~~CONFIDENTIAL~~

IBSEC-CSS-R-____

Computer Security Subcommittee

of the

United States Intelligence Board

Security Committee

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

I. PURPOSE:

To prescribe the basic guidance for the security analysis, test and evaluation of resource-sharing computer systems wherein the security, authority and integrity of the data stored and/or processed must be ensured. To specify the conditions, features, procedures and relative conditions which must be analyzed, tested and evaluated prior to the system receiving accreditation within the resource-sharing computer environment.[1]

II SCOPE:

The guidance contained herein is applicable to all

[1] DCID No. 1/16 (New Series) assignes the responsibility for the security analysis, test and evaluation as well as for the accreditation of such systems to individual USIB members.

~~CONFIDENTIAL~~

community intelligence functions using resource-sharing computer systems support for which special handling controls have been established.

III. REQUIREMENTS:

A. This guidance is required to sufficiently analyze, test, and evaluate resource-sharing computer systems to ensure that the security, authority, and integrity of information stored or processed in such systems is maintained by the system users.[2] Since all users in an expanded system environment may not work within one valuted area or within a single-level security environment, and may not possess the same security clearance, the techniques to be used must be beyond those used in current intelligence data handling systems.

B. Techniques for interfacing with other intelligence data handling systems are also required so that present and future resource-sharing computer systems can be fully utilized in an operational environment.

C. Techniques are required to handle the following conditions:

1. Simultaneous multi-level query using on-line terminals.

2/ Users are described as anyone connected with the resource-sharing computer system whether he be an operator, data base monitor, systems manager, systems analyst, librarian, job scheduler, Information System Security Officer, or functional area user of automated products.

2. Control of content integrity of the data base.

3. Maintenance of working data within the data base.

4. Selection and extraction of data elements from the data base to produce reports and products at various levels of security classification.

5. Control of on-line updating authority of data elements within the data base.

6. Others?

IV. OBJECTIVES:

The objectives of these guidelines are to provide technical approaches to fulfill multi-level security, authority, and integrity operation requirements based upon the following:

A. Hardware, software, and procedural techniques for controlling access to inputs and outputs.

B. Implementation factors in the application of such techniques.

C. System developments and tests being conducted or considered by various community agencies with comparable systems.

V. PROBLEM DEFINITION:

The problem of data protection in resource-sharing computer systems involves data security, authority, and integrity considerations. These three aspects of data protection overlap to some extent, and a deficiency in any of them may affect the others. These aspects are defined as follows:

A. Data security concerns prevention of disclosure of data to personnel or terminals at levels higher than authorized. Disclosure can occur through either accident or deliberate penetration.

B. Data authority is concerned with the authority for making changes to the system, primarily the data base; however, including any portion of the software or hardware systems which could affect data content.

C. Data integrity is concerned with the validity, accuracy, and completeness of data in the system, the isolation of errors; the problems of system degradation and recovery.

VI **DEFINITIONS:**

A. Security Analysis - This process will encompass the accumulation of all conceptual approaches for providing security protection of information handled (to be handled) within a resource-sharing computer system and applying these approaches as they pertain to the physical, software, hardware and procedural conditions of the system. The proof of security protection.

B. Security Test - The inspection and testing of the hardware, software, physical and procedural security features of the resource-sharing system under study. To be conducted by expert technical personnel to 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 system being evaluated. The evidence of security protection.

C. Security Evaluation - The determination that the system performance does, or does not, meet the criteria established for the resource-sharing environment as established herein. This process includes the study and interpretation of the results of both the analysis and test phases, and will ultimately provide the basis for the recommendations for system certification.

VII SPECIFIC PROCEDURES.

A. At an early phase in planning for a new automatic data processing (ADP) facility, or in planning for replacement or modification of an existing computer facility, the organization commander should consider methods for making most effective use of his ADP resources. In so doing, the various possible approaches to sharing ADP resources should be analyzed and each should be examined in light of the following factors:

1. Effectiveness of support to the Commander.

2. Existing national security regulations.

3. Existing "state-of-the-art" in computer and communications technology.

4. Comparative costs, including hardware, software, site preparation, personnel, management, security clearances, power, and air conditioning.

B. The degree to which ADP resources will be shared should be decided on a case-by-case basis. While both cost effectiveness and management implications will be considered, the controlling factors should be operational considerations and responsiveness consistent with security requirements.

C. Once the organization commander has determined that the subject computer system is required to operate in a resource-sharing environment, he will request system security analysis, test, evaluation and certification from his responsible USIB member. Upon receipt of such request, the USIB member will appoint a (or activate his appointed) team of technical experts who will perform the certification review. This team will be composed of competent individuals trained and experienced in both security and computer technical applications, policies and procedures.

1. The certification team will have earlier specified the exact test procedures and evaluation criteria for the type system. Additionally, the team will provide technical assistance to individual security officers who are charged to manage/approve/control changes in hardware/software to a system previously certified.

2. The team will specify (exercise or test) computer programs which overtly attempt to penetrate the system so that necessary statistical data can be collected.

3. Guidance will be provided by the responsible USIB member on procedures and other matters that may assist in arriving at a decision when approval to operate the computer in a resource-sharing environment is requested.

D. All accredited resource-sharing computer systems shall be analyzed, tested and evaluated for the possession of the following security capabilities, as an absolute minimum:

1. Information System Security Officer (ISSO): The commander shall appoint a security officer for the computer system who will be specifically responsible for ensuring continued application of the requirements set forth in DCID 1/16 (New Series), for reporting security deficiencies in system operation, and for controlling any changes in system operation as they may affect the security status of the total system. In order to perform some of the tasks associated with his position, the ISSO shall have the technical expertise of a highly skilled systems programmer. In those cases when it is impractible to assign a highly skilled systems programmer as ISSO, an individual possessing these capabilities will be made available/responsible to the ISSO for technical advise and consent.

a. Responsibilities of the ISSO should include as a minimum:

(1) Recommend system certification to the certifying authority (team).

(2) System inspection.

(3) Continuous system testing and attempted penetration.

(4) Review of all modifications to system hardware and software.

(5) Supervision of installation of changes or repair of system hardware and software.

(6) Control of authentication list.

(7) Supervision of implementation of revised authentication lists.

(8) Preparation of documentation on procedures related to the security of the system, including system messages to users.

(9) Preparation, coordination, approval and/or implementation, during system test, of the following:

(a) ISSO Guide.

(b) Initial test procedures.

(c) Security classification guide.

(d) Security control procedures.

(e) Test period operating techniques.

(f) Scheduling procedures.

(g) Installation guides.

(h) Revised Red/Black criteria for Main Computer and remote devices.

(i) Physical disconnect procedures.

(j) Approved sanitizing procedures.

(k) Statistics logging and correlation procedures.

(l) Test period programming guide.

(m) Core compartmentation procedures.

(n) Input/output processes.

(o) Operator interrupts and supervisor overrides procedures.

2. <u>Personnel Security and System Access Control Measures</u>: Access to the computer center shall be determined by the access approval level and need to know of the requesting individual. Access approval will be commensurate with the requirements as set forth in DCID 1/16 (New Series). This approval also applies to access authority to and use of remote terminals connected to the resource-sharing computer system. Administrative and procedural safeguards should be applied to provide data integrity to information and data handled by the operations center, the systems staff, and remote access users.

a. Communications links joining remote terminals and the central facility must be secured by approved methods.

b. The central computer spaces must be secure. Persons entering the area must have proper authorization and reason for being there.

c. All data delivered to and released from the central facility should be carefully logged in and signed for. Only authorized persons should be allowed to conduct these transactions.

d. Only authorized operator and systems and maintenance personnel should be allowed to operate equipment in the central computing area. These operators and programmers should be cleared for all categories of information processed by the system.

e. Only authorized personnel should be allowed access to magnetic tape, source deck libraries, data management systems, executives, operating systems and applications programs.

f. The user activity and ISSO must insure that only individuals with proper clearance and access authorization are permitted to utilize remote terminals located at their activity.

g. Hardware maintenance engineers and technicians should be granted access to all categories of information processed by the system.

3. Physical Security Protection: Physical security protection requirements shall be satisfied according to direction contained in DCID 1/16 (New Series). In all cases, access to or use of remote terminals will be determined by the security protection requirements of the information

designated for input/output at that terminal. Likewise, the central facility will possess certification for the handling of the highest classification of information designated for processing by the system. Physical security protection requirements which must be analyzed, tested and evaluated for adequacy area:

a. Personnel access control.

b. Physical disconnect procedures.

c. Emergency destruction procedures.

d. Shielding requirements, as pertains to physical security through emanations protection.

e. Security guard procedures.

f. Physical data distribution control procedures.

4. Communications Links: Communications links between all components of the system shall be secured in a manner appropriate for the transmission of the highest classified data designated to be handled by the link. The spectrum of the types of communications links can be from:

a. Store and forward switching networks using encryption devices to;

b. Direct dialing between systems with encrypted transmissions to;

c. Off-line teletype connections to;

d. Direct connection using encrypted transmission and distributed network message processing systems to;

e. Use of human interfaces at either end of an encrypted transmission to;

f. Use of special communications network for transmitting digital or analog data in a highly formatted or textual form to;

g. Use of direct data links between components of a system within a secure environment to;

h. Use of direct data links between components of a system within a multi-level security environment. All communication cables, conduits, wire-line distribution, connectors, terminals, cryptography, encryption/decryption equipment and procedures will be analyzed, tested and evaluated according to current governing directives.

5. Emanations Security Aspects: Control measures and tests will be applied to equipment and systems to the extent necessary to prevent the compromise of calssified or controlled information by the unauthorized interception of spurious emissions from equipment used to process the information. Individual USIB members will retain responsibility for applying control measures for those systems within their assigned area. Only measures essential to the prevention of compromise shall be applied. Electric phenomana cause all active electronic circuits to produce an electromagnetic field, immediately adjacent to the equipment and the surrounding space; which characterizes the

WORKPAPERS

electric current flowing in the circuit(s). In digital equipment, the signals emitted (radiated or conducted) may be considered as a series of impulses. Each impulse in the series may represent a "bit," or, if all bits in a character are generated simultaneously, a single character. A series of these impulses is often referred to as data related or, intelligence bearing signals, since they bear a relationship to the characters in process. However, these terms may be misleading because the signals emitted may be related to machine functions common to all programs in the processing cycle and not to raw or processed data with an intelligence value.

The multitude of signals that emanate from several components simultaneously may be especially difficult to detect, record and analyze. Therefore, equipment monitors must review the entire machine room, or remote-terminal area, as a highly complex source of emanations. Under these circumstances, the usefulness of any recorded emanations depends on the degree to which the measuring and recording system can identify each of the many different sources of emanations originated from within the system.

The term "Compromising Emanations" implies that the theoretical prescence of a signal alone does not suffice to classify the signal as compromising. The signal must be amenable to being: First, recorded on a suitable medium; and second, analyzed. The equipment and techniques necessary to these actions are numerous and limitations are serious due to:

a. The ADPE speed and complexity.

b. The coding methods used in the machine system.

c. The state-of-the-art limitation in broadband recording and other necessary equipments.

d. The broad frequency range over which signals occur.

e. The possible requirement for long-term, on-station monitoring without risk of detection.

Additionally environmental noise ~~noise~~ effects will ~~will~~ cause the signal-to-noise ratio (S/N) to decrease more rapidly than the measured signal amplitude, and thus reduce the emitted signal's susceptability to reliable analysis.

Many factors must be evaluated simultaneously when determining whether TEMPEST[1] control procedures should be applied to an ADP system, since no single factor will suffice to establish the installation's vulnurability or to identify the control procedures to be used. Factors known to affect vulnerability have been carefully evaluated to the extent that theoretical and limited test results allow.

1/

Page Denied

Next 2 Page(s) In Document Denied

g. Primary controls to consider are:

(1) Security Labels: Security classification and other required control labels shall be identified with the information and programs in the system to insure appropaite labeling of output/input and access authority. The use of these labels will be closely related to external labeling, internal file or record labeling and user identification/ authorization. Tapes, card decks, listings and displays shall contain proper security identification to alert the user to the security protection required for the handling of the information. Files (and/or records, when individual records or portions can be individually accessed) will contain in the identification and control labels, the appropriate security level of information contained within. Access to the file(or record) contents will be controlld through this 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.

(2) 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 systems will be required to identify themselves in some manner. The user activity must insure that only individuals with proper clearance and

access authorization x are permitted to utilize remote terminals located at their activity. Additionally, certain system xxx checks must be exercised to insure user authentication for the access of specified files or data which is available through the system. This identification is another level in the pyramidical check to insure that data security, authority and integrity are achieved and maintained. The mechanism through which this will be obtained shall consist of software and/or hardware devices, manual control procedures at terminal sites, and other appopriate measures designed to validate the identity and access authority of system users. Identification/authentication is the means by which a computer system assures that the individual at a temial is the person he represents himself to be. User authentication is usually provided on existing systems through a password. This technique can provide adequate protection for privacy purposes if:

(a) The passwords are given protection comparable to that required for the most sensitive imformation available to that user.

(b) They are changed periodically to minimize the possibility of compromise. (Comparable to changing safe conbinations).

(c) They are not user-generated (to prevent penetration by educated guessing).

More elaborate schemes such as one time passwords or challenge dependent passwords may not be necessary to achieve the objectives of privacy. However, installations handling very sensitive material should require these additional safeguards.

Numerous methodologies of user identification and 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:

- User name
- User classification and security release codes.
- Console identification.
- Console classification.
- Overlay identification.
- Program classification and security release codes.
- 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 others systems where direct interface becomes a reality.

(3) <u>Memory Protection:</u> Hardware and software control shall be exercised by the system over the addresses to which a user program has access. Within the software controls the most critical portion is the Supervisor (also called the Executive or the Monitor). The Supervisor acts as the over-all guard of the system. It is that portion of the software which internally manages job flow through the computer,

allocates system 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.

One of the highest security risks in the operation of resource-sharing computer systems occurs where users at remote terminals are permitted extensive programming capability in many languages and with any compilers. In such cases, extreme care must be exercised to insure that the user will not alter the Supervisor, thereby changing all the rules of the system operation. 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.

Coupled with the Supervisor and the hardware memory bounds below, the architecture of the computer must 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 must 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 bypassed.

The principal hardware techniques employed for segregating programs and data bases are various forms of memory bounds protection devices. These must be sufficient so that any attempt to read or write outside the area of memory assigned to a given user will be detected and prevented. It should be stressed, however, that memory bounds protection can fail. Therefore, it may be necessary to require a special program which will attempt to deliberately and frequently violate the memory bounds to verify that the protection device is, in fact, working. This is particularly important after a cold start, initial program load, or maintenance.

(4) 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. This reasoning follows the explanation in Memory Protection above. While the two modes must remain separate, both must recognize and be capable of handling the following:

- Types of I/O.
- I/O media characteristics.
- Processing interfaces between system resources.
- System resources involved.
- Data protection requirements.
- System status (on-line versus off-line).
- Ingredients of data protection/control (hardware, software, and procedures).

(5) Residue Clean Out: Another step toward security, authority, and integrity protection within resource-sharing computer systems is residue clean-out. Instructions for performing this function should be standard within the system for all user programs to execute residue clean-out under the following conditions:

- Upon job completion.
- Upon program error (without recovery)
- Upon notification by the Supervisor that an INTRUSION has been attempted.
- Upon site environment failure.
- Upon release of the allocated storage area to the Supervisor.

Upon execution of residue clean-out instructions, sample data will be printed/displayed to allow review by operator/user personnel to insure that the process has been successful. Measures shall then be implemented to insure that memory residue from terminated user programs is made inaccessible to unauthorized users.

(6) Access Control: It may be found, in a resource-sharing facility, that the number of personnel requiring special access will increase. This may be especially true in the early stages of a facilities' operation before it is certified for full multi-level security operations. Unfortunately, present technology offers no way to protect the operating system and the information contained in the system from subversion from

the central operations staff; i.e., operators, systems programmers, terminal users, etc. Therefore, administrative and procedural safeguards must be applied to protect classified information and data handled by the operations center and its attached remote terminals.

(a) The central computer spaces must be secure.

(b) The remote terminal areas shall be secured to the level of information to be processed by that station.

(c) Access shall be limited to persons possessing the authorization and requirement for entrance.

(d) Only authorized operator;and systems and maintenance personnel should be allowed to operate equipment in the central computer area. These operators and programmers must be cleared for all categories of information processed by the system.

(e) Only authorized personnel should be allowed access to magnetic tape and source deck libraries.

(f) The user activity must insure that only individuals with proper clearance and access authorization are permitted to enter the area and/or to utilize remote terminals located at this activity.

(g) Hardware maintenance engineers and technicians should be granted access to all categories of information processed by the system.

(h) The access control measures must be established, monitored and changed by the Information System Security Officer (ISSO), even though access control responsibility will rest with each individual within the resource-sharing facility.

(i) The control of access to the physical areas of the facility can take several forms, e.g. access roster, clearance badge, video monitor, security guard, etc. Whatever control method is used, it must insure absolute control of access to the resource-sharing system.

(7) Audit Trail Capability: The resource-sharing computer system shall 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 will allow for:

- Detection of data base/system misuse.
- Documentation of data base/system misuse.
- Audit of task performance.

The Audit Trail functions will be performed by the system Supervisor in connection with a special System Log and Access Authentication Library. As the Supervisor allocates portions of the system to users at terminals, it will have first verified the authority of the requestor to access the particular portion. The improper or unauthorized requests will be logged and, dependent upon the seriousness of the infraction, the system can take several actions. These actions range from job termination with accompanying audio and visual security alarms to a daily denial report for the ISSO. The system must maintain detailed data on all user actions. From this data, the actions of all users can be traced and weak areas isolated and corrected. The Audit Trail will receive data from the security verification programs which will be used to provide continuous checks on the system operation.

7. CONCLUSION: In the final analysis, the security of a resource-sharing computer system must come from an interlocking of personnel security, software techniques, communications security, and administrative procedures. Exclusive dependence on one area (for example, software) must be avoided. Sufficient experience with the day-to-day use of resource-sharing computer systems, and enough in-depth analysis is available to provide some confidence that the major problems with reference to security are known. If used properly and intelligently, and if subjected to stringent and frequent testing, resource-sharing computer systems employing today's hardware can provide acceptable protection of classified information, even multi-levels of classified information. In fact, they can probably provide greater protection than many manual methods of handling classified information. The knowledge, expertise and imagination of assigned resource-sharing computer systems managers, programmers, operators, analysts, and users will be tested and retested as systems grow in capabilities and complexity. Greater reliance on the systems and their capabilities will be required to fully exploit these capabilities and improve the

security, authority and integrity of information processed by the systems.