a. Extension of task to non-SCI
b. Not directive, for implementation

IBSEC-CSS-R

Computer Security Subcommittee
of the
United States Intelligence Board
Security Committee

Guidelines for the Security Analysis, Test and Evaluation of Resource-Sharing Computer Systems

I. Purpose:

To provide basic guidelines for the security analysis, test and evaluation of resource-sharing computer systems wherein the protection of the Community data stored and/or processed must be ensured. To list some of the conditions, features, procedures and related conditions which should be analyzed, tested and evaluated prior to system accreditation for resource-sharing computer operation, guidelines are developed for remotely accessed resource-sharing computer systems, they may also be applied to other systems.

II. Scope:

The guidance contained herein is applicable to all community intelligence functions using resource-sharing computer systems support for which special handling controls have been established.

II General:

Guidelines for Determination of System Security Capabilities:

As a basis for accreditation all accredited resource-sharing computer systems should be analyzed, tested and evaluated for the possession and functionally dependable operability of security protection features

Insert (1)

and procedures. ~~Computer security analysis, test and evaluation should constitute the basis for system accreditation.~~ [The results ~~culmination~~ of ~~this effort should be a statement either recommending or not recommending such accreditation and an explanation of the reasons for that statement.~~] The security analysis, test and evaluation should be conducted when the system is operating under relatively static, though productive, conditions. During this time systems changes must be separately evaluated in light of their impact on both the security of the system and the status of the analysis, test and evaluation. Test Plan. (Model incl. acceptability criteria)

Add feedback Stability → w/ examples Retesting & Continuing Review III

A. Security Analysis - This process will encompass the identification ~~accumulation~~ of all ~~conceptual approaches and~~ features for providing security protection of information handled (to be handled) within a resource-sharing computer system. ~~and applying these as they pertain~~ Determine how these features are applied to the software, hardware and procedural conditions of the system. [System configurations, capabilities, locations and procedures will vary widely among organizations using this guidance; however, it is essential that, insofar as possible, they all be analyzed based upon this guidance in conjunction with agency/departmental regulatory guidance.] Security analysis is requisite to security testing which is, in turn, requisite to security evaluation. While these may be independent phases, they are not mutually exclusive. In fact, the pursuit of one phase may require refinement of the others, regardless of the stage

Relationship of Environ to sec. reqts.

of completion of all. The security analysis will be the process of identifying security safeguards and ordering them into a framework based upon the manner and degree to which they are designed to guard against possible security vulnerabilities.

1. Hardware Controls

a. Memory protect device - A determination should be made to insure that a memory protect device feature is available to detect and prevent any attempt to read or write outside the area of memory assigned to a given user or application. These devices can fail, therefore, it is advisable to require a special program which will attempt to deliberately and frequently violate the memory bounds.

b. Separation of data by device (or within device) - Similar to memory protect, except that data separation is not normally additionally dependent upon software protection. However, when data is resident in memory, it is dependent upon memory protection.

c. Protection state variables - The execution state of a processor may include one or more variables which determine the interpretation of instructions executed by the processor. These variables should be identified at the outset of the security analysis exercise. For example, a processor might have a master/slave mode protection state variable, in which certain instructions are illegal except in master mode.

2. Software Controls

a. Security labels - Security classification and other required control labels should be identified with the information and programs in the system to insure appropriate labeling of output/input and access authority.

b. User Identification/Authentication - User identification/authentication for access to resource-sharing computer systems will primarily apply to remote users; however, all persons accessing any part of the system should be required to identify themselves in some manner. This will be the (software) means by which the system assures that the individual at a terminal or access unit is the person he represents himself to be and has authority to access information which he is requesting.

c. System Supervisor (also known as Executive and Monitor). The supervisor acts as the overall guard of the system. It is that portion of the software which internally manages job flow through the computer, allocates systems resources to jobs, and controls information flowing to and from files and terminals. The malfunction or deliberate alteration of the supervisor could couple information from one program to another; change the security classification of users, files or programs; or, at a minimum, destroy information in the system. For these reasons, rigid controls must be inforced to insure that only authorized personnel have access to the supervisor.

d. Privileged instructions - Coupled with the supervisor and the hardware controls, the architecture of the

computer should provide for privileged instructions. The set of privileged instructions must contain all input/output commands and also every command which could change a memory boundary or protection barrier. Moreover, the design of the computer should be such as to insure that only the supervisor program can operate the privileged instructions. It is absolutely essential that the supervisor program not be by-passed.

e. Separation of User/Executive Modes of Operation - The user and executive modes of system operation shall be separated so that a program operating in user mode is prevented from performing unauthorized executive functions.

f. Residue Cleanout - Instructions for performing residue cleanout of its data should be standard within the system for all user programs to execute under the following conditions:

✓ (1) Upon job completion.

✓ (2) Upon program error (without recovery)

~~(3) Upon notification by the Supervisor that an intrusion has been attempted.~~

~~(4) Upon site environment failure.~~ (eg power)

(5) Upon release of the allocated storage area to the supervisor.

(6) Upon each program ~~systems' bootstrap, whether system recovery or~~ initiation.

(7) Before allocation and after de-allocation of any assigned permanent user storage area.

(8) optionally, when determined necessary by the ISSO

g. Audit Trail - The computer system should produce in a secure manner an audit trail containing sufficient information to permit a regular security review of system activity. System usage recording functions can be used to detect improper use or maintenance of the data base. These functions are specifically directed toward protection of data security and assured integrity. They should be performed by the system Supervisor in connection with a special system log and access authentication library. The audit trail will allow for:

(1) Detection of data base/system misuse.

(2) Documentation of data base/system misuse.

(3) Audit of task performance.

3. Other Controls:

a. Personnel Security

(1) During the analysis, a determination will be made that all personnel who have an operational requirement to access the computer center and/or remote terminals have been cleared to the highest level of classified information stored or processed by the system. All other personnel must be properly escorted.

(2) Procedures will be insured for unescorted access to the computer center area. This access should be limited to personnel with a predetermined need and holding clearances commensurate with the highest category of classified information processed or stored by the system. Access to a

remote terminal should be limited to personnel who are cleared and have access approvals for information designated for output at that terminal.

b. Physical Security

(1) A determination will be made that the computer facility and remote terminals meet applicable physical security standards prescribed for safeguarding classified information stored or processed by the system.

(2) Physical security requirements for the computer center area should be based upon the over-all requirements of the entire system; however, remote terminal area requirements may be based upon the highest level of information designated for input/output at each terminal.

(3) Provisions may be made for downgrading area controls to the level of protection required for the information actually being processed provided that measures are taken to maintain a level of security commensurate with the highest category of classified information resident in the system.

c. Communications Links - The communications links between all components of a system shall be secured in a manner appropriate for the transmission of the highest classified data designated to be carried by the link.

d. Emanations Security - Control measures and tests will be applied to equipment and systems to the extent necessary to prevent the compromise of classified or controlled

information by the unauthorized interception of spurious emissions from equipment used to process the information. Individual organizations will retain the responsibility for applying control measures for those systems within their purview in accordance with the National Policy on Compromising Emanations.

e. Procedures and Administrative Safeguards

(1) Procedures and administrative processes and channels must be established to maintain access controls and to insure that system security measures are performing adequately.

(2) Procedures prescribed for systems users at remote terminals must provide adequate protection for all levels and categories of classified information handled by each terminal.

(3) Computer facility access procedures must be established to provide maximum control over access to the area.

B. Security Testing - This process will include the inspection and testing of the hardware, software, physical and procedural security features of the resource-sharing system under study. The testing will determine the degree to which the system conforms to the requirements of appropriate regulations and policies. The extent and duration of the inspection and testing, and the development of standards and other criteria to be met will depend heavily on the manner in

which the hardware and software is constructed and the class of the system being studied. The process measures the extent to which security safeguards guard against projected security vulnerabilities.

1. Hardware Controls

a. Memory Protect Device - This device should be exercised over a period of time, utilizing all available or representative programs, to insure the positive operability of the device.

b. Separation of data by device (or within device) - A check should be made to determine the extent of this technique and the security protection afforded data from these devices while they are core resident. This technique will depend upon other protection features once data has left the resident peripherals or devices.

c. Protection State Variables - The actual ability of the processor to access locations in primary memory will be tested to insure that all original and modified capabilities are known, understood and controlled.

2. Software Controls

a. Security labels - The use of security labels will be closely related to external labeling, internal file or record labeling and user identification/authorization. Access to the data contents will be controlled through the label identification. Furthermore, each user will possess access to

resident files based upon his identification/authorization label access authority, which will be contained in the access libraries and/or executive system.

b. User Identification/Authentication - The user activity must insure that only individuals with proper clearance and access authorization are permitted to utilize remote terminals at their activity. Additionally, software checks should be introduced and used to insure user authentication for the access of specified files or data which is available through the system. Numerous methodologies of user identification/authentication have been and are being devised. Regardless of the specific method chosen, the recommended approach of system resources from a security authority standpoint is a software lockout in which a number of program checks are made against the following input parameters:

(1) User name.

(2) User classification and security release codes.

(3) Console identification.

(4) Console classification.

(5) Overlay identification.

(6) Program classification and security release codes.

(7) Record classification and security release codes.

Software control of the release of data by security classification and control codes promises to provide greater efficiency in system usage with security control and provides a better foundation for control on interchanges of data with other systems where direct interface becomes a reality. The security test of this feature will determine the capabilities and functional operability.

c. System Supervisor - A check should be made to insure that rigid access control is exercised over the Supervisor. Only specified individuals should be permitted to change, modify, update or otherwise alter the Supervisor. A file-query system which merely provides the user at a remote terminal the capability to access files using a set of fully checked programs is probably the least dangerous mode of operation in a resource-sharing computer system.

d. Privileged Instructions - A check should be made to ascertain the extent of use of privileged instructions, if any exist. The check should also include user access to these instructions and maintenance responsibilities. A life test using the instructions should be accomplished against various software systems to verify the exact functions and results of the instructions from a security/data integrity standpoint.

e. Separation of User/Executive Modes of Operation - A test should be performed, after investigation of

the system documentation, to insure that application/user programs are incapable of performing any alteration to the executive. It may be necessary to investigate all user programs to make this determination.

f. Residue Cleanout - A test should be performed to confirm the operability of the residue cleanout function. Upon execution of residue cleanout instructions, sample data should be printed/displayed to allow review to insure that the process has been successful. Measures should be implemented to insure that memory residue from terminated user programs is made inaccessible to unauthorized users.

g. Audit Trail - During the testing of the audit trail software feature, special care must be used to confirm that all access and security authorization violations are detected and recorded. For this reason, special "spy" programs or intentional violator programs should be exercised against the system to determine the effectiveness of the audit trail to detect violators and give the appropriate alarm. The other system accounting capabilities of the audit trail should be secondary to security protect features.

C. Security Evaluation - Based upon the security analysis and test results, a thorough evaluation should be conducted with the final objective being system accreditation for multi-level security, resource-sharing computer environment. The decision should be based upon a demonstrated capability of the

entire system; its hardware, software, procedures, physical plant and personnel, that adequate protection can and will be provided the information scheduled to be processed by the system.