USE OF THE TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA(TCSEC) FOR COMPLEX, EVOLVING, MULTIPOLICY SYSTEMS

NCSC TECHNICAL REPORT-002
Library No. S-241,321
July 1994

FOREWORD

This Technical Report "Use of the Trusted Computer System Evaluation Criteria (TCSEC) for Complex, Evolving, Multipolicy Systems," though addressing a more general problem, and not written in the form of an interpretation, is written in the spirit of the "Trusted Database Management System Interpretation (TDI) of The Trusted Computer System Evaluation Criteria." This approach can be used in conjunction with TDI developed systems **or** in the cases where the TDI does not apply. The document is intended to be used as a basis update to, NCSC-TG-024, Version 1, Volume 2/4, "A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators."

Recommendations for revision to this publication are encouraged and will be reviewed periodically by the NCSC. Address all proposals for revision through appropriate channels to:

National Computer Security Center
9800 Savage Road
Fort George G. Meade, MD 20755-6000

ATTN: Standards, Criteria, and Guidelines Division

*Reviewed by:*____
GLENN GOMES
Chief, INFOSEC Standards, Criteria & Guidelines Division

*Released by:*____
ROBERT J. SCALZI
Chief, INFOSEC Systems Engineering Office

ACKNOWLEDGEMENTS

This document was written by Howard L. Johnson of Information Intelligence Sciences, Inc., supported and revised by U.S. Army Major Melvin L. DeVilbiss. Besides many NSA organizations, the document was reviewed by Department of the Army (ASIS), DISA, Grumman, MITRE, and NAVELEXSECSEN.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

NSA recently published "Design and Evaluation of INFOSEC Systems: The Computer Security Contribution to the Composition Discussion" [1]. It discusses how the TNI [2] and the TDI [3] complement the TCSEC [4] and provide powerful tools for extensibility to INFOSEC systems. The problem addressed "for both designers and evaluators, is how to approach a complex system such that the elements derived from the high-level system objectives (in the TCSEC context) enforce the security policy and that they can be shown to compose those objectives."

This paper addresses a different problem (though often it is mistaken as the same). The audience addressed here includes procurement initiators, certification evaluators, and Designated Approving Authorities (DAAs). The objective is to deal with existing, evolving systems, where the individual elements support security policies but do not in general support high-level system objectives. This paper details how to develop a set of high-level system objectives and to retrofit system elements in a cost/risk effective manner to allow continued secure evolution, accreditation, and secure mission support.

Today there exists a tremendous investment in evolving Department of Defense (DoD) command and control systems made up of intercommunicating entities. Many of these systems were developed without a precisely defined set of system level security objectives or security preserving interface rules. Elements are often heterogeneous in the security policies supported, the degree of assurance provided, and the inherent trust present. Often cascading security risk has not been considered. Only classification data policies have been supported at the interfaces. Most importantly, these systems support highly sensitive and critical U.S. missions on a daily basis.

We endorse and support the goals and concepts of [1] in its context. It is believed, however, that new goals and concepts are needed to deal with the current "evolving system acquisition problem."

1.1 PURPOSE

The purpose of this paper is to provide a methodology to assist the heads of DoD components to procure, certify, and accredit existing, evolving, multipolicy systems against the TCSEC [4] requirements, consistent with the guidance provided in the TNI [2] and the TDI [3]. This methodology must come to grips with the problems that exist in current operational command and control systems. The intended audience is anyone concerned with any aspect of these objectives.

A more immediate goal, once these ideas have been finalized, is to develop a STRAWMAN follow-on version of Volume 2 of the Procurement Guideline Series "Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators [5]," but it will apply to complex systems. This will provide a way to extend the guideline's application from the procurement of Evaluated Products List (EPL) [6] products (or the equivalent) to procurement of integrated systems, encouraging maximum use of EPL products in the system development/evolution.

1.2 TODAY'S OPERATIONAL SYSTEMS

Operational systems continue to be developed for the military, adding custom built elements onto existing systems. Some elements still in use were developed in the 70s. The TCSEC [4], first published in 1983, was used selectively on a few experimental developments in the early 80s. The TCSEC [4] was not made a DoD standard until 1985 and was slow to be adopted into policies and directives of the individual services. Part of the reason was lack of guidance on adaptation to complex connected systems of the type being implemented. This void was partially filled by the publication of the TNI [2] in mid 1987, the update to DoDD 5200.28 [7] in 1988, and availability of "The Trusted Network Interpretation Environments Guideline [8]," in late 1990. Practical experience was gained in several pilot projects.

Today, guidance is still lacking on exactly how the TCSEC [4], used primarily for products, can be adapted to evolving, built-to-specification systems. Problems exist in downgrade, cascading risk, and contractual compromise; not to mention the unavailability of trained expertise for testing and evaluation. The result is a wide variation in trust and security, perpetuated by continued misconceptions about the adequacy of existing protection and the nature of potential threat.

The following is a list of problems that can be encountered in operational environments and represents problems that must be solved. **Components of existing/evolving systems:**

Seldom are on the Evaluated Products List (EPL) [6] - Although this will change in the future, existing operational systems often do not use NSA evaluated products.

Often have different policies - System components evaluated during certification against different Orange Book division/class requirements, different security modes, or different operational policies are often linked together in complex systems by busses and networks.

Have been built with conflicting regulatory policies - Rigor was employed to make the TCSEC [4] internally consistent. The TNI [2] and TDI [3] have also been written with this goal in mind. The basic DoD set of three documents (5200.28 directive [7], manual [9], and standard [4]) are also consistent, for the most part. However, existing systems have employed additional directives from each of the individual services and agencies. These documents can lag DoD documents because of lengthy update cycles or they can lead DoD documents based on preemptive need. (Sometimes internal service policy will be developed hoping that it will be subsequently adopted by the DoD.)

Have varying degrees of trust and assurance - Some system components have been operating since the 70's, others received initial accreditation before the TCSEC [4] became a requirement, some used the TCSEC [4] requirements, and a few use Evaluated Products List (EPL) [6] trusted technologies. Recertifications and reaccreditations often list many deficiencies, but with the risks accepted by DAAs (feeling the pressures of high corrective costs and operational immediacy).

Generally do not consider cascading risk - Until publication of the TNI [2], cascading risk was not fully understood or appreciated. DoDD 5200.28 [7] states that the DAA "should be aware that connection to a network may involve additional risks" and that the concern is only with "connections to adjacent AISs." This has given the DAA the flexibility to largely ignore cascading risk.

Only enforce "classification policy" at the interface - Policy at interfaces normally includes more than classifications and clearances. There are discretionary and category (compartment, caveat) considerations. The concept of least privilege and other privilege restrictions (e.g., two man rule) must be supported.

Do not have well stated, enforced global objectives - Connected trusted components of existing evolving systems support their individual assigned policies, but do not in general support a global policy, such as those addressed in the TNI [2] and TDI [3].

Are not always strictly reaccredited with each added element - Once an element has undergone rigorous certification evaluation, and has been used operationally, there is a reluctance to subject it to another recertification when elements are added to the connected system, even though additional risk may have been introduced.

Are often crucial to National defense - Especially in crisis situations (e.g., the Gulf War) security is considered a secondary objective and if there is any conflict with the primary mission, the security of the system may be sacrificed.

1.3 SECURITY POLICY

1.3.1 Regulatory Security Policy

In the controlled process of Computer Security (COMPUSEC) product evaluation, the primary requirements document is DoD 5200.28-STD [4]. In the operational DoD world, two additional documents are equally important: DoDD 5200.28 [7] and DoD 5200.28-M [9].

a. DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)" [7] - This Directive applies to all automated information systems processing classified, sensitive unclassified, or unclassified information. It specifies the applicability of DoD 5200.28-STD [4]. It also specifies that systems requiring at least controlled (C2) access based on the risk assessment procedure (i.e., not all users necessarily have the need-to-know for all information) must have been upgraded by the end of 1992. This directive identifies the relationships of other areas of security to COMPUSEC. Enclosure 4 to DoDD 5200.28 [7] provides the risk assessment procedure to be carried out to determine the operating mode and division/class required to support the system's environment.

b. DoD 5200.28-M, "Automated Information System Security Manual" (Draft) [9] - This manual specifies automated information system (AIS) security roles and responsibilities. It outlines the risk management process: threat assessment, risk analysis, cost benefit analysis, and the selection and implementation of safeguards. Certification and accreditation requirements are discussed. The document discusses the relationship of Security Test and Evaluation to other areas of testing. This document also addresses provisions of the Computer Security Act of 1987, not addressed in DoDD 5200.28 [7].

c. DoD 5200.28-STD, "DoD Trusted Computer System Evaluation Criteria" [4] - This standard, referred to as the "Orange Book," deals with confidentiality protection for classified and sensitive data. It contains a set of basic requirements and evaluation criteria for assessing the effectiveness of security protection features provided to an automated information system. It specifies the discretionary and mandatory security policies to be enforced and the rules for access control.

For each DoD organization, there are also regulations imposed by organization or application specific security documents as well.

1.3.2 Operational Security Policy

Operational security policy specifies the security critical aspects of the system and the manner in which the regulatory policy is to be satisfied. Operational security policy specifies the tradeoff decisions made by the DAA between COMPUSEC and other security methods of protection. It involves a functional allocation of the various security related tasks to the elements of the system. It identifies security clearance requirements for users of different system elements and isolates classified and unclassified data from other data within the system. It determines where users must access multiple security levels in near real-time.

The actual assignment of operational security policy is arbitrary in the sense that there are usually many ways to satisfy security requirements. Cost, performance, and risk tradeoffs will help determine the eventual way in which the system will be built and deployed. The operational security policy may change several times during development and even over the rest of the system life-cycle.

1.4 THE TCSEC, TNI, AND TDI

Figure 1 provides a simple depiction of the relationship between policy, component(s), and trusted computing bases (TCBs, defined in the glossary). The TCSEC [4] addresses a single TCB and pertains to a single policy (i.e., division/class). However, throughout the TCSEC [4] one finds system; computer system; assembly of hardware, software and firmware. It is easy to interpret the TCB as being within a component or across components. Thus, the relationship in Figure 1 is too simplistic to accurately portray the ideas of the TCSEC [4].

The TDI [3], like the TCSEC [4], deals with TCBs. TCB subsets are defined in the TDI [3] by a relationship between them called "primitive." Figure 2 shows two less primitive TCBs for which it is not possible to verify the specification of either without a statement about the specification of the more primitive TCB. One could imagine, for example, constructing a single network TCB and then attaching to it less primitive nodal TCBs, satisfying the TCB subset requirements of the TDI [3], and gaining the advantage of evaluation by parts.

Partial order is a necessary condition for the structure of TCB subsets. There are no examples in the TDI [3] of multiple "more primitive" TCBs, nor is there anything obvious that prevents the possibility.

Nothing appears to preclude different specifications from a subsetted architecture from being drawn from different division/classes, however, it is intuitive that as dependencies of a higher division/class less primitive subset become more complicated, that there is a greater chance that the lower division/class specifications of the more primitive subset will not meet the specifications of the former. It still does not invalidate this approach as a structure. It just means that the full benefits of the evaluation-by-parts approach cannot be realized.

Cascading risk occurs when a penetrator can take advantage of multiple TCBs to compromise information across a range of security levels that is greater than the accreditation range of any of the TCBs he/she must defeat to do so. Because different division/classes are not addressed directly in the TDI [3], neither is cascading risk.

The TNI [2] primarily addresses a single trusted system view, where a single policy lies across components and the single Network TCB (NTCB) can be partitioned across some of those network components. There is no requirement, or even expectation, that every component have a partition, nor that any partition comprise a complete TCB. Thus, the TNI [2] deals with a single policy supported across multiple components and a single TCB partitioned across multiple components. The TNI [2] supports evolving systems only to the extent that added components do not invalidate the NTCB.

The TNI [2] acknowledges the existence of interconnected, accredited AISs and states that "it may not be practical to evaluate such a network using this interpretation or to assign it a trusted system rating." The TNI [2] Appendix C describes the rules for connecting separate accredited AISs and the circumstances in which these rules apply. Included in this description is a discussion of operational security policy, though not specifically stated as such, in the form of interconnection rules and the cascading problem.

2 PROPOSED APPROACH

As was stated earlier, it is not designers and (product) evaluators to whom this paper is directed. This paper, and its concepts, is directed to procurement initiators, certification evaluators, and DAAs. Further, we are dealing with the difficult case where the system being considered is an existing, evolving, multiple policy system, is being dealt with.

Reference [1] strongly makes the point that:

Design and Analysis of Systems Proceeds <u>from</u> Policy <u>to</u> Mechanisms.

The TCSEC [4], the TNI [2], and the TDI [3] incorporate the Bell-La Padula rules for implementing the DoD security policy. The policy from which we begin here is the organization's operational security policy, which assumes the Bell-La Padula model and assigns the required security variables to elements of the system. A way to ensure a proper statement of the operational policy is through Domains of Constant Policy (DOCPs). In the rest of this section we will do the following:

- o Define domains of constant policy in such a way that it addresses evolution, multiple policy, and shared risk in connected systems.

- o Address interface policy required between intercommunicating DOCPs.

o Address global policy and its application to systems where global policy has not previously been concern.

The idea of domains of constant policy was presented in [10] as a way to better test systems. It was expanded in [11] to deal with requirements definition in a phased build.

2.1 DOMAINS OF CONSTANT POLICY (DOCPs)

The primary reason for defining DOCPs is to have an entity analogous to a single policy system to which a division/class of the TCSEC [4] applies. Thus, for each DOCP, our goal is to identify or provide a set of mechanisms and a level of assurance that would satisfy the prescribed division/ class. If this is done properly, certification evaluation can make the statement that the requirements of the division/class have been satisfied for this DOCP.

Simply defined, a DOCP is that part of a system to which a single, unique operational security policy has been defined. It follows then that DOCPs are nonoverlapping subsets of the system, that, in combination, completely cover the system, as shown in Figure 3. More rigorously defined, a DOCP consists of a well-defined boundary (where an isolation mechanism exists or can be employed) and an n-tuple of policy defining security characteristics. (The isolation is required to ensure that communications is taking place only over the known, designated channels.)

Each DOCP will have a TCB for support of its own security requirements, however, some of the mechanisms (e.g., audit) may be shared with another DOCP. The boundary may be created by physical isolation or logical isolation (e.g. supported by the TCB reference monitor, defined by cryptographic isolation, or use of guard isolation). The n-tuple that represents operational policy can be simple (clearance and classification levels) or complicated (with categories and other parameters). For the purposes of this document, the basic portion of the n-tuple will be values of the parameters:

Minimum classification of data

Maximum classification of data

Minimum security clearance

Maximum security clearance

Categories (compartments/caveats)

Build status (existing, EPL [6] product, to be built)

Level of assurance achieved (EPL [6] evaluation at some level, certification evaluation at some level, none, other).

The derived portion of the n-tuple will be the values of the parameters:

Risk index

Exposed risk index due to cascading (discussed further in section 3)

Mode

TCSEC [4] division/class.

Some clarifying comments should be made at this point of the discussion:

- One possible policy is "no policy," e.g., no confidentiality requirement, thereby requiring no trust technology.

- This approach does not preclude using TNI [2] and TDI [3] approaches in any way. It does, however, deal with the cases in which they cannot be employed. In the case of an NTCB, all policies are incorporated into a single DOCP. In the case of the TDI [3], one DOCP depends on the mechanisms of another DOCP to satisfy its TCB requirements.

- A DOCP is a working entity in the sense that (as will be seen later) tradeoff decisions concerning policy, costs, and mechanisms may make it necessary to change the operational policy and therefore the DOCPs.

- No attempt has been made here to deal with integrity or denial of service in this document, however such an extension has been included in a straight forward manner elsewhere.

The reasons DOCP use is recommended as the conceptual approach in existing, evolving systems instead of TCBs (TCB subsets or peer entity TCBs) are as follows:

- It offers a more concrete definition and intuitive notion to procurement administrators and DAAs.

- It enforces the statement of operational policy.

- Since the operational policy is defined by the using organization, then so are the DOCPs.

o It enforces precise system covering boundary definition.

o It is not constrained to components.

o It allows, and in fact encourages, cost risk tradeoffs and iteration of operational policy assignment.

o It allows application to the pre TCSEC [4], pre TNI [2] and/or pre TDI [3] systems where the definitions of TCB must be interpreted.

o It does not preclude, and in-fact supports, use of the NTCB or TCB subsetting requirements of the TNI [2] and TDI [3] respectively.

o It forces consideration of cascading, interface policy based on mutual suspicion, and global considerations, where in general no formal global policy has been enforced or evaluated for the connected system.

o It accommodates/promotes the use of EPL [6] products since the basic building block entity of a system (a DOCP) has a single policy represented by a division/class requirement of the TCSEC [4].

o It addresses security interface requirements which must be satisfied if an EPL [6] product component is going to be integrated into the overall security of the AIS system, which may in turn contain other EPL [6] products, existing secure systems, or "to be custom built" specifications.

The rest of this section will deal with some of the specific considerations in the DOCP approach.

2.1.1 Mechanisms

The mechanisms associated with a DOCP are illustrated in Figure 4. They correspond to what is required by the TCSEC [4]. The asterisks on the figure identify mechanisms that require global consideration. There are times in which the mechanism that satisfies the requirements of the domain of constant policy is actually outside the domain. This is equivalent to the dependencies that a less primitive TCB subset may have, as stated in the TDI [3]. For example, users might be identified in a different place or audit data may actually be collected and analyzed outside the domain. These mechanisms still must be assured to meet the requirements of this particular DOCP. The concept of global mechanisms will be discussed in Section 2.3.

2.1.2 Kinds of Isolation

Isolation, as referred to in the TCSEC [4], involves the responsibility within the TCB to provide isolation of separate domains under its control in response to the single security policy which it must support. This is usually done by the reference monitor, but other parts of the TCB also play a role. In many current implemented evolving multi-policy systems, the controls that represent the single TCBs have been individually certified, however, because no system level certifications have been accomplished, deficiencies exist at the data interfaces and in the policies that support those interfaces. Here, we are expanding beyond what is required of a single TCB to a more global consideration, that is, the isolation of individual Domains of Constant Policy from one another.

There are forms of isolation, other than logical, that exist in addition to what is accomplished by the reference monitor. They include electronic isolation, cryptographic isolation, and guard enforced isolation, each of which can be used effectively to separate DOCPs.

2.1.3 Phased Build

The "build" type and time are used as parameters in determining DOCPs. Any part of the system that exists and is being used in support of the operational mission has undergone the scrutiny of the certification/accreditation process (perhaps more than once) and has been used in the operational environment. Anything existing probably was built under a different set of rules than the ones that currently apply (TNI [2], TDI [3], and even in a few cases, TCSEC [4]). The existing part of the system may be further broken into several DOCPs because of policy differences.

An EPL [6] product is known to precisely follow the letter of the evaluated division/class from the TCSEC [4], and, if applicable, as interpreted by the TNI [2] or the TDI [3]. It will be assured to have the level of trust accorded that division/class rating in a non-application environment. The greatest difficulty is the adaptation to a more specific set of operational policies, its connectivity to other elements of the system, and their mutual satisfaction of the set of required global policies.

Any portion of the system to be built or modified (including the modification of an EPL [6] product) carries with it the highest risk. There are many reasons for this, not all of which apply to each specific development situation. The portion to be built may be complex or may require division into several DOCPs, thereby introducing technical risk. Contractors often have many requirements to satisfy, in addition to security, that may dilute the contractor's ability to provide security requirements with sufficient emphasis. The security experience of the design team is often not as great as it is in a continuing product line, thereby introducing additional risk. The requirements and guidance to the contractor for special security requirements within an application are often not as succinct as those provided by NSA in DoD 5200.28-STD [4] for a product to be evaluated. In a custom development, more cost risk exists because it is a one-time expenditure. Overruns in the development of a secure product can be amortized over many copies.

Note that there may be a great difference in assurance provided between existing systems, EPL [6] products, and developmental systems. This is considered as a separate factor in the next section. The boundaries of build type and homogeneous assurance often coincide.

2.1.4 Levels of Assurance

Even though the same division/class functional requirements are used, for any two parts of a given system, there may still be a disparity between the quality and completeness of assurance.

Factors include whether it is an approved EPL [6] product or a custom component, development configuration management, the qualifications of the people performing assurance functions, the environment of assurance, or the size and complexity of the system. One approach to measure and compensate for differences is to develop some criteria (e.g., figure-of-merit) for assurance, consider the figure-of-merit as a risk factor, and take action on those portions of the system that have the highest risk factors as funds become available. The action alternatives can be to shut down and rebuild the system, retest, upgrade and retest again, or change the operational policy that is supported. The following is a list of some of the measurement topics that can be employed in the figure-of-merit determination, in addition to what is stated in the TCSEC [4]:

o Point in time of development and evaluation with respect to publication and acceptance of the TCSEC [4], the TNI [2], the TDI [3] and other pertinent guidance documents.

o Time expended in assurance functions.

o Amount, quality, consistency, and completeness of evidence.

o Skill of team: academic, training, experience (EPL [6] product versus one-time build).

o Development and usage environment.

o Resolution of problems discovered (exception handling).

o The degree/quality of configuration control.

2.1.5 Policy Iteration

There is a high functional dependency between mechanism cost, security risk, and the functional assignment of operational policy; and therefore the allocation of DOCPs. There is normally an increase in number of TCBs with more DOCPs. This means more mechanisms and a higher security cost. However, more DOCPs can more closely model involved operational policies and therefore probably decrease the risk of policy violation.

If policy is changed to combine what used to be two DOCPs by broadening the policy range of each DOCP onto one DOCP, there can be an accompanying cost savings. The broadened policy range most often is accompanied by a risk increase (as illustrated by the risk assessment procedure in enclosure 4 of DoDD 5200.28 [7]). This risk increase for a new acquisition might drive the new single DOCP to support a higher division/class, thereby potentially increasing costs. In other cases, mutual boundaries can be moved to decrease mechanism cost.

Stated another way, two connected DOCPs will each have a risk index less than or equal to the risk index of a DOCP formed by combining them (e.g., two system high DOCPs have less than or equal risk than one two level DOCP.) Increasing the number of DOCPs has the potential to decrease the assessed risk, and never to increase it. Remember, the statements above are made **without** considering mechanisms.

The DAA must go through a cost/risk tradeoff and iteration procedure until he/she finds the appropriate operational policy (i.e., assignment of DOCPs) that best meet the needs of his/her system.

These are not new ideas. A system high or dedicated security mode is normally a combining of multiple policies to decrease mechanism cost. Nevertheless, in so doing, operational flexibility is decreased and the risk to operational security is increased by potentially creating a sizable downgrade problem.

2.2 INTERFACE POLICY

A system strictly designed and developed according to the subset TCB concept defined by the TDI [3] or the Network TCB concept of the TNI[2] need not consider additional interface or global policy. However, in situations where individual accredited entities have been connected, both interface policy and global policies must be supported. Interface policy will be discussed in this section and global policy will be discussed in Section 2.3.

In particular, there needs to be an explicit interface policy considered between each DOCP and every other DOCP with which it communicates. The interface policy can be thought of as an augmentation to the exportation policy of the TCSEC [4], however, in many cases, both exportation and importation concerns are expressed. The need for a trusted path to share and mediate security variables also should be assessed.

2.2.1 Communications Responsibility - Sending

In communications data, a DOCP must support intercommunication (exporting) policies established by its division/class.

A DOCP has two interface responsibilities: 1) it must ensure that data it sends continues to be supported by the policies imposed on it, and 2) it must appropriately handle data it receives based on any policy information known about that data.

External, intercommunicating domains of constant policy (physically interfacing or not) are of two types: virtual communication channels and trusted absorbing nodes. If the sending DOCP somehow specifies a destination other than a physically connected DOCP and the intermediate DOCPs have the primary responsibility of seeing that the data (and often its policy) proceeds to its correct destination, the intermediate DOCPs are virtual communication channels. It is up to the sending DOCP to ensure that the virtual communications channels and the destination can be trusted to transfer the data according to its policy.

A trusted absorbing node is a DOCP somewhere in the path to the destination that can be trusted to receive the data, properly interpret the policy, and incorporate the policy for that data into its TCB. If this is not the final destination of the data, the trusted absorbing node assumes the security responsibility. An intercommunicating DOCP may be considered both a virtual communications channel and a trusted absorbing node depending on the circumstances. Often the determination is difficult. The most conservative approach, if there is any question, is to treat the intermediate node as a virtual communication channel.

Policy must be established with the eventual data recipient or the first intermediate trusted node. The policy can be discretionary and or mandatory and includes categories (compartments, caveats, need to know). The responsibility for establishing the policy, linking it with the data, and assuring proper understanding by the receiver is that of the sender. Policy can be preestablished based on data identification through DOCP agreements, it can be communicated via labels, or it can be communicated and implemented manually by security administrators.

Sending DOCPs must be assured that data is being released into a system that can be trusted to interpret and carry out the policy. Factors to consider include the potential for eavesdropping, spoofing, or policy alteration.

2.2.2 Communications Responsibility - Receiving

Once data is in the possession of a trusted node or receiving DOCP, it becomes the responsibility of that DOCP's TCB to impose its knowledge of the policy on that data and treat it accordingly. Suspected or actual violations of interface policy must be treated as a special case and the data must be protected.

2.2.3 Exposed Risk

A DOCP may not be affordably and certifiably able to support division/class increases determined by considering exposed risk. Special communications mechanisms or added protection features within the potentially receiving DOCP may help to ameliorate this situation. This can provide an operational solution that must be agreed to by the potentially sending DOCP. In any case, the DAA from the sending DOCP ultimately has responsibility for the decision.

2.2.4 Mutual Suspicion

A sending DOCP must establish interface policy consistent with the level of trust it has established for potentially receiving DOCPs. If the level of trust determined does not coincide with the certification and/or accreditation level given that DOCP, the sending DOCP should further restrict the communication policy, beyond that normally implied by the TCSEC [4] and its interpretations, to a level where the sending DOCP is willing to accept the remaining risk. Similarly, if a receiving DOCP cannot trust the content or policy associated with data provided by another DOCP, then a receipt and handling policy must be established consistent with the risk the receiving DOCP is willing to accept. This policy may be more restrictive than required by the TCSEC [4] and its interpretations.

2.3 GLOBAL POLICY

These considerations pertain to systems for which there can be or has been no accreditation against a well defined global policy such as those stated in the TDI[3] TCB subset policy and the TNI [2] NTCB policy.

2.3.1 Shared Mechanisms

If TCBs share mechanisms (e.g., identification/authentication or audit) each individual TCB must be accredited with both using that mechanism. The DAA must use the evidence from those accreditations to ensure consistency with interface policy between the entities and any less primitive policy of which this shared mechanism is a part.

2.3.2 Discretionary Access Control

To be secure, the entire connected system should satisfy a single discretionary access control policy. This can only be accomplished by isolation of objects under protection of a single TCB to the subjects within that TCB. Otherwise, it must be accomplished by sharing access control mechanisms or sharing access control information between mechanisms. In older systems that do not allow subjects to access objects in other systems, this requirement is often satisfied because only standard messages are formatted and allowed to be transmitted. In these cases the subjects do not have access to objects beyond the scope of their own TCB.

2.3.3 Identification/Authentication

Even if each TCB has its own data for identification and authentication, the information for individual users that may potentially request access in more than one TCB or may have access to objects in more than one TCB must be consistent. The individual cannot assume more than one identity or be performing two functions simultaneously (unless the system has accounted for such support).

2.3.4 Audit

There must be a way to associate audit records generated by different TCBs for the same individual subject.

2.3.5 Security Administrator

Someone must be assigned the authority and assume the responsibility of security administrator for each of the TCBs. In addition, a security administrator must represent the authority of each hierarchical stage of DAAs.

2.3.6 Recovery

Implications of failure of one of the component TCBs must be reviewed from the standpoint of impact to all of the other intercommunicating entities. A way to cooperatively shut down and recover in a secure manner must exist.

2.3.7 Global Noncompliance

A TCB that has not been assured of external compliance with global considerations, yet still has been allowed to operate within a connected system, must be treated as a risk within itself, to other connected TCBs, and to the system.

3 RISK MANAGEMENT

Several topics of risk management are discussed in this section, including the following:

- Propagated risk assessment to account for cascading risk.
- Policy iteration to optimize operational policy resulting from this assessment.
- Assessment of the risk once the protection mechanisms have been determined.
- Design iteration to again adjust the operational policy based on the cost risk analysis.

Many of these concepts of propagated risk were previously presented in [12].

3.1 PROPAGATED RISK ASSESSMENT

One small part of the risk management process is the risk assessment procedure identified in DoDD 5200.28, enclosure 4 [7], and the resultant action taken by the DAA. The risk assessment procedure proposed here is a simple extension to the procedure in that enclosure, treating cascading risk in its simplest interpretation. By-products are summed contributions of risk that are management flags to the DAA indicating which elements of his/her system are the major risk contributors.

The risk assessment procedure is similar to that in "Trusted Network Interpretation Environments Guideline [8]," except that this document recognizes that cascading risk does not just result from contiguous components.

The risk inherent to a DOCP is calculated from DoDD 5200.28, enclosure 4 [7], as if the DOCP were in isolation, and is called <u>inherent risk</u>. The <u>exposed risk</u> is the amount of change (increase) in DOCP risk resulting from consideration of cascading risk from all other DOCPs. This parameter may result in a change to the risk index and potentially assigned division/class. In the search for increased exposed risk, the search may end along a single path once a previously evaluated trusted absorbing node is encountered. Otherwise the search is to each logical receiver of data.

<u>Contributed risk</u> is the summed amount of increase in exposed risk potentially contributed by a single DOCP to all other DOCPs. (Two DOCPs could potentially change the risk level of a third DOCP from its original level, but in the analysis technique, only one actually does. Nevertheless, they both receive an increase in contributed risk.) <u>Solely contributed risk</u> is the risk contributed by a DOCP which could not have been also contributed by another DOCP.

Cascading risk is determined by the exposed risk factor. This parameter results in a change to the risk index and potentially the assigned division/class. the exposed risk can only be decreased by changing either the local operational policies or the operational policies of the contributing DOCPs. **The contributed risk factors are an indicator to the DAA where the changing of policy or the implementation of mechanisms (e.g., security guards), for example, can do the most good in reducing the risk of the overall system.**

The four risk factors (risk index, exposed risk index, contributed risk, and solely contributed risk) become part of the system "operational security policy." The procedure in DoDD 5200.28 enclosure 4 [7] deals only with security levels and clearances.

3.2 POLICY ITERATION

Before mechanisms are considered in the solution, Figure 5 shows how the operational requirements specification can be iterated, along with the definitions of DOCPs, based on risk considerations. The two contributed risk factors help identify to the DAA the areas where changes in operational policy can have the largest risk reduction advantage. The propagated risk assessment is reaccomplished to assess the shared risk aspects of the adjustments.

3.3 PROTECTION ASSESSMENT

The next step considers existing or planned security mechanisms. Compatibility with division/class criteria, use of downgrade guards, existence of interface enforcement mechanisms, and the approach to global enforcement are all important considerations. Temporal inconsistencies and potential vulnerabilities are assessment concerns, as are trusted startup, shutdown and recovery.

Besides protection mechanism assessment, there needs to be an assessment of assurance. This includes determining the evaluation rigor used, or planned to be used, in testing and evaluating the DOCP. This assessment uses the figures-of-merit approach discussed earlier.

3.4 DESIGN ITERATION

The second iteration, illustrated in Figure 6, like the first iteration, allows reexamination of the process all the way back to the specification of operational policy, modification of DOCPs, and respecification of interface policies to the identification mechanisms. The two contributed risk factors again help identify to the DAA areas where changes in operational policy can have the largest risk and cost reduction advantage. The protection assessment can be reaccomplished. What remains is a statement of the residual risk within the system. The DAA must determine what additional corrections or operational constraints must be observed to declare the system accredited to operate in the environment. **The final statement of operational security policy and mechanism architecture is then used as the basis for certification evaluation and accreditation.**

4 SUMMARY

This paper has introduced a way to deal with evolving, multipolicy systems using the TCSEC [4]. Rules are provided for the assembly and assurance of existing, new build, and EPL [6] components. This approach considers cascading risk and accommodates operational downgrade through data guards, an approach often used by the military to eliminate unnecessary policy constraints. This approach incorporates risk assessment. It provides an easily recognized strategy to the DAA for reducing risk with the minimum expenditure of funds. This approach also specifies assurance deficiencies in the system and helps to provide a strategy for correcting these deficiencies.

The domains of constant policy approach is a major step toward achieving the security recommended in the network TCB approach of the TNI [2] and the TCB approach recommended in the TDI [3] for evolving systems. In many cases the goal can be achieved without major redesign of existing systems. As systems continue to evolve, adding more function and capability, rigorous security goals can be realized.

BIBLIOGRAPHY

[1] C Technical Report 32-92, "The Design and Evaluation of INFOSEC Systems: The Computer Security Contribution to the Composition Discussion," June 1992

[2] NCSC-TG-005, "Trusted Network Interpretation (TNI) of the Trusted Computer System Evaluation Criteria(TCSEC)," National Security Agency, July 31, 1987

[3] NCSC-TG-021 "Trusted Database Management System Interpretation (TDI) of The Trusted Computer System Evaluation Criteria (TCSEC)," National Security Agency, April 1991

[4] DoD 5200.28-STD, "Department of Defense Trusted Computer System Evaluation Criteria," December 1985

[5] NCSC-TG-024, Version 1

Volume 1/4, "A Guide to Procurement of Trusted Systems: An Introduction to Procurement Initiators on Computer Security Requirements," December 1992

Volume 2/4, "A Guide to Procurement of Trusted Systems: Language for RFP Specifications and Statements of Work - An Aid to Procurement Initiators," June 30, 1993

Volume 3/4, "A Guide to Procurement of Trusted Systems: Computer Security Contract Data Requirements List and Data Item Descriptions Tutorial," February 28, 1994

Volume 4/4, "A Guide to Procurement of Trusted Systems: How to Evaluate a Bidder's Proposal Document - An Aid to Procurement Initiators **and** Contractors," (Draft)

[6] "Information Systems Security Products and Services Catalogue," Prepared by the National Security Agency, (Published Quarterly)

[7] DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," March 21, 1988

[8] NCSC-TG-011, "Trusted Network Interpretation Environments Guideline," National Security Agency, August 1, 1990

[9] DoD 5200.28-M, (Draft) "Automated Information System Security Manual," April 29, 1991

[10] Johnson, H.L., "An Approach to Security Test," AFCEA 4th Annual Symposium on C3I Technology, Information and Security, Philadelphia, PA, August 16-18, 1988

[11] AFSSM 5031, "Complex System Guide," Air Force Special Security Instruction," Air Force Cryptologic Support Center, Air Force Intelligence Command, 1991

[12] Johnson, H.L., and J.D. Layne, "Modeling Security Risk in Networks," Proceedings 11th National Computer Security Conference, NIST and NCSC, October 17-20, 1988, pp. 59-64

ACRONYMS

AIS	Automated Information System
COMPUSEC	Computer Security
DAA	Designated Approving Authority
DOCP	Domain of Constant Policy
DoD	Department of Defense
EPL	Evaluated Products List
INFOSEC	Information Security
NTCB	Network Trusted Computing Base
RFP	Request for Proposal
TCB	Trusted Computing Base
TCSEC	Trusted Computer System Evaluation Criteria
TDI	Trusted Database Management System Interpretation
TNI	Trusted Network Interpretation

GLOSSARY

Automated Information System - An assembly of computer hardware, software, and/or firmware configured to collect, create, communicate, compute, disseminate, process, store, and/or control data or information. (DoDD 5200.28)

Automated Security Policy - The set of restrictions and properties that specify how an AIS supports the Security Policy.

Certification - The technical evaluation of an AIS's security features and other safeguards, made in support of the accreditation process, which establishes the extent that a particular AIS design and implementation meets a set of specified security requirements. (DoDD 5200.28)

Certification Evaluation - (See Certification and Evaluation)

Contributed Risk - The summed amount of increase in exposed risk to all other DOCPs potentially contributed by a single DOCP.

Depends - A TCB subset depends (for its correctness) on TCB subset B if and only if the (engineering) arguments of the correct implementation of A with respect to its specification assume, wholly or in part, that the specification of B has been implemented correctly. (NCSC-TG-021)

Domain - The unique context in which a program is operating; in effect, the set of objects that a subject has the ability to access.

Domain of Constant Policy - That part of a system to which a single, unique operational security policy has been defined. DOCPs are nonoverlapping subsets of the system, that, in combination, completely cover the system. A DOCP consists of a well-defined boundary (where an isolation mechanism exists or can be employed) and an n-tuple of policy defining security characteristics.

Evaluation - Two types of evaluation are referred to: product evaluation and certification evaluation.

Exposed Risk - The amount of change (increase) in DOCP risk resulting from consideration of cascading risk from all other DOCPs. This parameter results in a change to risk index and potentially the assigned division/class.

Inherent Risk - Calculated risk for the element as if it were in isolation.

Network Trusted Computing Base - The totality of the protection mechanisms within a network system - including hardware, firmware, and software - the combination of which is responsible for supporting security policy. (NCSC-TG-005)

NTCB Partition - The totality of mechanisms within a single network component for enforcing the network policy, as allocated to the component; the part of the NTCB within a single network component.

Operational Security Policy - The policy decisions made by the DAA in accordance with DoDD 5200.28 (policy concerning security levels of user, classifications of data, security mode and assignment of all the above to different elements of the system). (NCSC-TG-005)

Primitive - An ordering relation between TCB subsets based on dependency (see "depends" above). A TCB subset B is more primitive than a second TCB subset A (and A is less primitive than B) if (a) A directly depends on B or (b) a chain of TCB subsets from A to B exists such that each element of the chain directly depends on its successor in the chain. (NCSC-TG-021)

Product - Used here in the same sense as used in the EPL, NSA Information System Security Products and Services Catalogue.

Product Evaluation - An evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. This term is used here in the same sense as used in the EPL, NSA Information System Security Products and Services Catalogue.

Regulatory Security Policy - Security policy represented by regulatory documents imposed on the procurement organization (especially DoDD 5200.28, DoD 5200.28-M, and DoD 5200.28-STD).

Security Evaluation - An evaluation accomplished to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done for the purpose of assessing a system's security safeguards with respect to a specific operational mission and is a major step in the certification and accreditation process.

Security Policy - The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Solely Contributed Risk - The risk contributed by a DOCP to another DOCP that was not also contributed by another DOCP.

System - (See Automated Information System)

TCB Subset - A set of software, firmware, and hardware (where any of these three could be absent) that mediates the access of a set S of subjects to a set O of objects on the basis of a stated access control policy P and satisfies the properties:

(1) M mediates every access to objects O by subjects in S,

(2) M is tamper resistant; and,

(3) M is small enough to be subject to analysis and tests, the completeness of which can be assured.

(NCSC-TG-021)

Trusted absorbing Node - A DOCP somewhere in the path from the sending DOCP to the destination DOCP that can be trusted to receive the data, properly interpret the policy, and incorporate the policy for that data into its TCB. If this is not the final destination, the trusted absorbing node takes the security responsibility from the sending DOCP from that point on. It is the responsibility of the sending DOCP to communicate the data, the recipient DOCP, and the appropriate policy to the trusted Absorbing Node.

Trusted Computing Base (TCB) - The totality of protection mechanisms within a computer system - including hardware, firmware, and software, the combination of which is responsible for enforcing security policy.

Virtual Communications Channel - If a sending DOCP somehow specifies a destination other than a physically connected DOCP, and the intermediate DOCPs each have the responsibility of seeing that the data (and often its policy) gets to its correct destination, these DOCPs are called virtual communication channels. It is up to the sending DOCP to be assured that the virtual communications channels and the destination can be trusted to transfer the data according to its policy.