Security Requirements for a

Class A1 M-Component

DIVISION A: VERIFIED PROTECTION

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

CLASS (A1): VERIFIED DESIGN

SYSTEMS IN CLASS (A1) ARE FUNCTIONALLY EQUIVALENT TO THOSE IN CLASS (B3) IN THAT NO ADDITIONAL ARCHITECTURAL FEATURES OR POLICY REQUIREMENTS ARE ADDED. THE DISTINGUISHING FEATURE OF SYSTEMS IN THIS CLASS IS THE ANALYSIS DERIVED FROM FORMAL DESIGN SPECIFICATION AND VERIFICATION TECHNIQUES AND THE RESULTING HIGH DEGREE OF ASSURANCE THAT THE NTCB IS CORRECTLY IMPLEMENTED. THIS ASSURANCE IS DEVELOPMENTAL IN NATURE, STARTING WITH A FORMAL MODEL OF THE SECURITY POLICY AND A FORMAL TOP-LEVEL SPECIFICATION (FTLS) OF THE DESIGN. INDEPENDENT OF THE PARTICULAR SPECIFICATION LANGUAGE OR VERIFICATION SYSTEM USED, THERE ARE FIVE IMPORTANT CRITERIA FOR CLASS (A1) DESIGN VERIFICATION:

- A FORMAL MODEL OF THE SECURITY POLICY MUST BE CLEARLY IDENTIFIED AND DOCUMENTED, INCLUDING A MATHEMATICAL PROOF THAT THE MODEL IS CONSISTENT WITH ITS AXIOMS AND IS SUFFICIENT TO SUPPORT THE SECURITY POLICY.
- AN FTLS MUST BE PRODUCED THAT INCLUDES ABSTRACT DEFINITIONS OF THE FUNCTIONS THE NTCB PERFORMS AND OF THE HARDWARE AND/OR FIRMWARE MECHANISMS THAT ARE USED TO SUPPORT SEPARATE EXECUTION DOMAINS.
- THE FTLS OF THE NTCB MUST BE SHOWN TO BE CON-SISTENT WITH THE MODEL BY FORMAL TECHNIQUES WHERE POSSIBLE (I.E., WHERE VERIFICATION TOOLS EXIST) AND INFORMAL ONES OTHERWISE.
- THE NTCB IMPLEMENTATION (I.E., IN HARDWARE, FIRMWARE, AND SOFTWARE) MUST BE INFORMALLY SHOWN TO BE CONSISTENT WITH THE FTLS. THE ELEMENTS OF THE FTLS MUST BE SHOWN, USING INFORMAL TECH-NIQUES, TO CORRESPOND TO THE ELEMENTS OF THE NTCB. THE FTLS MUST EXPRESS THE UNIFIED PROTEC-TION MECHANISM REQUIRED TO SATISFY THE SECURITY POLICY, AND IT IS THE ELEMENTS OF THIS PROTECTION MECHANISM THAT ARE MAPPED TO THE ELEMENTS OF THE NTCB.
- FORMAL ANALYSIS TECHNIQUES MUST BE USED TO IDEN-TIFY AND ANALYZE COVERT CHANNELS. INFORMAL TECH-NIQUES MAY BE USED TO IDENTIFY COVERT TIMING CHANNELS. THE CONTINUED EXISTENCE OF IDENTIFIED COVERT CHANNELS IN THE SYSTEM MUST BE JUSTIFIED. IN KEEPING WITH THE EXTENSIVE DESIGN AND DEVELOP-MENT ANALYSIS OF THE NTCB REQUIRED OF SYSTEMS IN CLASS (A1), MORE

STRINGENT CONFIGURATION MANAGE-MENT IS REQUIRED AND PROCEDURES ARE ESTABLISHED FOR SECURELY DISTRIBUTING THE SYSTEM TO SITES. A SYSTEM SECURITY ADMINISTRATOR IS SUPPORTED.

THE FOLLOWING ARE MINIMAL REQUIREMENTS FOR SYSTEM ASSIGNED A CLASS (A1) RATING:

Security Policy [4.1.1]

- Statement from DoD 5200.28-STD

Implied from the Introduction to the TCSEC.

- Interpretation

The network sponsor shall describe the overall network security policy enforced by the NTCB. At a minimum, this policy shall include the discretionary and mandatory requirements applicable to this class. The policy may require data secrecy, or data integrity, or both. The policy is an access control policy having two primary components: mandatory and discretionary. The policy shall include a discretionary policy for protecting the information being processed based on the authorizations of individuals, users, or groups of users. This access control policy statement shall describe the requirements on the network to prevent or detect "reading or destroying" sensitive information by unauthorized users or errors. The mandatory policy must define the set of distinct sensitivity levels that it supports. For the Class B1 or above the mandatory policy shall be based on the labels associated with the information that reflects its sensitivity with respect to secrecy and/or integrity, where applicable, and labels associated with users to reflect their authorization to access such information. Unauthorized users include both those that are not authorized to use the network at all (e.g., a user attempting to use a passive or active wire tap) or a legitimate user of the network who is not authorized to access a specific piece of information being protected.

Note that "users" does not include "operators," "system programmers," "technical control officers," "system security officers," and other system support personnel. They are distinct from users and are subject to the Trusted Facility Manual and the System Architecture requirements. Such individuals may change the system parameters of the network system, for example, by defining membership of a group. These individuals may also have the separate role of users.

> SECRECY POLICY: The network sponsor shall define the form of the discretionary and mandatory secrecy policy that is enforced in the network to prevent unauthorized users from reading the sensitive information entrusted to the network.
>
> DATA INTEGRITY POLICY: The network sponsor shall define the discretionary and mandatory integrity policy to prevent unauthorized users from modifying, viz., writing, sensitive information. The definition of data integrity presented by the network sponsor refers to the requirement that the information has not been subjected to unauthorized modification in the network. The mandatory integrity policy enforced by the NTCB cannot, in general, prevent modification while information is being transmitted between components. However, an integrity sensitivity label may reflect the confidence that the information has not been subjected to transmission errors because of the protection afforded during transmission. This requirement is distinct from the requirement for label integrity.

- Rationale

The word "sponsor" is used in place of alternatives (such as "vendor," "architect," "manufacturer," and "developer") because the alternatives indicate people who may not be available, involved, or relevant at the time that a network system is proposed for evaluation. A trusted network is able to control both the reading and writing of shared sensitive information. Control of writing is used to protect against destruction of information. A network normally is expected to have policy requirements to protect both the secrecy and integrity of the information entrusted to it. In a network the integrity is frequently as important or more important than the secrecy requirements. Therefore the secrecy and/or integrity policy to be enforced by the network must be stated for each network regardless of its evaluation class. The assurance that the policy is faithfully enforced is reflected in the evaluation class of the network.

This control over modification is typically used to protect information so that it may be relied upon and to control the potential harm that would result if the information were corrupted. The overall network policy requirements for integrity includes the protection for data both while being processed in a component and while being transmitted in the network. The access control policy enforced by the NTCB relates to the access of subjects to objects within each component. Communications integrity addressed within Part II relates to information while being transmitted.

The mandatory integrity policy (at class B1 and above) in some architectures may be useful in supporting the linkage between the connection oriented abstraction introduced in the Introduction and the individual components of the network. For example, in a key distribution center for end-to-end encryption, a distinct integrity category may be assigned to isolate the key generation code and data from possible modification by other supporting processes in the same component, such as operator interfaces and audit. The mandatory integrity policy for some architecture may define an integrity sensitivity label that reflects the specific requirements for ensuring that information has not been subject to random errors in excess of a stated limit nor to unauthorized message stream modification (MSM) -. The specific metric associated with an integrity sensitivity label will generally reflect the intended applications of the network.

Mandatory Only Components (M-Components) [A.3.1]

Mandatory Only Components are components that provide network support of the MAC Policy as specified in the Network Interpretation of the DoD Trusted Computer System Evaluation TCSEC. M-Components do not include the mechanisms necessary to completely support any of the 3 other network policies (i.e., DAC, Identification-Authentication, and Audit) as defined in the Interpretation.

In the requirements referenced, TCB will be understood to refer to the NTCB Partition of the M-Component. Also any reference to audit for an M-Component will be interpreted to mean "the M-Component shall produce audit data about any auditable actions performed by the M-Component". In addition the M-Component shall contain a mechanism for making the audit data available to an audit collection component.

1. Object Reuse [4.1.1.2]

- Statement from DoD 5200.28-STD

All authorizations to the information contained within a storage object shall be revoked prior to initial assignment, allocation or reallocation to a subject from the TCB's pool of unused storage objects. No information, including encrypted representations of information, produced by a prior subject's actions is to be available to any subject that obtains access to an object that has been released back to the system.

- Interpretation

The NTCB shall ensure that any storage objects that it controls (e.g., message buffers under the control of a NTCB partition in a component) contain no information for which a subject in that component is not authorized before granting access. This requirement must be enforced by each of the NTCB partitions.

- Rationale

In a network system, storage objects of interest are things that the NTCB directly controls, such as message buffers in components. Each component of the network system must enforce the object reuse requirement with respect to the storage objects of interest as determined by the network security policy. For example, the DAC requirement in this division leads to the requirement here that message buffers be under the control of the NTCB partition. A buffer assigned to an internal subject may be reused at the discretion of that subject which is responsible for preserving the integrity of message streams. Such controlled objects may be implemented in physical resources, such as buffers, disk sectors, tape space, and main memory, in components such as network switches.

2. Labels [4.1.1.3]

- Statement from DoD 5200.28-STD

Sensitivity labels associated with each ADP system resource (e.g., subject, storage object, ROM) that is directly or indirectly accessible by subjects external to the TCB shall be maintained by the TCB. These labels shall be used as the basis for mandatory access control decisions. In order to import non-labeled data, the TCB shall request and receive from an authorized user the sensitivity level of the data, and all such actions shall be auditable by the TCB.

- Interpretation

Non-labeled data imported under the control of the NTCB partition will be assigned a label constrained by the device labels of the single-level device used to import it. Labels may include secrecy and integrity[1] components in accordance with the overall network security policy described by the network sponsor. Whenever the term “label” is used throughout this interpretation, it is understood to include both components as applicable. Similarly, the terms “single-level” and “multilevel” are understood to be based on both the secrecy and integrity components of the policy. The mandatory integrity policy will typically have requirements, such as the probability of undetected message stream modification, that will be reflected in the label for the data so protected. For example, when data is imported its integrity label may be assigned based on mechanisms, such as cryptography, used to provide the assurance required by the policy. The NTCB shall assure that such mechanism are protected from tampering and are always invoked when they are the basis for a label.

If the security policy includes an integrity policy, all activities that result in message-stream modification during transmission are regarded as unauthorized accesses in violation of the integrity policy. The NTCB shall have an automated capability for testing, detecting, and reporting those errors/corruptions that exceed specified network integrity policy requirements. Message-stream modification (MSM) countermeasures shall be identified. A technology of adequate strength shall be selected to resist MSM. If encryption methodologies are employed, they shall be approved by the National Security Agency.

All objects must be labeled within each component of the network that is trusted to maintain separation of multiple levels of information. The label associated with any objects associated with single-level components will be identical to the level of that component. Objects used to store network control information, and other network structures, such as routing tables, must be labeled to prevent unauthorized access and/or modification.

- Rationale

The interpretation is an extension of the requirement into the context of a network system and partitioned NTCB as defined for these network interpretations. A single-level device may be regarded either as a subject or an object. A multilevel device is regarded as a trusted subject in which the security range of the subject is the minimum-maximum range of the data expected to be transmitted over the device.

The sensitivity labels for either secrecy or integrity or both may reflect non-hierarchical categories or hierarchical classification or both.

[1] See, for example, Biba, K.J., “Integrity Consideration for Secure Computer Systems,” ESD-TR-76-372, MTR-3153, The MITRE Corporation, Bedford, MA, April 1977.

For a network it is necessary that this requirement be applied to all network system resources at the (B2) level and above.

The NTCB is responsible for implementing the network integrity policy, when one exists. The NTCB must enforce that policy by ensuring that information is accurately transmitted from source to destination (regardless of the number of intervening connecting points). The NTCB must be able to counter equipment failure, environmental disruptions, and actions by persons and processes not authorized to alter the data. Protocols that perform code or format conversion shall preserve the integrity of data and control information.

The probability of an undetected transmission error may be specified as part of the network security policy so that the acceptability of the network for its intended application may be determined. The specific metrics (e.g., probability of undetected modification) satisfied by the data can be reflected in the integrity sensitivity label associated with the data while it is processed within a component. It is recognized that different applications and operational environments (e.g., crisis as compared to logistic) will have different integrity requirements.

The network shall also have an automated capability of testing for, detecting, and reporting errors that exceed a threshold consistent with the operational mode requirements. The effectiveness of integrity countermeasures must be established with the same rigor as the other security-relevant properties such as secrecy.

Cryptography is often utilized as a basis to provide data integrity assurance. Mechanisms, such as Manipulation Detection Codes (MDC)-, may be used. The adequacy of the encryption or MDC algorithm, the correctness of the protocol logic, and the adequacy of implementation must be established in MSM countermeasures design.

3. Label Integrity [I 4.1.1.3.1]

- Statement from DoD 5200.28-STD

Sensitivity labels shall accurately represent sensitivity levels of the specific subjects or objects with which they are associated. When exported by the TCB, sensitivity labels shall accurately and unambiguously represent the internal labels and shall be associated with the information being exported.

- Interpretation

The phrase “exported by the TCB” is understood to include transmission of information from an object in one component to an object in another component. Information transferred between NTCB partitions is addressed in the System Integrity Section. The form of internal and external (exported) sensitivity labels may differ, but the meaning shall be the same. The NTCB shall, in addition, ensure that correct association of sensitivity labels with the information being transported across the network is preserved.

As mentioned in the Trusted Facility Manual Section, encryption transforms the representation of information so that it is unintelligible to unauthorized subjects. Reflecting this transformation, the sensitivity level of the ciphertext is generally lower than the cleartext. It follows that cleartext and ciphertext are contained in different objects, each possessing its own label. The label of the cleartext must be preserved and associated with the ciphertext so that it can be restored when the cleartext is subsequently obtained by decrypting the ciphertext. If the cleartext is associated with a single-level device, the label of that cleartext may be implicit. The label may also be implicit in the key.

When information is exported to an environment where it is subject to deliberate or accidental modification, the TCB shall support the means, such as cryptographic checksums, to assure the accuracy of the labels. When there is a mandatory integrity policy, the policy will define the meaning of integrity labels.

- Rationale

Encryption algorithms and their implementation are outside the scope of these interpretations. Such algorithms may be implemented in a separate device or may be incorporated in a subject of a larger component. Without prejudice, either implementation packaging is referred to as an encryption mechanism herein. If encryption methodologies are employed in this regard, they shall be approved by the National Security Agency (NSA). The encryption process is part of the Network Trusted Computer Base partition in the components in which it is implemented.

The encryption mechanism is not necessarily a multilevel device or multilevel subject, as these terms are used in these criteria. The process of encryption is multilevel by definition. The cleartext and ciphertext interfaces carry information of different sensitivity. An encryption mechanism does not process data in the sense of performing logical or arithmetic operations on that data with the intent of producing new data. The cleartext and ciphertext interfaces on the encryption mechanism must be separately identified as being single-level or multilevel. If the interface is single-level, then the sensitivity of the data is established by a trusted individual and implicitly associated with the interface; the Exportation to Single-Level Devices criterion applies.

If the interface is multilevel, then the data must be labeled; the Exportation to Multilevel Devices criterion applies. The network architect is free to select an acceptable mechanism for associating a label with an object. With reference to encrypted objects, the following examples are possible:

1. Include a label field in the protocol definition of the object.
2. Implicitly associate the label with the object through the encryption key. That is, the encryption key uniquely identifies a sensitivity level. A single or private key must be protected at the level of the data that it encrypts.

4. Exportation of Labeled Information [4.1.1.3.2]

- Statement from DoD 5200.28-STD

The TCB shall designate each communication channel and I/O device as either single-level or multilevel. Any change in this designation shall be done manually and shall be auditable by the TCB. The TCB shall maintain and be able to audit any change in the sensitivity level or levels associated with a communications channel or I/O device.

- Interpretation

Each communication channel and network component shall be designated as either single-level or multilevel. Any change in this designation shall be done with the cognizance and approval of the administrator or security officer in charge of the affected components and the administrator or security officer in charge of the NTCB. This change shall be auditable by the network. The NTCB shall maintain and be able to audit any change in the device labels associated with a single-level communication channel or the range associated with a multilevel communication channel or component. The NTCB shall also be able to audit any change in the set of sensitivity levels associated with the information which can be transmitted over a multilevel communication channel or component.

- Rationale

Communication channels and components in a network are analogous to communication channels and I/O devices in stand-alone systems. They must be designated as either multilevel (i.e., able to distinguish and maintain separation among information of various sensitivity levels) or single-level. As in the TCSEC, single-level devices may only be attached to single-level channels.

The level or set of levels of information that can be sent to a component or over a communication channel shall only change with the knowledge and approval of the security officers (or system administrator, if there is no security officer) of the network, and of the affected components. This requirement ensures that no significant security-relevant changes are made without the approval of all affected parties.

5. Exportation to Multilevel Devices [4.1.1.3.2.1]

- Statement from DoD 5200.28-STD

When the TCB exports an object to a multilevel I/O device, the sensitivity label associated with that object shall also be exported and shall reside on the same physical medium as the exported information and shall be in the same form (i.e., machine-readable or human-readable form). When the TCB exports or imports an object over a multilevel communications channel, the protocol used on that channel shall provide for the unambiguous pairing between the sensitivity labels and the associated information that is sent or received.

- Interpretation

The components, including hosts, of a network shall be interconnected over “multilevel communication channels,” multiple single-level communication channels, or both, whenever the information is to be protected at more than a single sensitivity level. The protocol for associating the sensitivity label and the exported information shall provide the only information needed to correctly associate a sensitivity level with the exported information transferred over the multilevel channel between the NTCB partitions in individual components. This protocol definition must specify the representation and semantics of the sensitivity labels (i.e., the machine-readable label must uniquely represent the sensitivity level).

The “unambiguous” association of the sensitivity level with the communicated information shall meet the same level of accuracy as that required for any other label within the NTCB, as specified in the criterion for Label Integrity. This may be provided by protected and highly reliable direct physical layer connections, or by traditional cryptographic link protection in which any errors during transmission can be readily detected, or by use of a separate channel. The range of information imported or exported must be constrained by the associated device labels.

- Rationale

This protocol must specify the representation and semantics of the sensitivity labels. See the Mandatory

Access Control Policies section in Appendix B. The multilevel device interface to (untrusted) subjects may be implemented either by the interface of the reference monitor, per se, or by a multilevel subject (e.g., a “trusted subject” as defined in the Bell-LaPadula Model) that provides the labels based on the internal labels of the NTCB partition.

The current state of the art limits the support for mandatory policy that is practical for secure networks. Reference monitor support to ensure the control over all the operations of each subject in the network must be completely provided within the single NTCB partition on which that subject interfaces to the NTCB. This means that the entire portion of the “secure state” represented in the formal security policy model that may be changed by transitions invoked by this subject must be contained in the same component.

The secure state of an NTCB partition may be affected by events external to the component in which the NTCB partition resides (e.g., arrival of a message). The effect occurs asynchronously after being initiated by an event in another component or partition. For example, indeterminate delays may occur between the initiation of a message in one component, the arrival of the message in the NTCB partition in another component, and the corresponding change to the secure state of the second component. Since each component is executing concurrently, to do otherwise would require some sort of network-wide control to synchronize state transitions, such as a global network-wide clock for all processors; in general, such designs are not practical and probably not even desirable. Therefore, the interaction between NTCB partitions is restricted to just communications between pairs (at least logically) of devices-multilevel devices if the device(s) can send/receive data of more than a single level. For broadcast channels the pairs are the sender and intended receiver(s). However, if the broadcast channel carries multiple levels of information, additional mechanism (e.g., cryptochecksum maintained by the TCB) may be required to enforce separation and proper delivery.

A common representation for sensitivity labels is needed in the protocol used on that channel and understood by both the sender and receiver when two multilevel devices (in this case, in two different components) are interconnected. Each distinct sensitivity level of the overall network policy must be represented uniquely in these labels.

Within a monolithic TCB, the accuracy of the sensitivity labels is generally assured by simple techniques, e.g., very reliable connections over very short physical connections, such as on a single printed circuit board or over an internal bus. In many network environments there is a much higher probability of accidentally or maliciously introduced errors, and these must be protected against.

6. Exportation to Single-Level Devices [4.1.1.3.2.2]

- Statement from DoD 5200.28-STD

Single-level I/O devices and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the TCB shall include a mechanism by which the TCB and an authorized user reliably communicate to designate the single sensitivity level of information imported or exported via single-level communication channels or I/O devices.

- Interpretation

Whenever one or both of two directly connected components is not trusted to maintain the separation of information of different sensitivity levels, or whenever the two directly connected components have only a single sensitivity level in common, the two components of the network shall communicate over a single-level channel. Single-level components and single-level communication channels are not required to maintain the sensitivity labels of the information they process. However, the NTCB shall include a reliable communication mechanism by which the NTCB and an authorized user (via a trusted path) or a subject within an NTCB partition can designate the single sensitivity level of information imported or exported via single-level communication channels or network components. The level of information communicated must equal the device level.

- Rationale

Single-level communications channels and single-level components in networks are analogous to single level channels and I/O devices in stand-alone systems in that they are not trusted to maintain the separation of information of different sensitivity levels. The labels associated with data transmitted over those channels and by those components are therefore implicit; the NTCB associates labels with the data because of the channel or component, not because of an explicit part of the bit stream. Note that the sensitivity level of encrypted information is the level of the ciphertext rather than the original level(s) of the plaintext.

7. Labeling Human-Readable Output [4.1.1.3.2.3]

- Statement from DoD 5200.28-STD

The ADP system administrator shall be able to specify the printable label names associated with exported sensitivity labels. The TCB shall mark the beginning and end of all human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly[1] represent the sensitivity of the output. The TCB shall, by default, mark the top and bottom of each page of human-readable, paged, hardcopy output (e.g., line printer output) with human-readable sensitivity labels that properly1 represent the sensitivity of the page. The TCB shall, by default and in an appropriate manner, mark other forms of human readable output (e.g., maps, graphics) with human-readable sensitivity labels that properly1 represent the sensitivity of the output. Any override of these markings defaults shall be auditable by the TCB.

- Interpretation

[1] The hierarchical classification component in human-readable sensitivity labels shall be equal to the greatest hierarchical classification of any of the information in the output that the labels refer to; the non-hierarchical category component shall include all of the non-hierarchical categories of the information in the output the labels refer to, but no other nonhierarchical categories.

This criterion imposes no requirement to a component that produces no human-readable output. For those that do produce human-readable output, each sensitivity level that is defined to the network shall have a uniform meaning across all components. The network administrator, in conjunction with any affected component administrator, shall be able to specify the human-readable label that is associated with each defined sensitivity level.

- Rationale

The interpretation is a straightforward extension of the requirement into the context of a network system and partitioned NTCB as defined for these network interpretations.

8. Subject Sensitivity Labels [4.1.1.3.3]

- Statement from DoD 5200.28-STD

The TCB shall immediately notify a terminal user of each change in the sensitivity level associated with that user during an interactive session. A terminal user shall be able to query the TCB as desired for a display of the subject's complete sensitivity label.

- Interpretation

An NTCB partition shall immediately notify a terminal user attached to its component of each change in the sensitivity level associated with that user.

- Additional Network Component Interpretation

An M-Component need not support direct terminal input in which case this requirement is not applicable. Any MComponent which does support direct terminal input must meet the requirement as stated.

- Rationale

The local NTCB partition must ensure that the user understands the sensitivity level of information sent to and from a terminal. When a user has a surrogate process in another component, adjustments to its level may occur to maintain communication with the user. These changes may occur asynchronously. Such adjustments are necessitated by mandatory access control as applied to the objects involved in the communication path.

- Additional Network Component Rationale

The only way that a user can change the current level of the session is to be directly connected to a component that supports the MAC Policy. If the user is directly connected to a component that does not support the MAC Policy then the user will always operate at the level of the component to which he is directly attached. If the user is directly connected to a M-Component then this M-Component must meet the requirements as stated. M-Components which may be part of the network which do not directly communicate with users need not support this requirement since the requirement will be met by the M-Component with which the user is directly communicating.

9. Device Labels [4.1.1.3.4]

- Statement from DoD 5200.28-STD

The TCB shall support the assignment of minimum and maximum sensitivity levels to all attached physical devices. These sensitivity levels shall be used by the TCB to enforce constraints imposed by the physical environments in which the devices are located.

- Interpretation

This requirement applies as written to each NTCB partition that is trusted to separate information based on sensitivity level. Each I/O device in a component, used for communication with other network components, is assigned a device range, consisting of a set of labels with a maximum and minimum. (A device range usually contains, but does not necessarily contain, all possible labels “between” the maximum and minimum, in the sense of dominating the minimum and being dominated by the maximum.)

The NTCB always provides an accurate label for information exported through devices. Information exported or imported using a single-level device is labelled implicitly by the sensitivity level of the device. Information exported from one multilevel device and imported at another must be labeled through an agreed-upon protocol, unless it is libeled implicitly by using a communication link that always carries a single level.

Information exported at a given sensitivity level can be sent only to an importing device whose device range contains that level or a higher level. If the importing device range does not contain the given level, the information is relabelled upon reception at a higher level within the importing device range. Relabelling should not occur otherwise.

- Rationale

The purpose of device labels is to reflect and constrain the sensitivity levels of information authorized for the physical environment in which the devices are located.

The information transfer restrictions permit one-way communication (i.e., no acknowledgements) from one device to another whose ranges have no level in common, as long as each level in the sending device range is dominated by some level in the receiving device range. It is never permitted to send information at a given level to a device whose range does not contain a dominating level. (See Appendix C for similar interconnection rules for the interconnected AIS view.)

10. Mandatory Access Control [4.1.1.4]

- Statement from DoD 5200.28-STD

The TCB shall enforce a mandatory access control policy over all resources (i.e., subjects, storage objects, and I/O devices) that are directly or indirectly accessible by subjects external to the TCB. These subjects and objects shall be assigned sensitivity labels that are a combination of hierarchical classification levels and non-hierarchical categories, and the labels shall be used as the basis for mandatory access control decisions. The TCB shall be able to support two or more such sensitivity levels. (See the Mandatory Access Control interpretations.) The following requirements shall hold for all accesses between all subjects external to the TCB and all objects directly or indirectly accessible by these subjects. A subject can read an object only if the hierarchical classification in the subject’s sensitivity level is greater than or equal to the hierarchical classification of the object’s sensitivity level and the non-hierarchical categories in the subject’s sensitivity level include all the non-hierarchical categories in the object’s sensitivity level. A subject can write an object only if the hierarchical classification in the subject’s sensitivity level is less than or equal to the hierarchical classification of the object’s sensitivity level and the non-hierarchical categories in the subject’s sensitivity level are included in the non-hierarchical categories in the object’s sensitivity level. Identification and authentication data shall be used by the TCB to authenticate the user’s identity and to ensure that the sensitivity level and authorization of subjects external to the TCB that may be created to act on behalf of the individual user are dominated by the clearance and authorization of that user.

- Interpretation

Each partition of the NTCB exercises mandatory access control policy over all subjects and objects in its component. In a network, the responsibility of an NTCB partition encompasses all mandatory access control functions in its component that would be required of a TCB in a standalone system. In particular, subjects and objects used for communication with other components are under the control of the NTCB partition. Mandatory access control includes secrecy and integrity control to the extent that the network sponsor has described in the overall network security policy.

Conceptual entities associated with communication between two components, such as sessions, connections and virtual circuits, may be thought of as having two ends, one in each component, where each end is represented by a local object. Communication is viewed as an operation that copies information from an object at one end of a communication path to an object at the other end. Transient data-carrying entities, such as datagrams and packets, exist either as information within other objects, or as a pair of objects, one at each end of the communication path.

The requirement for "two or more" sensitivity levels can be met by either secrecy or integrity levels. When there is a mandatory integrity policy, the stated requirements for reading and writing are generalized to: A subject can read an object only if the subject's sensitivity level dominates the object's sensitivity level, and a subject can write an object only if the object's sensitivity level dominates the subject's sensitivity level. Based on the integrity policy, the network sponsor shall define the dominance relation for the total label, for example, by combining secrecy and integrity lattices.

- Rationale

An NTCB partition can maintain access control only over subjects and objects in its component. At levels B2 and above, the NTCB partition must maintain access control over all subjects and objects in its component. Access by a subject in one component to information contained in an object in another component requires the creation of a subject in the remote component which acts as a surrogate for the first subject.

The mandatory access controls must be enforced at the interface of the reference monitor (viz. the mechanism that controls physical processing resources) for each NTCB partition. This mechanism creates the abstraction of subjects and objects which it controls. Some of these subjects outside the reference monitor, per se, may be designated to implement part of an NTCB partition's mandatory policy, e.g., by using the "trusted subjects" defined in the Bell-LaPadula model.

The prior requirements on exportation of labeled information to and from I/O devices ensure the consistency between the sensitivity labels of objects connected by a communication path. As noted in the introduction, the network architecture must recognize the linkage between the overall mandatory network security policy and the connection oriented abstraction. For example, individual data-carrying entities such as datagrams can have individual sensitivity labels that subject them to mandatory access control in each component. The abstraction of a single-level connection is realized and enforced implicitly by an architecture while a connection is realized by single-level subjects that necessarily employ only datagrams of the same level.

The fundamental trusted systems technology permits the DAC mechanism to be distributed, in contrast to the requirements for mandatory access control. For networks this separation of MAC and DAC mechanisms is the rule rather than the exception.

The set of total sensitivity labels used to represent all the sensitivity levels for the mandatory access control (combined data secrecy and data integrity) policy always forms a partially ordered set. Without loss of generality, this set of labels can always be extended to form a lattice, by including all the combinations of non-hierarchical categories. As for any lattice, a dominance relation is always defined for the total sensitivity labels. For administrative reasons it may be helpful to have a maximum level which dominates all others.

11. Trusted Path [4.1.2.1.1]

- Statement from DoD 5200.28-STD

The TCB shall support a trusted communication path between itself and users for use when a positive TCB-to-user connection is required (e.g., login, change subject sensitivity level). Communications via this trusted path shall be activated exclusively by a user or the TCB and shall be logically and unmistakably distinguishable from other paths.

- Interpretation

A trusted path is supported between a user (i.e., human) and the NTCB partition in the component to which the user is directly connected.

- Additional Network Component Interpretation

An M-Component need not support direct user input (e.g., the M-Component may not be attached to any user I/O devices such as terminals) in which case this requirement is not applicable. Any M-Component which does support direct communication with users must meet the requirement as stated. In addition, an M-Component with directly connected users must provide mechanisms which establish the clearance of users and associate that clearance with the users current session.

- Rationale

When a user logs into a remote component, the user id is transmitted securely between the local and remote NTCB partitions in accordance with the requirements in Identification and Authentication.

Trusted Path is necessary in order to assure that the user is communicating with the NTCB and only the NTCB when security relevant activities are taking place (e.g., authenticate user, set current session sensitivity level). However, Trusted Path does not address communications within the NTCB, only communications between the user and the NTCB. If, therefore, a component does not support any direct user communication then the component need not contain mechanisms for assuring direct NTCB to user communications.

The requirement for trusted communication between one NTCB partition and another NCTB partition is addressed in the System Architecture section. These requirements are separate and distinct from the user to NTCB communication requirement of a trusted path. However, it is expected that this trusted communication between one NTCB partition and another NTCB partition will be used in conjunction with the trusted path to implement trusted communication between the user and the remote NTCB partition.

- Additional Network Component Rationale

Trusted Path is necessary in order to assure that the user is communicating with the TCB and only the TCB when security relevant activities are taking place (e.g., authenticate user, set current session security level). However, Trusted Path does not address communications within the TCB, only communications between the user and the TCB. If, therefore, an M-Component does not support any direct user communication then the M-Component need not contain mechanisms for assuring direct TCB to user communications.

In the case where an M-Component does support direct user communication the Clearance of the user must be established by the M-Component. There are three possible means of providing this support: a) all direct user connections are via single-level channels, where the maximum level of the channel equals the minimum level of the channel, and physical access to the channel implies clearance to the level of the channel; in this case there may exist no security relevant activities so that the applicable trusted path requirements may be met by reason of the device labels alone, b) some direct user connections are via single-level channels, where the maximum level of the channel does not equal the minimum level of the channel, and physical access to the channel implies clearance to the maximum level of the channel, c) some direct user connections are via singlelevel channels, where the maximum level of the channel does not equal the minimum level of the channel, and the MComponent contains some internal mechanism for mapping the user clearance to the range on the channel. The first two options map the user clearance to the activities of the user through external means. The third option requires some internal mechanism. Such a mechanism might be a user id/password/clearance database maintained by the MComponent. Another acceptable mechanism might be a protocol and interface definition within the M-Component for obtaining such information (via a multilevel channel - the channel is multilevel because it is passing labels, i.e., the user clearance) from some other M-Component.

12. System Architecture [4.1.3.1.1]

- Statement from DoD 5200.28-STD

The TCB shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). The TCB shall maintain process isolation through the provision of distinct address spaces under its control. The TCB shall be internally structured into well-defined largely independent modules. It shall make effective use of available hardware to separate those elements that are protection-critical from those that are not. The TCB modules shall be designed such that the principle of least privilege is enforced. Features in hardware, such as segmentation, shall be used to support logically distinct storage objects with separate attributes (namely: readable, writable). The user interface to the TCB shall be completely defined and all elements of the TCB identified. The TCB shall be designed and structured to use a complete, conceptually simple protection mechanism with precisely defined semantics. This mechanism shall play a central role in enforcing the internal structuring of the TCB and the system. The TCB shall incorporate significant use of layering, abstraction and data hiding. Significant system engineering shall be directed toward minimizing the complexity of the TCB and excluding from the TCB modules that are not protection-critical.

- Interpretation

The system architecture criterion must be met individually by all NTCB partitions. Implementation of the requirement that the NTCB maintain a domain for its own execution is achieved by having each NTCB partition maintain a domain for its own execution. Since each component is itself a distinct domain in the overall network system, this also satisfies the requirement for process isolation through distinct address spaces in the special case where a component has only a single subject.

The NTCB must be internally structured into well-defined largely independent modules and meet the hardware requirements. This is satisfied by having each NTCB partition so structured. The NTCB controls all network resources. These resources are the union of the sets of resources over which the NTCB partitions have control. Code and data structures belonging to the NTCB, transferred among NTCB subjects (i.e., subjects outside the reference monitor but inside the NTCB) belonging to different NTCB partitions, must be protected against external interference or tampering. For example, a cryptographic checksum or physical means may be employed to protect user authentication data exchanged between NTCB partitions.

Each NTCB partition must enforce the principle of least privilege within its component. Additionally, the NTCB must be structured so that the principle of least privilege is enforced in the system as a whole.

The NTCB must be designed and structured according to the network security architecture to use a complete, conceptually simple protection mechanism. Furthermore, each NTCB partition must also be so designed and structured.

Significant system engineering should be directed toward minimizing the complexity of each NTCB partition, and of the NTCB. Care shall be taken to exclude modules (and components) that are not protection-critical from the NTCB.

It is recognized that some modules and/or components may need to be included in the NTCB and must meet the NTCB requirements even though they may not appear to be directly protection-critical. The correct operation of these modules/components is necessary for the correct operation of the protection-critical modules and components. However, the number and size of these modules/components should be kept to a minimum.

Each NTCB partition provides isolation of resources (within its component) in accord with the network system architecture and security policy so that “supporting elements” (e.g., DAC and user identification) for the security mechanisms of the network system are strengthened compared to C2, from an assurance point of view, through the provision of distinct address spaces under control of the NTCB.

As discussed in the Discretionary Access Control section, the DAC mechanism of a NTCB partition may be implemented at the interface of the reference monitor or may be distributed in subjects that are part of the NTCB in the same or different component. When distributed in NTCB subjects (i.e., when outside the reference monitor), the assurance requirements for the design and implementation of the DAC shall be those of class C2 for all networks of class C2 or above.

- Additional Network Component Interpretation

An M-Component must meet the requirement as stated. In this interpretation the words “The user interface to the TCB shall be completely defined...” shall be interpreted to mean the interface between the reference monitor of the MComponent and the subjects external to the reference monitor shall be completely defined.

- Rationale

The requirement that the NTCB be structured into modules and meet the hardware requirements applies within the NTCB partitions in the various components.

The principle of least privilege requires that each user or other individual with access to the system be given only those resources and authorizations required for the performance of this job. In order to enforce this principle in the system it must be enforced in every NTCB partition that supports users or other individuals. For example, prohibiting access by administrators to objects outside the NTCB partition (e.g., games) lessens the opportunity of damage by a Trojan Horse.

The requirement for the protection of communications between NTCB partitions is specifically directed to subjects that are part of the NTCB partitions. Any requirements for such protection for the subjects that are outside the NTCB partitions are addressed in response to the integrity requirements of the security policy.

There are certain parts of a network (modules and/or components) that may not appear to be directly protection-critical in that they are not involved in access control decisions, do not directly audit, and are not involved in the identification/authentication process. However, the security of the network must depend on the correct operation of these modules and/or components. An example of this is a single level packet switch. Although it may not normally be involved directly in enforcing the discretionary security policy, this switch may be trusted not to mix data from different message streams. If the switch does not operate correctly, data could get mixed, and unauthorized access could result. Therefore, these modules/components must be included in the NTCB and must meet the NTCB requirements applicable to the policy element(s) for which they are responsible.

- Additional Network Component Rationale

The M-Component may not have a direct user interface but is expected to support subjects which are not part of the TCB. It is important that the interface between the TCB and subjects external to the TCB be completely defined. (Note that in such a case the subjects are always internal to the component, viz., are “internal subjects”).

13. System Integrity [4.1.3.1.2]

- Statement from DoD 5200.28-STD

Hardware and/or software features shall be provided that can be used to periodically validate the correct operation of the on-site hardware and firmware elements of the TCB.

- Interpretation

Implementation of the requirement is partly achieved by having hardware and/or software features that can be used to periodically validate the correct operation of the hardware and firmware elements of each component’s NTCB partition. Features shall also be provided to validate the identity and correct operation of a component prior to its incorporation in the network system and throughout system operation. For example, a protocol could be designed that enables the components of the partitioned NTCB to exchange messages periodically and validate each other’s correct response. The protocol shall be able to determine the remote entity’s ability to respond. NTCB partitions shall provide the capability to report to network administrative personnel the failures detected in other NTCB partitions.

Intercomponent protocols implemented within a NTCB shall be designed in such a way as to provide correct operation in the case of failures of network communications or individual components. The allocation of mandatory and discretionary access control policy in a network may require communication between trusted subjects that are part of the NTCB partitions in different components. This communication is normally implemented with a protocol between the subjects as peer entities. Incorrect access within a component shall not result from failure of an NTCB partition to communicate with other components.

- Rationale

The first paragraph of the interpretation is a straightforward extension of the requirement into the context of a network system and partitioned NTCB as defined for these network criteria.

NTCB protocols should be robust enough so that they permit the system to operate correctly in the case of localized failure. The purpose of this protection is to preserve the integrity of the NTCB itself. It is not unusual for one or more components in a network to be inoperative at any time, so it is important to minimize the effects of such failures on the rest of the network. Additional integrity and denial of service issues are addressed in Part II.

It should be clear that some integrity and denial of service features can reside outside the NTCB. Otherwise all software in a network would be in the NTCB. Every piece of software that has an opportunity to write to some data or protocol field is "trusted" to preserve integrity or not cause denial of service to some extent. For example, it is necessary to "trust" TELNET to correctly translate user data, and to eventually transmit packets. FTP also has to be "trusted" to not inappropriately modify files, and to attempt to complete the file transfer. These protocols can be designed, however to exist outside the NTCB (from a protection perspective). It is beneficial to do this type of security engineering so that the amount of code that must be trusted to not disclose data is minimized. Putting everything inside the NTCB contradicts the requirement to perform "significant system engineering ... directed toward ... excluding from the TCB modules that are not protection critical," which removes the primary difference between B2 and B3. If everything has to be in the TCB to ensure data integrity and protection against denial of service, there will be considerably less assurance that disclosure protection is maximized.

14. Covert Channel Analysis [4.1.3.1.3]

- Statement from DoD 5200.28-STD

The system developer shall conduct a thorough search for covert channels and make a determination (either by actual measurement or by engineering estimation) of the maximum bandwidth of each identified channel. (See the Covert Channels Guideline section.) FORMAL METHODS SHALL BE USED IN THE ANALYSIS.

- Interpretation

The requirement, including the TCSEC Covert Channel Guideline, applies as written. In a network, there are additional instances of covert channels associated with communication between components. THE FORMAL METHODS SHALL BE USED IN THE ANALYSIS OF EACH INDIVIDUAL COMPONENT DESIGN AND IMPLEMENTATION.

- Additional Network Component Interpretation

An M-Component must meet the requirement as stated. In addition, if the analysis indicates that channels exist that need to be audited (according to the Covert Channel Analysis Guideline), the M-Component shall contain a mechanism for making audit data (related to possible use of covert channels) available outside of the M-Component (e.g., by passing the data to an audit collection component).

- Rationale

The exploitation of network protocol information (e.g., headers) can result in covert storage channels. Exploitation of frequency of transmission can result in covert timing channels. The topic has been addressed in the literature.

- Additional Network Component Rationale

If an M-Component contains covert channels that need to be audited the M-Component must produce the audit data such that auditing can be performed. Since all covert channels in the network occur in an M-Component, the M-Component must be the source of the audit record which records the possible use of the covert channel.

15. Trusted Facility Management [4.1.3.1.4]

- Statement from DoD 5200.28-STD

The TCB shall support separate operator and administrator functions. The functions performed in the role of a security administrator shall be identified. The ADP system administrative personnel shall only be able to perform security administrator functions after taking a distinct auditable action to assume the security administrator role on the ADP system. Non-security functions that can be performed in the security administration role shall be limited strictly to those essential to performing the security role effectively.

- Interpretation

This requirement applies as written to both the network as a whole and to individual components which support such personnel.

- Additional Network Component Interpretation

An M-Component must meet the requirement as stated except for the words "The procedures for examining and maintaining the audit files as well as...". These words are interpreted to mean "the mechanisms and protocols associated with exporting of audit data must be defined." Also, the words "...to include changing the security characteristics of a user", shall not be applicable to an M-Component.

- Rationale

It is recognized that based on the allocated policy elements some components may operate with no human interface.

- Additional Network Component Rationale

An M-Component does not maintain the audit files nor does it provide mechanisms for examining them. It must, however provide mechanisms for exporting the audit files and these mechanisms need to be defined in the Trusted Facility Manual. The M-Component also does not maintain user information.

16. Trusted Recovery [4.1.3.1.5]

- Statement from DoD 5200.28-STD

Procedures and/or mechanisms shall be provided to assure that, after an ADP system failure or other discontinuity, recovery without a protection compromise is obtained.

- Interpretation

The recovery process must be accomplished without a protection compromise after the failure or other discontinuity of any NTCB partition. It must also be accomplished after a failure of the entire NTCB.

- Rationale

This is a straightforward extension of the requirement into the network context, and takes into account that it is possible for parts of the system to fail while other parts continue to operate normally. This may be a security-relevant event; if so it must be audited.

17. Security Testing [4.1.3.2.1]

- Statement from DoD 5200.28-STD

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. A team of individuals who thoroughly understand the specific implementation of the TCB shall subject its design documentation, source code, and object code to through analysis and testing. Their objectives shall be: to uncover all design and implementation flaws that would permit a subject external to the TCB to read, change, or delete data normally denied under the mandatory or discretionary security policy enforced by the TCB; as well as to assure that no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users. The TCB shall be found resistant to penetration. All discovered flaws shall be removed or neutralized and the TCB retested to demonstrate that they have been eliminated and that new flaws have not been introduced. Testing shall demonstrate that the TCB implementation is consistent with the descriptive top-level specification. No design flaws and no more than a few correctable implementation flaws may be found during testing and there shall be reasonable confidence that few remain. MANUAL OR OTHER MAPPING OF THE FTLS TO THE SOURCE CODE MAY FORM A BASIS FOR PENETRATION TESTING. (See the security testing guidelines.)

- Interpretation

Testing of a component will require a testbed that exercises the interfaces and protocols of the component including tests under exceptional conditions. The testing of a security mechanism of the network system for meeting this criterion shall be an integrated testing procedure involving all components containing an NTCB partition that implement the given mechanism. This integrated testing is additional to any individual component tests involved in the evaluation of the network system. The sponsor should identify the allowable set of configurations including the sizes of the networks. Analysis or testing procedures and tools shall be available to test the limits of these configurations.

A change in configuration within the allowable set of configurations does not require retesting. The testing of each component will include the introduction of subjects external to the NTCB partition for the component that will attempt to read, change, or delete data normally denied. If the normal interface to the component does not provide a means to create the subjects needed to conduct such a test, then this portion of the testing shall use a special version of the untrusted software for the component that results in subjects that make such attempts. The results shall be saved for test analysis. Such special versions shall have an NTCB partition that is identical to that for the normal configuration of the component under evaluation.

The testing of the mandatory controls shall include tests to demonstrate that the labels for information imported and/or exported to/from the component accurately represent the labels maintained by the NTCB partition for the component for use as the basis for its mandatory access control decisions. The tests shall include each type of device, whether single-level or multilevel, supported by the component.

The NTCB must be found resistant to penetration. This applies to the NTCB as a whole, and to each NTCB partition in a component of this class.

- Additional Network Component Interpretation

An M-Component must meet the requirement as stated except for the words “normally denied under the ... discretionary security policy,” which are not applicable to an M-Component.

- Rationale

The phrase “no subject (without authorization to do so) is able to cause the TCB to enter a state such that it is unable to respond to communications initiated by other users” relates to the security services (Part II of this TNI) for the Denial of Service problem, and to correctness of the protocol implementations.

Testing is an important method available in this evaluation division to gain any assurance that the security mechanisms perform their intended function. A major purpose of testing is to demonstrate the system’s response to inputs to the NTCB partition from untrusted (and possibly malicious) subjects.

In contrast to general purpose systems that allow for the dynamic creation of new programs and the introductions of new processes (and hence new subjects) with user specified security properities, many network components have no method for introducing new programs and/or processes during their normal operation. Therefore, the programs necessary for the testing must be introduced as special versions of the software rather than as the result of normal inputs by the test team. However, it must be insured that the NTCB partition used for such tests is identical to the one under evaluation.

Sensitivity labels serve a critical role in maintaining the security of the mandatory access controls in the network. Especially important to network security is the role of the labels for information communicated between components - explicit labels for multilevel devices and implicit labels for single-level devices. Therefore the testing for correct labels is highlighted.

The requirement for testing to demonstrate consistency between the NTCB implementation and the FTLS is a straightforward extension of the TCSEC requirement into the context of a network system.

- Additional Network Component Rationale

An M-Component does not support a discretionary security policy, and therefore testing for violations of such a policy is of no value.

18. Design Specification and Verification [4.1.3.2.2]

- Statement from DoD 5200.28-STD

A formal model of the security policy supported by the TCB shall be maintained over the life cycle of the ADP system that is proven and demonstrated to be consistent with its axioms. A descriptive top-level specification (DTLS) of the TCB shall be maintained that completely and accurately describes the TCB in terms of exceptions, error messages, and effects. A FORMAL TOP-LEVEL SPECIFICATION (FTLS) OF THE TCB SHALL BE MAINTAINED THAT ACCURATELY DESCRIBES THE TCB IN TERMS OF EXCEPTIONS, ERROR MESSAGES, AND EFFECTS. THE DTLS AND FTLS SHALL INCLUDE THOSE COMPONENTS OF THE TCB THAT ARE IMPLEMENTED AS HARDWARE AND/OR FIRMWARE IF THEIR PROPERTIES ARE VISIBLE AT THE TCB INTERFACE. THE FTLS SHALL BE SHOWN to be an accurate description of the TCB interface. A convincing argument shall be given that the DTLS is consistent with the model AND A COMBINATION OF FORMAL AND INFORMAL TECHNIQUES SHALL BE USED TO SHOW THAT THE FTLS IS CONSISTENT WITH THE MODEL. THIS VERIFICATION EVIDENCE SHALL BE CONSISTENT WITH THAT PROVIDED WITHIN THE STATE-OF-THE-ART OF THE PARTICULAR NATIONAL COMPUTER SECURITY CENTER-ENDORSED FORMAL SPECIFICATION AND VERIFICATION SYSTEM USED. MANUAL OR OTHER MAPPING OF THE FTLS TO THE TCB SOURCE CODE SHALL BE PERFORMED TO PROVIDE EVIDENCE OF CORRECT IMPLEMENTATION.

- Interpretation

The overall network security policy expressed in this model will provide the basis for the mandatory access control policy exercised by the NTCB over subjects and storage objects in the entire network. The policy will also be the basis for the discretionary access control policy exercised by the NTCB to control access of named users to named objects. Data integrity requirements addressing the effects of unauthorized MSM need not be included in this model. The overall network policy must be decomposed into policy elements that are allocated to appropriate components and used as the basis for the security policy model for those components.

The level of abstraction of the model, and the set of subjects and objects that are explicitly represented in the model, will be affected by the NTCB partitioning. Subjects and objects must be represented explicitly in the model for the partition if there is some network component whose NTCB partition exercises access control over them. The model shall be structured so that the axioms and entities applicable to individual network components are manifest. Global network policy elements that are allocated to components shall be represented by the model for that component.

AN FTLS FOR A NETWORK CONSISTS OF A COMPONENT FTLS FOR EACH UNIQUE TRUSTED NETWORK COMPONENT, PLUS ANY GLOBAL DECLARATIONS AND ASSERTIONS THAT APPLY TO MORE THAN ONE COMPONENT. IF THE MODEL FOR EACH COMPONENT REPRESENTS ALL THE GLOBAL MANDATORY POLICY ELEMENTS ALLOCATED TO THAT COMPONENT, THERE MAY NOT BE ANY GLOBAL ASSERTIONS NEEDED, AND IN THIS CASE THE COLLECTION OF COMPONENT FTLS, WITH ANY SHARED DECLARATIONS, IS THE NETWORK FTLS. EACH COMPONENT FTLS SHALL DESCRIBE THE INTERFACE TO THE NTCB PARTITION OF ITS COMPONENTS. The requirements for a network DTLS are given in the Design Documentation section.

- Additional Network Component Interpretation

An M-Component must meet the requirement as stated.

Security Policy is interpreted to mean the MAC Policy supported by the component. Model is interpreted to be those portions of a reference monitor model that are relevant to the MAC Policy supported by the Component (e.g., the representation of the current access set and the sensitivity labels of subjects and objects, and the Simple Security and Confinement Properties of the Bell and LaPadula Model).

- Rationale

The treatment of the model depends to a great extent on the degree of integration of the communications service into a distributed system. In a closely coupled distributed system, one might use a model that closely resembles one appropriate for a stand-alone computer system.

In all cases, the model of each partition will be expected to show the role of the NTCB partition in each kind of component. It will most likely clarify the model, although not part of the model, to show access restrictions implied by the system design; for example, subjects representing protocol entities might have access only to objects containing data units at the same layer of protocol. The allocation of subjects and objects to different protocol layers is a protocol design choice which need not be reflected in the security policy model.

THE FTLS MUST REPRESENT THE UNDERLYING REFERENCE MONITOR AND ANY SUBJECTS IMPLEMENTING THE MANDATORY POLICY. OTHER POLICY ELEMENTS DISTRIBUTED IN NTCB SUBJECTS (SEE THE INTERPRETATION OF SYSTEM ARCHITECTURE) NEED NOT BE REPRESENTED BY THE FTLS.

19. Configuration Management [4.1.3.2.3]

- Statement from DoD 5200.28-STD

During THE ENTIRE LIFE-CYCLE, I.E. DURING THE DESIGN, DEVELOPMENT, and maintenance of the TCB, a configuration management system shall be in place FOR ALL SECURITYRELEVANT HARDWARE, FIRMWARE, AND SOFTWARE that maintains control of changes to THE FORMAL MODEL, the descriptive AND FORMAL top-level SPECIFICATIONS, other design data, implementation documentation, source code, the running version of the object code, and test fixtures and documentation. The configuration management system shall assure a consistent mapping among all documentation and code associated with the current version of the TCB. Tools shall be provided for generation of a new version of the TCB from source code. Also available shall be tools, MAINTAINED UNDER STRICT CONFIGURATION CONTROL, for comparing a newly generated version with the previous TCB version in order to ascertain that only the intended changes have been made in the code that will actually be used as the new version of the TCB. A COMBINATION OF TECHNICAL, PHYSICAL, AND PROCEDURAL SAFEGUARDS SHALL BE USED TO PROTECT FROM UNAUTHORIZED MODIFICATION OR DESTRUCTION THE MASTER COPY OR COPIES OF ALL MATERIAL USED TO GENERATE THE TCB.

- Interpretation

The requirement applies as written, with the following extensions:

1. A configuration management system must be in place for each NTCB partition.
2. A configuration management plan must exist for the entire system. If the configuration management sys-tem is made up of the conglomeration of the confi-guration management systems of the various NTCB par-titions, then the configuration management plan must address the issue of how configuration control is applied to the system as a whole.

ALL MATERIAL USED IN GENERATING A NEW VERSION OF THE NTCB AND EACH NTCB PARTITION MUST BE PROTECTED, REGARDLESS OF WHERE IT PHYSICALLY RESIDES.

- Rationale

Each NTCB partition must have a configuration management system in place, or else there will be no way for the NTCB as a whole to have an effective configuration management system. The other extensions are merely reflections of the way that networks operate in practice.

THIS NEW REQUIREMENT EXPLICITLY MANDATES THE PROTECTION OF MATERIAL USED TO GENERATE AN NTCB PARTITION, EVEN WHEN THE GENERATION OCCURS BY DOWN-LINE LOADING OF A REMOTE COMPONENT.

20. Trusted Distribution [4.1.3.2.4]

- Statement from DoD 5200.28-STD

A TRUSTED ADP SYSTEM CONTROL AND DISTRIBUTION FACILITY SHALL BE PROVIDED FOR MAINTAINING THE INTEGRITY OF THE MAPPING BETWEEN THE MASTER DATA DESCRIBING THE CURRENT VERSION OF THE TCB AND THE ON-SITE MASTER COPY OF THE CODE FOR THE CURRENT VERSION. PROCEDURES (E.G., SITE SECURITY ACCEPTANCE TESTING) SHALL EXIST FOR ASSURING THAT THE TCB SOFTWARE, FIRMWARE, AND HARDWARE UPDATES DISTRIBUTED TO A CUSTOMER ARE EXACTLY AS SPECIFIED BY THE MASTER COPIES.

- Interpretation

THIS REQUIREMENT APPLIES AS STATED, WITH THE ADDITIONAL REQUIREMENT THAT, IF DOWN-LINE LOADING IS USED, THERE MUST BE A TRUSTED METHOD OF GENERATING, SENDING, AND LOADING ANY SOFTWARE INVOLVED.

- Rationale

THIS IS A STRAIGHTFORWARD EXTENSION OF THE REQUIREMENT INTO THE NETWORK CONTEXT.

21. Security Features User's Guide [4.1.4.1]

- Statement from DoD 5200.28-STD

A single summary, chapter, or manual in user documentation shall describe the protection mechanisms provided by the TCB, interpretations on their use, and how they interact with one another.

- Interpretation

This user documentation describes user visible protection mechanisms at the global (network system) level and at the user interface of each component, and the interaction among these.

- Rationale

The interpretation is an extension of the requirement into the context of a network system as defined for these network criteria. Documentation of protection mechanisms provided by individual components is required by the criteria for trusted computer systems that are applied as appropriate for the individual components.

22. Trusted Facility Manual [4.1.4.2]

- Statement from DoD 5200.28-STD

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given. The manual shall describe the operator and administrator functions related to security, to include changing the security characteristics of a user. It shall provide interpretations on the consistent and effective use of the protection features of the system, how they interact, how to securely generate a new TCB, and facility procedures, warnings, and privileges that need to be controlled in order to operate the facility in a secure manner. The TCB modules that contain the reference validation mechanism shall be identified. The procedures for secure generation of a new TCB from source after modification of any modules in the TCB shall be described. It shall include the procedures to ensure that the system is initially started in a secure manner. Procedures shall also be included to resume secure system operation after any lapse in system operation.

- Interpretation

This manual shall contain specifications and procedures to assist the system administrator(s) maintain cognizance of the network configuration. These specifications and procedures shall address the following:

1. The hardware configuration of the network itself;
2. The implications of attaching new components to the network;
3. The case where certain components may periodically leave the network (e.g., by crashing, or by being disconnected) and then rejoin;
4. Network configuration aspects that can impact the security of the network system; (For example, the manual should describe for the network system administrator the interconnections among components that are consistent with the overall network system architecture.)
5. Loading or modifying NTCB software or firmware (e.g., down-line loading).
6. Incremental updates; that is, it must explicitly indicate which components of the network may change without others also changing.

The physical and administrative environmental controls shall be specified. Any assumptions about security of a given network should be clearly stated (e.g., the fact that all communications links must be physically protected to a certain level).

The components of the network that form the NTCB must be identified. Furthermore, the modules within an NTCB partition that contain the reference validation mechanism (if any) within that partition must be identified. The procedures for the secure generation of a new version (or copy) of each NTCB partition from source must be described. The procedures and requirements for the secure generation of the NTCB necessitated by changes in the network configuration shall be described.

Procedures for starting each NTCB partition in a secure state shall be specified. Procedures must also be included to resume secure operation of each NTCB partition and/or the NTCB after any lapse in system or subsystem operation.

- Rationale

There may be multiple system administrators with diverse responsibilities. The technical security measures described by these criteria must be used in conjunction with other forms of security in order to achieve security of the network. Additional forms include administrative security, physical security, emanations security, etc.

Extension of this criterion to cover configuration aspects of the network is needed because, for example, proper interconnection of components is typically essential to achieve a correct realization of the network architecture.

As mentioned in the section on Label Integrity, cryptography is one common mechanism employed to protect communication circuits. Encryption transforms the representation of information so that it is unintelligible to unauthorized subjects. Reflecting this transformation, the sensitivity of the ciphertext is generally lower than the cleartext. If encryption methodologies are employed, they shall be approved by the National Security Agency (NSA).

The encryption algorithm and its implementation are outside the scope of these interpretations. This algorithm and implementation may be implemented in a separate device or may be a function of a subject in a component not dedicated to encryption. Without prejudice, either implementation packaging is referred to as an encryption mechanism herein.

The requirements for descriptions of NTCB generation and identification of modules and components that form the NTCB are straightforward extensions of the TCSEC requirements into the network context. In those cases where the vendor does not provide source code, an acceptable procedure shall be to request the vendor to perform the secure generation.

Given the nature of network systems (e.g., various components tend to be down at different times, and the network system must continue operation without that component), it is imperative to know both how to securely start up an NTCB partition, and how to resume operation securely. It is also necessary to know how to resume secure operation of the NTCB after any partition has been down.

23. Test Documentation [4.1.4.3]

- Statement from DoD 5200.28-STD

The system developer shall provide to the evaluators a document that describes the test plan, test procedures that show how the security mechanisms were tested, and results of the security mechanisms' functional testing. It shall include results of testing the effectiveness of the methods used to reduce covert channel bandwidths. THE RESULTS OF THE MAPPING BETWEEN THE FORMAL TOP-LEVEL SPECIFICATION AND THE TCB SOURCE CODE SHALL BE GIVEN.

- Interpretation

The "system developer" is interpreted as "the network system sponsor". The description of the test plan should establish the context in which the testing was or should be conducted. The description should identify any additional test components that are not part of the system being evaluated. This includes a description of the test-relevant functions of such test components and a description of the interfacing of those test components to the system being evaluated. The description of the test plan should also demonstrate that the tests adequately cover the network security policy. The tests should include the features described in the System Architecture and the System Integrity sections. The tests should also include network configuration and sizing.

THE MAPPING BETWEEN THE FTLS AND THE NTCB SOURCE CODE MUST BE CHECKED TO ENSURE TO THE EXTENT POSSIBLE THAT THE FTLS IS A CORRECT REPRESENTATION OF THE SOURCE CODE, AND THAT THE FTLS HAS BEEN STRICTLY ADHERED TO DURING THE DESIGN AND DEVELOPMENT OF THE NETWORK SYSTEM. THIS CHECK MUST BE DONE FOR EACH COMPONENT OF THE NETWORK SYSTEM FOR WHICH AN FTLS EXISTS.

- Rationale

The entity being evaluated may be a networking subsystem (see Appendix A) to which other components must be added to make a complete network system. In that case, this interpretation is extended to include contextual definition because, at evaluation time, it is not possible to validate the test plans without the description of the context for testing the networking subsystem.

The bandwidths of covert channels are used to determine the suitability of a network system for a given environment. The effectiveness of the methods used to reduce these bandwidths must therefore be accurately determined.

24. Design Documentation [4.1.4.4]

- Statement from DoD 5200.28-STD

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the TCB. The interfaces between the TCB modules shall be described. A formal description of the security policy model enforced by the TCB shall be available and an explanation provided to show that it is sufficient to enforce the security policy. The specific TCB protection mechanisms shall be identified and an explanation given to show that they satisfy the model. The descriptive top-level specification (DTLS) shall be shown to be an accurate description of the TCB interface. Documentation shall describe how the TCB implements the reference monitor concept and give an explanation why it is tamper resistant, cannot be bypassed, and is correctly implemented. The TCB implementation (i.e., in hardware, firmware, and software) shall be informally shown to be consistent with the FORMAL TOP-LEVEL SPECIFICATION (FTLS). The elements of the FTLS shall be shown, using informal techniques, to correspond to the elements of the TCB. Documentation shall describe how the TCB is structured to facilitate testing and to enforce least privilege. This documentation shall also present the results of the covert channel analysis and the tradeoffs involved in restricting the channels. All auditable events that may be used in the exploitation of known covert storage channels shall be identified. The bandwidths of known covert storage channels, the use of which is not detectable by the auditing mechanisms, shall be provided. (See the Covert Channel Guideline section.) HARDWARE, FIRMWARE, AND SOFTWARE MECHANISMS NOT DEALT WITH IN THE FTLS BUT STRICTLY INTERNAL TO THE TCB (E.G., MAPPING REGISTERS, DIRECT MEMORY ACCESS I/O) SHALL BE CLEARLY DESCRIBED.

- Interpretation

Explanation of how the sponsor's philosophy of protection is translated into the NTCB shall include a description of how the NTCB is partitioned. The security policy also shall be stated. The description of the interfaces between the NTCB modules shall include the interface(s) between NTCB partitions and modules within the partitions if the modules exist. The sponsor shall describe the security architecture and design, including the allocation of security requirements among components.

The documentation includes both a system description and a set of component DTLS's. The system description addresses the network security architecture and design by specifying the types of components in the network, which ones are trusted, and in what way they must cooperate to support network security objectives. A component DTLS shall be provided for each trusted network component, i.e., each component containing an NTCB partition. Each component DTLS shall describe the interface to the NTCB partition of its component. Both the system description and each component DTLS shall be shown consistent with those assertions in the model that apply to it. Appendix A addresses component evaluation issues.

To show the correspondence between the FTLS and the NTCB implementation, it suffices to show correspondence between each component FTLS and the NTCB partition in that component.

As stated in the introduction to Division B, the sponsor must demonstrate that the NTCB employs the reference monitor concept. The security policy model must be a model for a reference monitor.

The security policy model for each partition implementing a reference monitor shall fully represent the access control policy supported by the partition, including the discretionary and mandatory security policy for secrecy and/or integrity. For the mandatory policy the single dominance relation for sensitivity labels, including secrecy and/or integrity components, shall be precisely defined.

- Rationale

The interpretation is a straightforward extension of the requirement into the context of a network system as defined for this network interpretation. Other documentation, such as description of components and description of operating environment(s) in which the networking subsystem or network system is designed to function, is required elsewhere, e.g., in the Trusted Facility Manual.

In order to be evaluated, a network must possess a coherent Network Security Architecture and Design. (Interconnection of components that do not adhere to such a single coherent Network Security Architecture is addressed in the Interconnection of Accredited AIS, Appendix C.) The Network Security Architecture must address the security-relevant policies, objectives, and protocols. The Network Security Design specifies the interfaces and services that must be incorporated into the network so that it can be evaluated as a trusted entity. There may be multiple designs that conform to the same architecture but are more or less incompatible and non-interoperable (except through the Interconnection Rules). Security related mechanisms requiring cooperation among components are specified in the design in terms of their visible interfaces; mechanisms having no visible interfaces are not specified in this document but are left as implementation decisions.

The Network Security Architecture and Design must be available from the network sponsor before evaluation of the network, or any component, can be undertaken. The Network Security Architecture and

Design must be sufficiently complete, unambiguous, and free from obvious flaws to permit the construction or assembly of a trusted network based on the structure it specifies.

When a component is being designed or presented for evaluation, or when a network assembled from components is assembled or presented for evaluation, there must be a priori evidence that the Network security Architecture and Design are satisfied. That is, the components can be assembled into a network that conforms in every way with the Network Security Architecture and Design to produce a physical realization that is trusted to the extent that its evaluation indicates.

In order for a trusted network to be constructed from components that can be built independently, the Network Security Architecture and Design must completely and unambiguously define the security functionality of components as well as the interfaces between or among components. The Network Security Architecture and Design must be evaluated to determine that a network constructed to its specifications will in fact be trusted, that is, it will be evaluatable under these interpretations.

The term “model” is used in several different ways in a network context, e.g., a “protocol reference model,” a “formal network model,” etc. Only the “security policy model” is addressed by this requirement and is specifically intended to model the interface, viz., “security perimeter,” of the reference monitor and must meet all the requirements defined in the TCSEC. It must be shown that all parts of the TCB are a valid interpretation of the security policy model, i.e., that there is no change to the secure state except as represented by the model.

25. RAMP

The vendor shall have in place procedures, mechanisms, tools, and personnel that comply with the Rating Maintenance Phase (RAMP) requirements for the Trusted Evaluation Program, as applicable to the systems rated B2 and above as enumerated in ANNOUNCE transaction [0268].