~~S-E-C-R-E-T~~

IBSEC-CSS-R-6
3 February 1971

UNITED STATES INTELLIGENCE BOARD

SECURITY COMMITTEE

MEMORANDUM FOR: Members of the Security Committee

SUBJECT : Guidelines for the Security Analysis, Testing, and Evaluation of Resource-Sharing Computer Systems

1. As requested at the last Security Committee meeting, all members submitted by 29 January their concurrence in or comments on the proposed "Guidelines for the Security Analysis, Testing, and Evaluation of Resource-Sharing, Computer Systems" developed by the Computer Security Subcommittee (CSS) in response to the tasking by the Board.

2. To expedite final action on the paper, all comments received were referred to the Subcommittee for collective consideration and resolution. This was accomplished at the 29 January CSS meeting and resulted in several minor changes in the earlier paper.

3. A copy of the revised guideline paper is attached for your final review and approval. If no further comment is furnished the Secretary's office [redacted] by the close of business 12 February 1971, the paper will be considered approved by the Committee and will be forwarded to the Board. STAT

[redacted] STAT

Secretary

cc: CSS Members

GROUP I
Excluded from automatic downgrading and

IBSEC-CSS-R-6
3 FEB 1971

GUIDELINES FOR THE SECURITY ANALYSIS, TESTING, AND EVALUATION OF RESOURCE-SHARING COMPUTER SYSTEMS

PURPOSE:

1. To provide basic guidelines for the security analysis, testing, and evaluation of resource-sharing computer systems wherein the protection of data stored and/or processed must be insured. To identify features, procedures, and related conditions which should be analyzed, tested, and evaluated prior to accreditation for resource-sharing system operation. While the guidelines are developed principally for resource-sharing systems, they may also be applicable to other computer systems.

GENERAL:

2. As a basis for security accreditation, resource-sharing computer systems should be analyzed, tested, and evaluated for the possession and reliability of protective features and procedures. These efforts should result in one of the following:

a. A determination and certification that system security features, procedures, and other conditions are adequate for the protection of data in the system;

b. Identification of vulnerable areas of system operations with recommendations for corrective action which can serve as a basis for further security testing and re-evaluation;

c. Recommendation against system certification due to serious system security deficiencies which are identified and explained.

3. The conditions under which the analysis, testing, and evaluation are conducted should be such that system operation is

both productive and stable. The process should be scheduled for a period in which, for example, the system is not undergoing any major software, hardware, or procedural modifications. Changes taking place in the system during the process should be separately evaluated in the light of their impact on both system security and the status of the testing process.

4. In many cases, due to operational requirements, the analysis, testing and evaluation process must be a discrete though recurring activity. On the other hand the advantages of continuous analysis and testing should be recognized, since almost any system is constantly undergoing change.

5. It is acknowledged that system configurations, capabilities, locations, and procedures vary widely among organizations which may use these guidelines. It is essential that insofar as possible the analysis and testing process be based upon these guidelines in conjunction with applicable regulatory issuances. These guidelines are meant therefore to suggest a method for matching the environment of a given system with the security requirements demanded for information it is to process and store. System security analysis is requisite to the testing process; both the analysis and testing phases provide the groundwork for system evaluation. While all three may be independent phases, they are not mutually exclusive. They all may contribute to a feedback loop serving to identify security deficiencies, initiate remedial action, and in turn permit further testing and re-evaluation.

TEST PLAN:

6. Judicious application of these guidelines in the security analysis, testing, and evaluation of a specific system dictates the need for an orderly approach to the process including the preparation of a test plan as a first step. Development of this plan for testing and evaluating a specific system should include predetermination of the criteria under which the results will be considered acceptable. In some respects these criteria will consist of the presence of required security features; in other cases, however, acceptability will be determined quantitatively in terms of the probability of failure in the system's overall security posture.

SYSTEM SECURITY ANALYSIS:

7. The security analysis of system operation consists of the following:

a. Description of the security environment in which a given system is intended to operate;

b. Identification of protective hardware, software, personnel, physical, and procedural security features.

c. Determination of the presence or absence of such features and procedures required by appropriate regulatory issuances;

d. Documentation as to how these features are applied to the hardware, software, and operating conditions of the specific system under review;

e. The ordering of these safeguards into a framework showing the manner and degree to which they are designed to guard against possible security vulnerabilities; it is desirable, although not universally practical, to attempt the application of quantitative methods including statistical probability to this phase of the process.

8. The analysis should be oriented toward determining whether system security features collectively provide the degree of protection adequate for the needs of the information being stored or processed in the system, and also meet the requirements of pertinent regulatory issuances.

SECURITY TESTING:

9. This process includes the examination and attempted subversion of all system security features and procedures, singly and in combination, to determine whether they are effective and cohesive in providing the desired data security control. The extent and duration of this phase of the process will depend on the complexity of the system involved, and the sensitivity of the data.

SECURITY EVALUATION:

10. This phase of the process is based upon the security analysis and the testing results. Where the analysis should provide concrete information as to the possession and logical capabilities of the system's protective features, the testing results will give evidence to support or deny the actual dependability of these features. This proof and evidence in the evaluation phase must be assessed in the light of system security requirements. The acceptability of the results should be determined in accordance with the criteria established in the test plan and should be based upon a demonstrated capability of the entire system, including its hardware, software, personnel, physical, and procedural security features. The evaluation should determine whether adequate protection can and will be provided in accordance with established requirements.

FEATURES TO BE ANALYZED AND TESTED:

11. Among the protective measures, features, and procedures in a computer system operation needing examination in the analysis and testing phase are the following:

a. Software/Hardware Controls:

(1) Memory Protect: A determination should be made to insure that hardware and software control is exercised by the system over the addresses to which a user program has access. Since devices and techniques used for this purpose can fail, it is advisable to determine the presence and reliability of a special program which will attempt to violate memory bounds deliberately and frequently. Testing of such protect devices and techniques should be conducted over a period of time, utilizing all available or at least representative programs to insure the positive efficiency of this feature.

(2) Separation of Data by/within Storage Medium: Semilar to memory protect, except that data separation is normally not additionally dependent upon software protection; this separability must be reviewed to determine its presence and reliability.

(3) Protection State Variables: Any one or more variables included in the execution state of a processor which determine the interpretation of instructions executed should be identified in the security analysis phase. The actual ability of the processor to access locations in memory should be tested to insure that all original and modified capabilities are known, understood, and adequately controlled.

(4) Security Labels: The presence and efficacy of security classification and other required control labels and the reliability of the software utilizing these labels should be checked in both the analysis and testing phases.

(5) User Identification/Authentication: Although user identification/authentication features will primarily apply to remote users of resource-sharing systems, all persons accessing any part of a system should be identified and controlled in some manner. If the control mechanisms are based on software and/or hardware, their adequacy must be examined and tested. If manual control procedures are used, their efficacy should be taken into consideration in the analysis phase of the overall process.

(6) System Supervisor: It is imperative to examine the functional dependability of and the security control by the system supervisor, which acts as the overall control of system operations. This portion of the software (also known as the executive or the monitor) internally manages job flow through the computer, allocates system resources to jobs and controls data

flowing to and from files and terminals. Since it represents a critical element in the security of system operation it is worthy of close scrutiny in the analysis and test phases. This scrutiny should determine that rigid controls are exercised to limit access to the supervisor to authorized personnel, especially for the purpose of changing it in any way.

(7) Privileged Instructions: The analysis and testing phases should determine that the architecture of the system provides a capability for privileged instructions and protection thereof. This capability for controlling all input/output commands, and commands to change memory boundaries and protection barriers should be verified. Moreover, it should be determined that the supervisor program alone can operate or provide access to these privileged instructions. The testing phase should attempt to ascertain any user access to such instructions. An actual test of these instructions should be performed within various software systems to verify their reliability from a security and data integrity standpoint.

(8) Separation of User/Supervisor Modes of Operation: The analysis and test process shall determine the separation of the user and supervisor modes of system operation and insure that a program operating in user mode is prevented from performing unauthorized executive functions. After analysis of system documentation, the test should be oriented toward the verification that application/user programs are incapable of any alteration to the supervisor. This test may reveal a necessity for investigation of all user programs in this regard.

(9) Residue Cleanout: The security analysis and testing phases should verify the presence of instructions for performing residue cleanout which the system should execute under the following conditions:

(a) Upon system initiation or recovery;

(b) Either upon job completion, before allocation, or after deallocation of any assigned permanent user storage area;

(c) Whenever determined necessary by the system security officer.

Further, measures should be identified and their efficiency tested to insure that residue from terminated user programs is made inaccessible to unauthorized users.

(10) Audit Trails: The presence and reliability of the system's security audit trail must be examined in the analysis and testing phases. It should be determined that this feature contains sufficient information to permit a regular security review of system activity and that the audit trail is in fact reviewed for this purpose, and not generated solely as a record of system transactions. During the testing of the audit trail software feature, special care should be used to confirm that access and security authorization violations and incidents are detected and recorded. For this purpose, special "spy" programs or routines which attempt to violate the security controls of the system may be exercised to determine the effectiveness of this feature.

b. Other Controls:

(1) Personnel Security: During the analysis, a determination should be made that all personnel having unescorted access to the system have been appropriately cleared and approved for data stored or processed by the system.

The test process should also insure that all other personnel are properly escorted and monitored during

periods of system access. Procedures should be checked especially with reference to unescorted entry to the computer center area and remote terminal locations.

(2) Physical Security: The analysis phase should include a review of the physical security considerations of the computer facility and remote terminal areas. Physical security requirements in this regard should be measured in terms of standards prescribed for safeguarding classified information stored or processed in the system; evaluation of this aspect must be accomplished with reference to applicable regulatory issuances.

In the analysis and testing phases particular attention should be paid to areas where different degrees of control and protection are required at different times. Of particular significance in this regard are cases where the security level of the computer operation changes periodically to permit broader or narrower security access to the system in different modes.

(3) Communications Links: Examination and review of the security of the communications links in the system should be made during the analysis and testing process by the appropriate authority in each agency. The purpose of this review should be to insure that all links between system components are protected in a manner appropriate for the transmission of the classified data carried by the link.

(4) Emanations Security: The adequacy of control measures necessary to prevent the compromise of classified or controlled information by the unauthorized interception of spurious emissions from the system's information processing equipment will be verified during the testing phase. Individual organizations retain the responsibility for applying control measures in this area in accordance with the national policy on compromising emanations.

(5) Procedures and Administrative Safeguards: In addition to the technical hardware/software features mentioned above and the more traditional physical and personnel security controls, as in the manual world, security efficiency of system operation depends largely on basic administrative and procedural safeguards. Such protection techniques applied to the computer environment include maintenance of access lists, review of audit trails, manual control of terminal areas, etc. In the analysis and testing phases, these safeguards need examination and evaluation in a manner similar to the more technical controls mentioned. The analysis phase may well identify flaws in such procedures requiring remedial action. Further, the reliability of such procedures should be measured in the context of whether they are both practical and realistic. For example, it should be determined that such a manual control procedure is not only an adequate countermeasure for a given vulnerability but also that it is one that will be adhered to by the people using the system.