(2)

NRL Report 8897

An Approach to Determining Computer Security Requirements for Navy Systems

CARL E. LANDWEHR

Computer Science and Systems Branch
Information Technology Division

and

H. O. LUBBES

Computer Resources Division
Naval Electronic Systems Command

May 13, 1985

NAVAL RESEARCH LABORATORY
Washington, D.C.

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION: UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION/AVAILABILITY OF REPORT: Approved for public release; distribution is unlimited.
2b DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S): NRL Report 8897	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION: Naval Research Laboratory; 6b OFFICE SYMBOL (If applicable): Code 7593	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (City, State, and ZIP Code): Washington, DC 20375-5000	7b. ADDRESS (City, State, and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION: Naval Electronic Systems Command; 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code): Washington, DC 20363-5001	10 SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.
64711N	X0714		DN 380-523

11 TITLE (Include Security Classification)

An Approach to Determining Computer Security Requirements for Navy Systems

12 PERSONAL AUTHOR(S)
Landwehr, Carl E. and Lubbes,* H. O.

13a. TYPE OF REPORT	13b TIME COVERED	14. DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Final	FROM May 1984 TO Jan 1985	1985 May 13	15

16 SUPPLEMENTARY NOTATION

*Computer Resources Division, Code 814T, Naval Electronic Systems Command, Washington, DC 20360

17 COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	(See Page ii) These (The Orange Book)

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

The DoD Trusted Computer System Evaluation Criteria define requirements corresponding to specified levels of security functions and assurance. ~~They~~ do not, however, help determine what level system is required for a specific environment. It is at present left to the system developer to try to assess what level of system is necessary in the environment in which the system is expected to be used. This report proposes a straightforward technique a developer can use to map a specific system architecture and application environment to a particular requirement level as defined in the Criteria. This technique is applicable throughout the system life cycle, so that security requirements can be updated as changes to system structure and function occur. [illegible] Information System); IAIPS (Intermediate Automated Intelligence Processing System)

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT: ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION: UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL: Carl E. Landwehr	22b TELEPHONE (Include Area Code): (202) 767-3381; 22c. OFFICE SYMBOL: Code 7593

DD FORM 1473, 84 MAR — 83 APR edition may be used until exhausted. All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

18. SUBJECT TERMS

Multilevel security
Evaluation criteria
Environments
Security requirements
Trusted computer system
Trusted computing base
Computer security
Network security

CONTENTS

AN APPROACH TO DETERMINING COMPUTER SECURITY REQUIREMENTS FOR NAVY SYSTEMS

INTRODUCTION

This report presents a method for determining the hardware and software security requirements of a system based on

- the local processing capability available to a system user;
- the kind of communication path between the user's local device and the primary system components;
- the flexibility of the processing capability the system provides to the user;
- the environment in which the system was developed; and
- the difference between the clearance held by the least-cleared user of the system and the classification of the most sensitive data processed by the system.

This method takes into account current policy [1], guidance [2], proposed future guidance [3], and current technical literature in computer security. It can be understood as a risk evaluation of a system that can be conducted at a very early stage in the life cycle of a system. This method also can be repeated as the structure and functions of the system change during its development and operation. Depending on the inherent risk that a system (or system design) displays, different levels of security requirements may be imposed to reduce the operational risk of the system to an acceptable level. Applications of this method to several environments are provided as examples.

The technique described here does not consider requirements for degaussing of removable storage units, TEMPEST requirements, protection from physical hazards, emergency destruction, or other security requirements not related to the hardware and software architecture of the system.

REVIEW OF CURRENT GUIDANCE FOR COMPUTER SECURITY REQUIREMENTS

Existing documents [1] define policy, procedures, and technical guidance for computer security. The technical guidance is based on concepts that are up to 12 years old. Computer security research has increased knowledge of how to specify system security functions and how to assure that secure systems implement them correctly; the DoD Trusted Computer System Evaluation Criteria (the Orange Book) [2] document this knowledge.

The Orange Book provides a set of security requirements of two kinds: specific security feature requirements, which call for particular system functions to provide data security, and assurance requirements, which call for testing, documentation, and verification to assure that the security features are correctly implemented. A system that satisfies all requirements listed in the Orange Book would be designated A1. Systems that satisfy specified, nested subsets of the requirements are designated B3, B2, B1, C2, C1, D, in order of decreasing requirements.

Manuscript approved January 24, 1985.

The Orange Book does not provide guidance as to what level of system is appropriate for a particular operational environment. A draft application doctrine [3] has been developed, however, that defines the level of system required for a particular environment based only on the classification of the data processed by the system, the clearances of its users, and the environment in which it was developed. This simple scheme is inadequate for use in assessing Navy security requirements; a more comprehensive method is proposed here.

Reviewing the specific technical requirements imposed by current DoD directives governing compartmented mode operation shows that, with minor exceptions, each requirement corresponds to one included in the B2 subset specified by the Orange Book. Because its requirements are developed more systematically and within a more comprehensive framework, the Orange Book provides better technical guidance than the existing DoD directives.

An analogy that illustrates the relationship between the Orange Book requirements and those of existing directives can be drawn from automobile safety regulations. A specific regulation (like existing directives) might require cars to be equipped with lap and shoulder belts. A less specific (but still precise) regulation (like the Orange Book) might require a passenger restraint system. A car equipped with air bags would satisfy the Orange Book kind of regulation and would in fact be safe even though it would not satisfy the more narrow requirement for lap and shoulder belts.

The technical approach advocated in OPNAVINST 5239.1A is based on conducting a risk assessment to define a specific annual loss expectancy, in dollars, for a system. Based on this assessment, cost/benefit analyses of potential countermeasures are to be conducted, but no specific technical requirements are provided that developers might use to guide their efforts in developing systems initially or in specifying countermeasures.

APPLYING TECHNICAL COMPUTER SECURITY GUIDANCE EFFECTIVELY

Although it is imperfect in many respects, as a technical basis for specifying computer security requirements, the Orange Book is the most comprehensive and current document available. A method is needed for applying the Orange Book to the components of large scale, geographically dispersed systems operated by the Navy, so that the appropriate requirements from the Orange Book can be identified for each system. Such a method is defined below. As shown in Fig. 1, it involves:

- extracting from each system (or system design) the factors that affect the risk that its operation may lead to the unauthorized disclosure of sensitive information,
- quantifying these factors, and
- determining system security requirements (in terms of the levels defined in the Orange Book) that reduce the system risk to an acceptable level.

This method can be understood as a risk evaluation based on the threat of unauthorized disclosure of sensitive information. The asset of the system is sensitive information, defined in terms of its classification level; the vulnerabilities of the system depend on the degree of control it exerts on its users. The system risk combines the value of the assets, the vulnerabilities of the system, and the clearance of the users.

Identifying the Risk Factors

To determine a system's security requirements, it is necessary to consider the environment in which that system operates. The Orange Book specifies levels of requirements independent of system environment. The draft application doctrine [3] characterizes a system's environment in terms of three

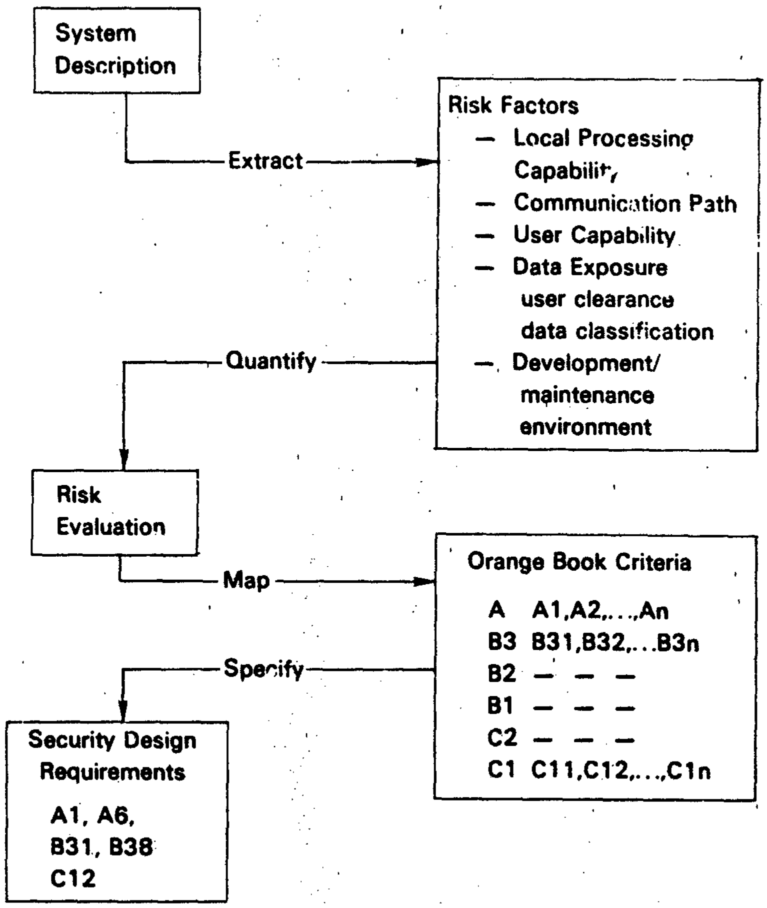

Fig. 1 — Steps in applying Guidance

parameters, the maximum clearance of the least-cleared user, the maximum classification of data processed by the system, and the environment in which the system is developed and maintained (open or closed). Although simple to evaluate, these parameters omit important factors that affect actual system risk.

The factors that should be considered are discussed below. For each factor, different levels of risk are defined so that the difference between two adjacent levels in each factor represents a roughly comparable increase (or decrease) in risk. Factors are defined so that they are roughly independent—a change in one factor does not imply a change in another factor. These properties allow numbering the risk levels and combining them, in most cases using simple addition.

Something as abstract as risk cannot be quantified precisely. Recognizing this, we have not attempted to make fine distinctions, and some systems still will fall near the boundaries of the proposed classes. Nevertheless, the scheme described below, coarse as it is, captures the intuition and experience of computer security practitioners and is preferable to simply setting these considerations aside because they cannot be made precise.

Local Processing Capability

Some systems have receive-only terminals (e.g., stock transaction displays, airline terminal monitors); users of these terminals have no way to enter system commands directly. These terminals represent a lower level of risk than interactive terminals that permit both sending and receiving information. Replacing a fixed-function interactive terminal with a programmable terminal, personal computer, or other programmable device introduces a higher level of risk because the user now can program the terminal to enter commands. A user who accesses a system from a fixed-function terminal but via a programmable host computer would be considered to have the same local processing capability as one who uses a personal computer as a terminal. The identified risk levels for local processing capability are:

Level 1: receive-only terminal

Level 2: fixed-function interactive terminal

Level 3: programmable device (access via personal computer or programmable host).

Communication Path

The communication path between terminal and host can also affect system risk. A terminal that has a simplex receive-only link to its host via a store-and-forward (S/F) network (e.g., using the fleet broadcast) poses less risk than one that is connected via a duplex store-and-forward link, since the simplex path prevents the user from submitting requests to the system. Terminals that are connected to a host, either directly, through a local-area network, or through a long-haul packet network (e.g., DDN), are more vulnerable to penetrations than those connected only through a store-and-forward net. This is because of the increased bandwidth and closer host-terminal interaction they permit. The identified risk levels for communication path are:

Level 1: store/forward, receive-only

Level 2: store/forward, send/receive

Level 3: interactive (I/A), via direct connection, local-area net, or long-haul packet net.

User Capability

Regardless of the local processing available to a user or the communication path used to access a host, if that host is programmed only to provide predefined outputs regardless of the inputs the user presents, it is less risky than a system that responds to user transactions. In this sense, the system that generates the ticker tape for a stock exchange is less at risk to the terminals that display the tape than an interactive electronic banking system is to automated teller machines. Finally, a transaction-based system is less at risk from its users than a system that permits its users full programming capabilities. The identified risk levels for user capability are:

Level 1: output only

Level 2: transaction processing

Level 3: full programming.

Development/Maintenance Environment

A system that has been developed and is maintained by cleared individuals under close configuration control (closed environment) should pose less risk than one that is not developed and maintained in this way (open environment). This distinction has been proposed in the draft application doctrine [3]. It seems a reasonable one, but relatively few examples of systems developed and maintained according to the proposed definition of closed environment have been identified outside of the intelligence community. For simplicity, we assume that systems are developed and operated in an open environment. Systems that are developed and maintained in a closed environment may therefore be subject to slightly less stringent requirements than will result from our approach.

Data Exposure

A system that has a greater disparity between the clearance of its least-cleared user and the classification of the most sensitive data it processes is more at risk than one that has a lesser disparity. The draft application doctrine proposes a scheme for numbering and classifying risk range; we adopt this scheme but call it data exposure to distinguish it from other risk factors. Clearance levels are identified as:

Level 0: uncleared

Level 1: uncleared, but authorized access to sensitive unclassified information

Level 2: confidential clearance

Level 3: secret clearance

Level 4: top secret/background investigation

Level 5: top secret/special background investigation

Level 6: top secret/special background investigation, with authorization for one compartment

Level 7: top secret/special background investigation, with authorization for more than one compartment.

Classification levels are numbered:

Level 0: unclassified

Level 1: sensitive unclassified information

Level 2: confidential

Level 3: secret

Level 4: secret with one category

Level 5: top secret with no categories, or secret with two or more categories

Level 6: top secret with one category

Level 7: top secret with two or more categories.

Data exposure is computed as the difference between the level of the least-cleared user of a system and the maximum level of data processed by the system. It thus ranges from a value of 0 (all users cleared for all data) to 7 (system processes top secret data with two or more categories and some users are uncleared.

Applying the Risk Factors

For a particular system, each of the factors above must be evaluated to assess its overall risk. Based on that risk, security requirements can then be determined. These requirements are characterized here in terms of the levels defined in the Orange Book because they have been published and reviewed widely. If a different subsetting of the Orange Book requirements later proves more appropriate than the current set of levels, the new subsets can be substituted. Tables 1 through 3 provide the necessary mappings between factor values, risk factor levels, and security requirements. Note that in a given system, different terminals may provide different functions, lead to different levels of risk, and impose different security requirements. Security requirements for the system as a whole must be determined on the basis of the most risky part. As noted previously, the tables assume that all systems are developed and maintained under open environment conditions.

Table 1 — Process Coupling Risk

Local Processing Capability	Communication Path		
	1. S/F Net (one-way)	2. S/F Net (two-way)	3. I/A Net or Direct Connection (LAN,DDN)
1. Receive-only terminal	2[1]	3	4
2. Interactive terminal (fixed function)	2	4	5[2,4]
3. Programmable device (Access via personal computer or programmable host)	4	5	6[3]

Table 2 — System Risk

User Capability	Process Coupling Risk				
	2	3	4	5	6
1. Output-only (subscriber)	3[1]	4	5	6	7
2. Transaction processing	—	5	6	7[2]	8
3. Full programming	—	6	7	8[4]	9[3]

Table 3 — Mapping System Risk and Data Exposure to Orange Book Levels

Data Exposure	System Risk						
	3	4	5	6	7	8	9
0	C1	C1	C1	C1/C2	C2[2]	C2	C2
1	C1/C2	C2	C2	C2	C2/B1	B1	B1
2	C2	C2/B1	B1	B1	B1	B1/B2[4]	B2[3]
3	B1	B1	B1/B2	B2	B2/B3	B3	B3/A1
4	B2[1]	B2/B[illegible]	B3	B3/A1	A1	A1	A1
5	B3/A1	A1	A1	—	—	—	—
6	—	—	—	—	—	—	—
7	—	—	—	—	—	—	—

[1] Ocean Surveillance Information System (OSIS) subscriber environment
[2] OSIS analyst environment
[3] Integrated Automated Intelligence Processing System (IAIPS) analyst environment
[4] Orange Book environment
[5] Air Force Data Services Center (AFDSC) Multics programmer

Table 1. Together, local processing capability and communication path characterize what computer security literature refers to as the process coupling risk. This term defines how well a process in one computer can maintain its integrity in the face of attempts to subvert it from outside. A high degree of coupling represents a close degree of interaction between two processes, hence a greater vulnerability of one to the other. If there is a very limited, well-defined set of requests one process can make of the other, the degree of process coupling will be low. Process coupling risk in a system, as shown in Table 1, is the sum of the local processing capability and communication path risks, with one exception. A fixed function, interactive terminal attached to a one-way store-and-forward communication path does not increase risk over a receive-only terminal on the same link. A programmable device increases risk over the interactive terminal, since, if improperly programmed, it might corrupt labels transmitted with data.

Table 2. The process coupling value from Table 1 combined with the appropriate user capability factor value yields an overall system risk that is independent of the data exposure. As in Table 1, the entries of Table 2 have been obtained by summing the risk factor values from each axis. The entries for a process coupling of 2 (receive-only or interactive terminal on a receive-only link) have been omitted for user capabilities of transaction processing and full programming, since a receive-only link cannot support either of these capabilities.

Table 3. This table relates the system risk with the data exposure to yield a level from the Orange Book that defines the security requirements for the system. As noted above, the Orange Book levels may later be replaced by related but distinct sets of features and assurances. The entries in this table were generated by working through examples and considering the guidance provided by the draft application doctrine and current DoD directives governing compartmented mode. Blank entries indicate that for the specified data exposure level and system risk it does not appear technically feasible to meet the appropriate security requirements at the time.

EXAMPLES

Ocean Surveillance Information System

Consider the application of the technique outlined above to the Ocean Surveillance Information System (OSIS). OSIS collects information from a variety of SI and Genser sources and distributes it to a variety of SI and Genser customers. OSIS maintains two major data bases: a track data base of sighting information that is both automatically and manually updated and a technical data base that contains characteristics of hostile and friendly platforms. There are two major classes of OSIS users: analysts and subscribers.

OSIS analysts are the direct operators of the system. They resolve ambiguities when the system cannot associate a particular sighting with a particular platform; they can cause messages to be sent to subscribers automatically on a regular basis; they can update the data bases. These analysts operate interactive terminals that are located in OSIS spaces and connected directly to the OSIS computers.

OSIS subscribers receive reports generated by OSIS. They are located outside the OSIS spaces and receive reports over a variety of different communication networks on receive-only terminals. They cannot directly enter data into the OSIS system, but they can issue requests (via normal message channels) for regular updates on the location of particular platforms, for example. These requests are received by OSIS analysts who set up filters that automatically channel relevant reports to the subscriber. Once the appropriate filter is set up, no further human intervention is required.

Since analysts and subscribers are permitted different kinds of functions, have different clearances, and communicate with the OSIS system over different paths, this technique must be applied separately to each class of user.

Local Processing Capability

Analysts operate fixed function interactive terminals, so they represent a risk level of 2. Subscribers operate receive-only terminals and have a risk level of 1.

Communication Path

Analysts communicate with OSIS machines directly, so their risk level is 3. Subscribers communicate over a one-way store-and-forward network; their risk level is 1.

User Capability

Analysts are permitted to issue transactions directly to OSIS, but they do not have full programming capability; the risk level is 2. Subscribers have output-only capability; the risk level is 1.

Data Exposure

OSIS processes data at the top secret (TS) level with multiple compartments; the classification level is 7. OSIS analysts hold TS clearances with special background investigations (SBI) and are authorized access for all compartments that OSIS processes. Consequently, their clearance level is also 7 and the data exposure for analysts is 0. Some OSIS subscribers hold only secret clearances with no compartment authorizations; their clearance level is 3, yielding a data exposure for subscribers of 4.

Using the Tables

First, for analysts, Table 1 shows that a local processing capability risk of 2 and communication path risk of 3 yields a process coupling risk of 5. Table 2 combines a user capability risk of 2 with a process coupling risk of 5 to yield a system risk of 7. Table 3 maps a data exposure of 0 and a system risk of 7 to a C2-level system requirement.

For subscribers, Table 1 combines a local processing capability risk of 1 with a communication path risk of 1 to yield a process coupling risk of 2. Table 2 combines a user capability risk of 1 with a process coupling risk of 2 to give a system risk of 3. Finally, Table 3 maps a data exposure of 4 and a system risk of 3 to a B2 level system requirement.

Since OSIS includes both kinds of users, the more stringent of the two requirements (i.e., B2) would apply. Changes to the environments of either subscribers or analysts (such as the introduction of personal computers in place of fixed function terminals) would require the risk evaluation to be repeated, and could lead to a change in the level of security requirement.

Other Systems and Environments

Results for two other environments, the Integrated Automated Intelligence Processing System (IAIPS) and the Orange Book environment, are noted in Tables 1 through 3 and are briefly explained here. IAIPS is a database system for intelligence analysts that provides each analyst with a personal computer as a terminal. The personal computers are connected via a local-area network to the host system. As noted in Table 1, the process coupling risk is thus 6. IAIPS analysts are also permitted full programming capability on the host system, yielding a system risk of 9, as shown in Table 2. The IAIPS system will contain top secret, multicompartment data (=7) and, though all of its users will have top secret clearances with special background investigations, some of them will not be authorized for any compartments (=5), yielding a data exposure of 2. Table 3 shows that a system risk of 9 and data exposure of 2 leads to a security requirement for a B2-level system for IAIPS.

The Orange Book does not explicitly define an environment. However, the predecessors of the Orange Book criteria were first developed in the context of an interactive computer system that provided users with directly connected, fixed-function terminals and full programming capability. The corresponding entries in Tables 1 and 2 are noted; they yield a system risk of 8. Since no data exposure is defined for the Orange Book environment, Table 3 shows the result for the Air Force Data Services Center (AFDSC) Multics environment which provides full programming to users at fixed function, directly connected terminals. AFDSC Multics includes noncompartmented data classified up to top secret. Since some users have only secret clearances, data exposure is 2, and the resulting security requirement from Table 3 is for a B1/B2 system. Multics is currently being evaluated by the DoD Computer Security Evaluation Center and is expected to achieve a B2 rating.

DISCUSSION

Here we address some possible objections to the approach described above.

Objection: The proposed scheme imposes different requirements on a host computer, based on characteristics of the user's terminal and the communication path between the terminal and the host. These are outside the security perimeter of the host and therefore should not affect the security required of it.

Response: Security considerations include not only protecting data up to the point that it leaves the system but also resisting attacks on the system by external users. Users with personal computers and direct connections to systems have proven to be a greater threat (e.g. in terms of their ability to defeat password schemes) than those who have only fixed-function terminals at their disposal. Each higher Orange Book level adds assurance requirements as well as security feature requirements. While the security features added at a particular level may or may not improve protection against threats posed by terminals and networks connected to a host, the increased assurance provided by each incremental level should decrease the likelihood of flaws that could be exploited from outside the security perimeter. It is thus appropriate to increase the Orange Book level required of a host based on the risk factors assigned to the user capability and communication path.

Objection: The proposed approach in some cases permits hosts to meet lower security requirements than would the draft application doctrine [3].

Response: The approach proposed here distinguishes aspects of application system structure that reduce its vulnerability to outside attacks. The draft application doctrine determines the level of system required, based primarily on the clearances of system users and the classification of data stored in the system. There is no distinction, for example, between a system in which users can only view output and one in which users can construct and execute their own programs. Consequently, the proposed requirements must be based on the worst-case assumption (user programming). By providing a more detailed model of the environment, the approach proposed here permits a more accurate assessment of the security actually required.

Objection: Previous attempts to distinguish rigorously between a system that can be programmed and one to which only transactions can be submitted have failed.

Response: While a formal mathematical distinction between systems that users can program and those that perform a fixed set of functions in response to user requests may never be defined, it does not seem to be a difficult distinction to make in practice. In cases that are difficult to decide (e.g., a transaction-processing database system that permits a complex query and update capability), it is safe to assign the system the higher risk factor.

Objection: Because the proposed approach determines host security requirements partly based on system architecture, changes to the architecture may lead to different security requirements.

Response: This is actually a benefit of the approach. As a system changes during its design, development, and operation, the effects of those changes on host security requirements can be easily assessed, providing a practical way to use the Orange Book requirements throughout the system life cycle. If, for example, a B2 host will not be available to support an application as originally planned and a B1 host must be used instead, the approach proposed here can help determine how system functions, user capabilities, or communication paths could be restricted to compensate for the less secure host. Conversely, if new functions or terminals are added to a system already under development, this approach can indicate whether host security will need to be upgraded as a result. The only tradeoff that would be recognized under the draft application doctrine would be limiting the classification of the data processed by the system or increasing the clearance level of its users.

SUMMARY AND RECOMMENDATIONS

Existing technical guidance for computer security has been reviewed, and an approach to determining architectural system hardware/software security requirements has been proposed. Approaches for determining other security requirements (e.g., TEMPEST, degaussing, COMSEC, contingency planning) are beyond the scope of this approach. The proposed approach for hardware/software requirements uses the technical requirements and the system levels listed in the Orange Book.

Specifically, we recommend:

- that the security requirements documented in the Orange Book be used as the baseline for technical (hardware and software) computer security requirements;
- that the procedure outlined in this report be used to determine the appropriate subset of technical computer security requirements in lieu of OPNAVINST 5239.1A; and
- that the Navy conduct a thorough review of the structure of levels in the Orange Book and propose an organization of requirements that meshes with Navy needs.

REFERENCES

1. OPNAV Instruction 5239.1A, Department of the Navy ADP Security Program, 3 Aug., 1982.

2. Department of Defense Trusted Computer System Evaluation Criteria, DoD Computer Security Evaluation Center, CSC-STD-001-83, 15 Aug. 1983.

3. Brand, S., "Environmental Guidelines for Using the DoD Trusted Computer System Evaluation Criteria," Proc. Seventh DoD/NBS Computer Security Initiative Conference, Sept. 1984, Gaithersburg, MD, pp. 17-23.

END

FILMED

8-85

DTIC