm or logic; the mechanisms.

As in the German Green Book, the ITSEC defines ten functionality classes. The first five of these are compatible with requirements defined in the Orange Book.

In the ITSEC The security functions selected to satisfy the security objectives are one aspect of the technical security of a

system or product. Equally important is assurance - verification that the selected functions will satisfy the security objectives.

Assurance is addressed from both the correctness and effectiveness points of view. Seven levels of correctness (E0 through E6) have been defined. These represent ascending levels of confidence in the correctness of the security functions and mechanisms. E0 represents inadequate confidence in the correctness. E6 represents the highest level of confidence. Correctness is addressed from the point of view of construction of the TOE, covering both the development process and the development environment, and also the operation of the TOE. These levels map to the seven levels of assurance requirements in Orange Book classes D through A1.

If a TOE is successfully rated from the point of view of correctness it will be evaluated for effectiveness. This assesses whether the security functions and mechanisms that are provided in the TOE actually satisfy the security requirements. The TOE is evaluated for suitability of functionality, how the chosen functions work together, the consequences of known and discovered vulnerabilities, and ease of use. The strength of the security mechanisms against direct attack is also assessed.

Effectiveness levels are defined within the context of the correctness criteria. The requirements for effectiveness do not change by level, but rather build upon the correctness assessment and are performed to the same level of rigor as that assessment. If a TOE fails evaluation of either correctness or effectiveness, or cannot be completed for any other reason, it is assigned a rating of E0.

The ITSEC criteria are <u>not</u> a design guide for secure products or systems. It is the responsibility of the organization requesting the evaluation of the TOE to determine the security objectives and to choose the security functions to fulfill them. The ITSEC is an evolving document. It is expected that several additional versions will be produced before the participating nations agree on a final wording. It should also be noted that although the ITSEC discusses the integrity and availability problems it offers no solutions.

7.0 ANALYSIS AND COMPARISON OF SECURITY CRITERIA SETS

This section of the report will provide the following:

1. A discussion of the three U.S. security criteria documents (Orange Book, Red Book, TDI)

2. A comparison of the U.S. criteria and its European counterpart the ITSEC.

Note: Because the German Green Book has been superseded by and incorporated into the ITSEC no specific reference will be made to that criteria set.

7.1 U.S. SECURITY EVALUATION CRITERIA - ORANGE BOOK, RED BOOK, TDI

A criticism often made of the Orange Book is that it is dependent on security models that represent DoD national security concerns for protecting classified information from disclosure. As a result, the emphasis in the Orange Book is on confidentiality. For some organizations, however, the data integrity issue is a higher concern.

The Orange Book does not explicitly call out a set of data integrity-based access rules. It does, however, require B2-level systems and above to execute out of a protected domain, that is, that the TCB itself be a protected subsystem. The mechanism used to do this is usually, but not always, exported to applications. Thus an integrity mechanism is generally available as a byproduct of a system operating at the B2 level. The Orange Book criteria would have to be modified to mandate an integrity mechanism that provides for the integrity of information. In addition, the Orange Book lacks direction with respect to requirements for separation of duty, and access based on roles.

Another problem with the Orange Book is that it places great emphasis on controlling users yet virtually ignores the question of what those authorized users actually do with the information. It is built on the philosophy that if you can control who can get at the information, then you don't have to check the information itself. Many organizations need to provide controls for access to information, but have an equally important task of ensuring that the data is correct. The public would quickly loose confidence in an automated banking system that didn't provide such assurrances.

Because it adopts the DoD view that security is mainly a confidentiality issue, the Orange Book falls short of providing the model required by some users. Manufacturers and vendors of computer products that focus on the commercial, rather than the DoD market, often lack experience in interpreting and implementing Orange Book criteria. It is very likely that many of the vendors who will be competing for government contracts will fall into this category. This points out a need for a set of criteria that expands on the Orange Book and written in terms that commercial

designers can understand.

The Orange Book and Red Book criteria do not address all of the security concerns that arise when one actually deploys a system, whether it consists of a single computer or is composed of multiple computer and network products from different vendors. Procedural, physical and personnel safeguards enter into overall system security, and these are only partially addressed by these two documents. System security requires a thorough analysis of the system in question, taking into account not only the ratings of products that might be used to build the system, but also the threats directed against the system. Based on this analysis a security architecture can then be proposed and developed.

The ratings scheme used in the Orange Book and Red Book have led some users to apply product ratings to entire systems. Users must avoid the temptation of applying the environment guidelines developed in the Orange Book to entire systems. Complex networked computers are much more difficult to characterize from the security standpoint than are products.

In the Orange Book concept, trust is in an operating system residing on a host computer. This limitation led to the development of the Red Book which deals with network environments and the TDI which focuses on databases. None of these documents, however, addresses the multitude of complex security issues inherent in distributed host systems, a type of architecture that is becoming increasingly more widespread within private and government sectors.

Both the Red Book and the TDI extend the evaluation classes and provide interpretations of the Orange Book; the former for trusted computer/communications network systems, the latter for trusted database management systems. As refinements to the Orange Book, however, each of these documents share the previously noted criticisms of the parent document.

The TDI provides additional insight into the issues relevant in the design, implementation, evaluation, and accreditation of trusted database management systems. The Red Book extends the Orange Book criteria to networks of computers ranging from isolated local area networks to wide area internetwork systems. Both deal with issues of concern to many users in specifying and developing a modernized system architecture, but as stand-alone documents neither can be pointed to as providing a total solution.

7.2 U.S. vs. EUROPEAN SECURITY EVALUATION CRITERIA

Security evaluation criteria provide a standard for expressing security characteristics and establish an objective basis for evaluating a product relative to these characteristics. Criteria also serve as frameworks for users/purchasers and for manufacturers. Users employ criteria in the selection and acquisition of computer and network products. A user might rely on an independent evaluation of a product to validate vendor claims for security. A product rating could also be used in developing computer and network procurement requirements and specifications. Manufacturers rely on criteria for guidance in the development of products and use evaluations as a means of product differentiation.

The U.S. criteria sets (Orange Book, Red Book, TDI) and the European ITSEC represent different approaches to security evaluation. Each of the national sets reflects the trade-offs made by the developers of the security criteria in the areas of functionality and assurance.

Security functionality refers to the facilities by which security services are provided to users. These facilities may include access control mechanisms, audit, identification/authentication mechanisms and others. Systems differ in the number, type, and combination of security mechanisms provided. Differences in functionality are usually easy to understand because they result from mechanisms with which a user interacts.

Security assurance, on the other hand, is more abstract and thus harder to evaluate. A product rating intended to describe security assurance expresses an evaluator's degree of confidence in the effectiveness of the implementation of security functionality. As a result, criteria for assessing security assurance are based primarily on requirements for increasingly rigorous development practices, documentation, analysis, configuration management, and testing. Relative degrees of assurance may also be indicated by rankings based on the strength of underlying encryption mechanisms.

It is possible for two products that seem to provide the same security functionality to provide different levels of assurance. This can occur due to differences in the mechanisms used to implement the functionality or because of differing approaches to product development, documentation or testing.

The result is a dilemma for users and evaluators. Because of the complex technology involved in the field of computer and networks, users generally do not have the time, experience, or know-how to

evaluate the security assurance of a product. Even evaluators cannot examine every aspect of a computer system. Thus it becomes necessary to evaluate security assurance using indirect methods that involve analyzing development practices, documentation, testing, etc.

Assurance evaluation requires two steps. The first, design evaluation, attempts to assure that a particular proposed system design actually provides the functionality it attempts rather than simply appearing to do so. A design evaluation helps to uncover fundamental system design flaws. Step two is implementation evaluation. This is generally more difficult, costly and time consuming than design evaluation. Some critics have pointed out that the NCSC implementation evaluation process occurs after product implementation, thereby slowing the delivery of evaluated products to the marketplace.

The U.S. criteria and the ITSEC take different approaches to grouping functionality and assurance characteristics. In the Orange Book, functionality and assurance are combined to define a set of system security ratings that include four divisions (D,C,B,A), and classes within each. At the present time six classes, reflecting increasing provision for security, have been defined: C1, C2, B1, B2, B3, A1. In the U.S. criteria the language for expressing security characteristics and the basis for evaluation are embodied in the requirements for each division and class. This represents a highly bundled approach to criteria for each rating. B2, for example, is a combination of a set of security functions and security assurance attributes.

The ITSEC, the set of harmonized criteria developed by Germany, France, the Netherlands, and the United Kingdom, unbundles functional criteria and the correctness aspect of assurance for a TOE. Functional criteria are presently developed for ten classes. ITSEC functionality classes F1 to F5 correspond to Orange Book classes C1, C2, B1, B2, and B3. Using the notion of the "security target" it is possible for a user or manufacturer to define other functionality profiles to meet other defined sets of security needs. Correctness criteria, labeled E0 to E6, are intended to provide increased assurance. E2 through E6 map approximately to the assurance aspects of Orange Book classes C2 through A1. Functionality and assurance are evaluated independently in the ITSEC. This is a major difference between the U.S. and the European criteria sets.

There are advantages and disadvantages to the ITSEC approach. Dealing separately with functionality and assurance has the

potential for simplifying the evaluation process. It does, however, increase the number of rating combinations. Also the ITSEC does not require the security relevant parts of the system to be isolated into a TCB. Because this document is undergoing revision at this time it is too early to determine how effective this approach will be or if it will be modified.

Because it deals, at least in a limited fashion, with the issues of integrity and availability, the ITSEC goes beyond some of the ideas first introduced in the Orange Book. Neither of these documents, however, provides all the answers with respect to security evaluation criteria. For example, it has been suggested that the ITSEC ratings for integrity and availability be graded similarly to criteria F1 through F5 for confidentiality. This approach has recently been suggested by the Canadian government.

During the fall of 1990 a group of U.S., German, and U.K. scientists analyzed the ITSEC to determine what was involved in achieving compliance with an F5/E5 rating and what the impact would be upon a B3 targeted trusted system that was under development. A report of their findings entitled **Apparent Differences Between the U.S. TCSEC and the European ITSEC** was submitted to the 1991 IEEE Symposium on Research in Security and Privacy. The ITSEC was examined to determine how a trusted system could be evaluated as F5/E5 yet fail to meet B3 criteria, and how a system could be evaluated as B3 yet fail to meet F5/E5. Differences indicated places where a developer would have to do additional work to comply with both sets of criteria. The authors conclude that although the B3 and F5/E5 requirements are similar, a system targeted at one rating would not meet the other.

NIST, NCSC, and many other federal organizations, have furnished comments to the initial draft of the ITSEC. In general the U.S. is supportive of the European efforts to develop security evaluation criteria, but points out the need to give researchers the time and opportunity to build and evaluate products based on the ITSEC's concepts. A phased approach to the development of criteria is suggested by the U.S. In addition both NIST and NCSC stress a willingness to work with the European community on an international set of evaluation criteria.

From the political and commercial viewpoints the possibility of one universally accepted set of criteria is attractive. Multinational vendors of computer systems do not wish to incur the costs and delays associated with multiple evaluations under different national criteria sets. A standard criteria set would also eliminate the problem of one country refusing to recognize the

results of an evaluation performed by an organization in another country, for political or technical reasons.

8.0 TRUSTED SYSTEM TECHNOLOGY

NIST believes that a computer security protection strategy should consist of a mix of physical, administrative, and technical safeguards, including trusted system technology. This technology provides the methods and mechanisms within a computer system that are responsible for enforcing the security policy. The use of trusted system technology can be an effective part of a larger computer security protection strategy for satisfying confidentiality, integrity and availability requirements.

Government agencies must determine if they have a need for systems with trusted technology features. NCSC has published a list of evaluated products (EPL) from which agencies may select systems that best meet their security requirements. It must be remembered, however, that these products primarily address confidentiality requirements. Section 9.0 discusses some of the NIST, NSA and international efforts to develop criteria for achieving more effective integrity and availability controls in computer and telecommunications products.

In a multi-user environment, controlling user access to information is an important security concern. Using the C2 level criteria defined in the Orange Book will enable organizations to improve data confidentiality through discretionary access control. It should be noted that while access controls are a necessary part of achieving integrity and availability, there are other requirements for integrity and availability not covered by the Orange Book.

Mandatory separation of sensitive information is provided by the "B" division of the Orange Book. These types of systems enforce a mandatory access control or multi-level security policy. A risk analysis must be conducted to determine if such devices are cost effective.

Today more and more computers are being interconnected via networks and organized into distributed systems. In the federal government this has resulted in a complex situation in which many agencies require a mix of security requirements; some needing access control, some needing integrity control, and some needing both. To assist federal agencies in the future, NIST plans to develop additional guidance on how to use trusted system technology to protect computer systems containing sensitive information. That planned guide will include more detailed information on the extent

to which that technology provides system-level confidentiality, integrity and availability for unclassified systems. The planned guide will also stress the key point that the risk analysis-based process of identifying valid information protection is an essential prerequisite for determining the full set of protection mechanisms (trusted systems included) to be effectively applied to computer systems. This guide will provide users operating in an unclassified environment with guidance similar to that furnished in the NSA document, **Guidance for Applying the DoD Trusted Computer System Criteria in Specific Environments**, that focuses on trusted technology in systems processing classified information.

9.0 FUTURE U.S. EFFORTS IN THE DEVELOPMENT OF SECURITY CRITERIA

Neither the Orange Book nor the ITSEC address the entire spectrum of complex issues relating to the design, development and evaluation of trusted information systems. That process involves the specification of four separate and distinct types of requirements:

1. Requirements for the security-enforcing functions of the actual product or system;

2. Requirements for the design and development of the product or system;

3. Requirements for the evidence to be used in the evaluation of the trustworthiness of the product or system;

4. Requirements for the evaluation process to be used in assessing the trustworthiness of the product or system.

Each of these requirements classes is necessary to build trusted products and systems having a specified capability with a selected level of confidence in performance.

To address the shortcomings of existing U.S. and European security evaluation criteria, NIST and NCSC plan to work together for the next several years to develop new criteria, standards, and guidelines for designing and assessing the security of computer systems. This effort should lead to a new Federal Information Processing Standard (FIPS) specifying functional requirements for trusted information systems and identifying methods for their design and development. The planned standard will focus on NIST's responsibilities for protecting sensitive, unclassified information, consistent with the provisions of the Computer

Security Act of 1987. NSA will provide technical support to NIST for the development of the FIPS and use the standard to the maximum extent possible in fulfilling its responsibilities for protecting national security information. Integrity of computer systems and data will be emphasized in the new U.S. criteria set.

The cooperative effort between NIST and NSA will focus on the development of a common core of trust technology that supports diverse security objectives and that is broadly applicable to the Federal Government (civilian and military) and potentially the private sector. The agreement to cooperate in this joint venture reflects the commitment of both NIST and NSA to produce credible, widely-accepted standards to protect sensitive, unclassified Federal Government information assets.

User and vendor experiences with existing systems will be studied along with various alternatives for evaluating products and determining their conformance to specified requirements. The proposed set of security criteria will complement the Orange Book and where appropriate incorporate features of the ITSEC. The Orange Book and its supporting documents will serve as the initial basis for specifying requirements for security functions for trusted products and systems. The ITSEC will serve as the basis for specifying requirements for evidence to be used in the evaluation of trusted products and systems. To the greatest extent possible, the new FIPS will be based on an open systems approach.

NIST believes that it is important to get feedback from the user community with respect to security criteria they feel they need. For example, what are the requirements for B1 or B2 systems outside of the DoD? Is the level of assurance they provide really required? Does the current evaluation process make sense for NIST's constituents? Answers to questions such as these will drive the work on the new criteria standard and result in a new generation of evaluation criteria that expand on the current set of functional requirements for security and address issues such as networking and distributed databases.

Participation in computer security standards activities such as the ITSEC will enable NIST to influence criteria harmonization efforts on an international level. This will help provide the basis for international mutual recognition of security product evaluations.

The end results of this cooperative effort will be standards and guidelines to:

1. Assist developers in specifying requirements for designing and building trusted information systems;

2. Assist evaluators, certifiers and accreditors in assessing the trustworthiness of information systems;

3. Assist federal and private sector users in procuring, implementing, operating and administering trusted information systems.

10.0 CONCLUSIONS

Computer based information systems now play an important and often vital role in all sectors of the government and society. Whether for business, public sector or domestic use, the possibilities for access to these resources are becoming greater and more widespread. As a result, the risks, such as those associated with unauthorized access, or loss of integrity, are a cause for concern.

Awareness of risks has led to an increased use of information technology products to provide computer based solutions to security problems. In many environments these provide the principal means of preventing the theft or destruction of valuable assets.

Government agencies that are engaged in updating or replacing computer and telecommunications systems, are responsible for selecting products that provide security features commensurate with anticipated security risks. The selection should be based upon an analysis of the security risks for each system within its particular environment. The selected controls should address estimated risk and magnitude of potential loss of confidentiality, integrity and availability.

Lack of information about the strengths and weaknesses of particular products can result in over-investment in unnecessary features, or lead to an increased exposure to risk. Government agencies face several problems which can add to risks when purchasing products to meet security requirements. These include:

1. The security claims for a product may not be justified;

2. The security claims may be presented in a form which makes comparison between competing products difficult;

3. The products may interact with other products in a way that exposes a vulnerability;

4. The products may originate from a potentially unreliable source;

5. The products may have inadequate supporting documentation.

Each of the security criteria documents reviewed in this report has its strengths and weaknesses. With respect to the security requirements of many computer architectures none of the documents provides all the answers. Recognition of these shortcomings has led to the NIST/NCSC decision to create a set of federal evaluation criteria that will emphasize integrity and availability, in addition to confidentiality. Also NIST and NCSC are studying the need for security criteria in distributed computer systems to address integrity, availability and confidentiality of unclassified information.

NIST believes that users and manufacturers will both benefit from this approach. Users will gain from increased confidence in:

1. The suitability of security products they choose;

2. The security capabilities of the products they choose;

3. More cost effective security solutions.

Vendors of security products will gain from:

1. Targeting their future product developments to market requirements with greater confidence;

2. A fair and objective evaluation of their products;

3. Improved marketability of their products, perhaps internationally.

At the present time there is no standardized, independent and general means by which government agencies can determine a measure of confidence in the security provided by hardware and software products. What is desirable is a method of comparing differing security capabilities of similar products. Users also need a metric that allows them to determine how well the security features of particular products meet all or some of their security requirements when integrating a number of products to form a system. The recommendations expected from the new NIST/NCSC security criteria standard should provide some of the solutions and answers to this complex issue.

11.0 EPILOGUE

The analysis presented in this document was based on Version 1.0 (May 1990) of the ITSEC. Since that date Version 1.1 (Jan 1991), and Version 1.2 (June 1991) of the ITSEC have been released.

Version 1.0 underwent widespread international review by 20 countries. In September 1990, the Commission of European Countries sponsored a review conference that was attended by 500 experts in the field of information security. The comments received from this review were used to produce interim Version 1.1 in January 1991.

ITSEC Version 1.1 provided the basis for a further round of review, including written comments and a final review workshop, organized by the European Commission in April 1991. Fifty experts who had made a substantial contribution to the review of Version 1.0 participated. The result was Version 1.2 issued in June 1991.

To aid the process of further harmonization and development of security evaluation criteria, Version 1.2 has been adopted by the European Commission on a provisional basis for two years. The practical experience acquired will be used to review and further develop the ITSEC at the end of this period. In addition, considerations arising from further international harmonization will also be taken into account, relating in particular to the U.S. and Canadian approaches to evaluation. The long-term goal of this work is to enable international mutual recognition of evaluations.

12.0 REFERENCES

1. **Department of Defense Trusted Computer System Evaluation Criteria** (TCSEC); DoD 5200.28-STD; December 1985; also known as the Orange Book.[2]

2. **Trusted Network Interpretation**; NCSC-TG-005; July 1987; also known as the Red Book.

3. **Trusted Database Management System Interpretation**; NCSC-TG-021; August 1990; also known as the TDI

[2]Copies of the Orange Book and Red Book may be obtained from: Office of Standards and Products, National Computer Security Center, Fort Meade, MD 20755-6000, Attention: Chief, Computer Security Standards.

4. **IT Security Criteria - Criteria for the Evaluation of Trustworthiness of Information Technology (IT) Systems**; German Information Security Agency (GISA); 1st Version 1989; also known as the German Green Book

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

6. **NCSL Bulletin; Guidance to Federal Agencies on the Use of Trusted Systems Technology**; July 1990; published by the National Institute of Standards and Technology

7. **Analysis and Comments on the Draft Information Technology Security Evaluation Criteria (ITSEC)**; National Institute of Standards and Technology and National Computer Security Center; August 2, 1990

8. **Apparent Differences Between the U.S. TCSEC and the European ITSEC;** Dr. Martha A Branstad, Trusted Information Systems, Inc., USA; Dr. David Brewer, Gamma Secure Systems Ltd., UK; Mr. Christian Jahl, IABG Software Technology, Germany; Helmut Kurth, IABG Software Technology, Germany; Dr. Charles P. Pfleeger, Trusted Information Systems, Inc., USA; November 2, 1990

13.0 LIST OF ACRONYMS

DoD	Department of Defense
FIPS	Federal Information Processing Standard
GISA	German Information Security Agency
ISO	International Standards Organization
IT	Information Technology
ITSEC	"Information Technology Security Evaluation Criteria"
NCSC	National Computer Security Center
NIST	National Institute of Standards and Technology
NSA	National Security Agency
OSI	Open Systems Interconnection
TCB	Trusted Computing Base
TCSEC	"Trusted Computer Security Evaluation Criteria"
TDI	"Trusted Database Management System Interpretation"
TNI	"Trusted Network Interpretation"
TOE	Target of Evaluation

NIST-114A
(REV. 3-89)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY

BIBLIOGRAPHIC DATA SHEET

1. PUBLICATION OR REPORT NUMBER
NISTIR 4774

2. PERFORMING ORGANIZATION REPORT NUMBER

3. PUBLICATION DATE
MARCH 1992

4. TITLE AND SUBTITLE

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

5. AUTHOR(S)

Charles R. Dinkel

6. PERFORMING ORGANIZATION (IF JOINT OR OTHER THAN NIST, SEE INSTRUCTIONS)

U.S. DEPARTMENT OF COMMERCE
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
GAITHERSBURG, MD 20899

7. CONTRACT/GRANT NUMBER

8. TYPE OF REPORT AND PERIOD COVERED

9. SPONSORING ORGANIZATION NAME AND COMPLETE ADDRESS (STREET, CITY, STATE, ZIP)

10. SUPPLEMENTARY NOTES

[ ] DOCUMENT DESCRIBES A COMPUTER PROGRAM; SF-185, FIPS SOFTWARE SUMMARY, IS ATTACHED.

11. ABSTRACT (A 200-WORD OR LESS FACTUAL SUMMARY OF MOST SIGNIFICANT INFORMATION. IF DOCUMENT INCLUDES A SIGNIFICANT BIBLIOGRAPHY OR LITERATURE SURVEY, MENTION IT HERE.)

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.

12. KEY WORDS (6 TO 12 ENTRIES; ALPHABETICAL ORDER; CAPITALIZE ONLY PROPER NAMES; AND SEPARATE KEY WORDS BY SEMICOLONS)

computers; computer security; ITSEC; Orange Book; Red Book; security evaluation criteria; trust; trusted computer system

13. AVAILABILITY

[X] UNLIMITED

[ ] FOR OFFICIAL DISTRIBUTION. DO NOT RELEASE TO NATIONAL TECHNICAL INFORMATION SERVICE (NTIS).

[ ] ORDER FROM SUPERINTENDENT OF DOCUMENTS, U.S. GOVERNMENT PRINTING OFFICE, WASHINGTON, DC 20402.

[X] ORDER FROM NATIONAL TECHNICAL INFORMATION SERVICE (NTIS), SPRINGFIELD, VA 22161.

14. NUMBER OF PRINTED PAGES
29

15. PRICE
A03

ELECTRONIC FORM