FINAL EVALUATION REPORT OF TOP SECRET VERSION 3.0

(U.S.) Department of Defense
Washington, DC

Apr 85

U.S. DEPARTMENT OF COMMERCE
National Technical Information Service
NTIS®

FINAL EVALUATION REPORT

Of

Top Secret

Version 3.0

2 APRIL 1985

(UNCLASSIFIED)

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 Unlimited
2b DECLASSIFICATION/DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S): CSC-EPL-85/002	5 MONITORING ORGANIZATION REPORT NUMBER(S): S226,550
6a NAME OF PERFORMING ORGANIZATION: Department of Defense Computer Security Center; 6b OFFICE SYMBOL (If applicable)	7a NAME OF MONITORING ORGANIZATION
6c ADDRESS (City, State and ZIP Code): 9800 Savage Road, Ft. Meade, MD 20755-6000	7b ADDRESS (City, State and ZIP Code)
8a NAME OF FUNDING/SPONSORING ORGANIZATION; 8b OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c ADDRESS (City, State and ZIP Code)	10 SOURCE OF FUNDING NOS: PROGRAM ELEMENT NO; PROJECT NO; TASK NO; WORK UNIT NO
11 TITLE (Include Security Classification): Final Evaluation Report: TOP SECRET Version 3.0 (UNCLASSIFIED)	
12 PERSONAL AUTHOR(S): Israel, Howard; LaFountain, Steven; Hogan, Michael *; Rub, Jerzy * (* AEROSPACE Corporation)	
13a TYPE OF REPORT: Final; 13b TIME COVERED FROM _____ TO _____	14 DATE OF REPORT (Yr, Mo, Day): 85/04/02; 15 PAGE COUNT
16 SUPPLEMENTARY NOTATION	
17 COSATI CODES: FIELD; GROUP; SUB GR	18 SUBJECT TERMS (Continue on reverse if necessary and identify by block number): Trusted Computer System Evaluation Criteria, TOP SECRET Version 3.0, EPL, IBM, DoDCSC, MVS, C2

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

The Department of Defense Computer Security Center (DoDCSC) was established in January 1981 to encourage the widespread availability of trusted computer systems for use by facilities processing classified or other sensitive data.

In the second quarter of FY83, CGA Software Products Group, Inc. requested that the DoDCSC evaluate Version 3.0 of their commercially available TOP SECRET security package for the OS/VS2 MVS operating system. MVS is an IBM operating system for its 303X, 308X, 4341, 370/158 and 370/168 processors.

The security features provided by Version 3.0 of TOP SECRET were evaluated against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria dated 15 August 1983.

20 DISTRIBUTION/AVAILABILITY OF ABSTRACT: UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☒ DTIC USERS ☐	21 ABSTRACT SECURITY CLASSIFICATION: UNCLASSIFIED
22a NAME OF RESPONSIBLE INDIVIDUAL	22b TELEPHONE NUMBER (Include Area Code); 22c OFFICE SYMBOL

DD FORM 1473, 83 APR — EDITION OF 1 JAN 73 IS OBSOLETE.

SECURITY CLASSIFICATION OF THIS PAGE

CSC-EPL-85/002
Library No. S225,550

FOREWORD

This publication, TOP SECRET Release 3.0 Final Evaluation Report, is being issued by the Department of Defense Computer Security Center under the authority and in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of this report is to document the results of the formal evaluation of CGA's TOP SECRET security package. The requirements stated in this report are taken from the Department of Defense Trusted Computer System Evaluation Criteria dated 15 August 1983.

Approved:

Robert L. Brotzman
Director
DoD Computer Security Center

2 April 1985

TABLE OF CONTENTS

EVALUATION TEAM MEMBERS

Howard M. Israel
Steven M. LaFountain
DoD Computer Security Center
9800 Savage Road
Ft. Meade, MD 20755-6000

Michael O. Hogan
Jerzy W. Rub
The Aerospace Corporation
Mail Station M1/106
P.O. Box 92957
Los Angeles, CA 90009

EXECUTIVE SUMMARY

In April of 1983, CGA Software Products Group, Inc. requested that the Department of Defense Computer Security Center (DoDCSC) evaluate Version 3.0 of TOP SECRET, their commercially available add-on security package for the OS/VS2 Multiple Virtual Storage (MVS) operating system. MVS is an IBM operating system for the 303x, 308x, 4341, 370/158, and 370/168 machines.

The security protection provided by Version 3.0 Level 163 of the TOP SECRET add-on security package with Feature Option #43 in use was evaluated against the requirements specified by the Department of Defense Trusted Computer System Evaluation Criteria (the Criteria) dated 15 August 1983.

The DoDCSC evaluation team determined that the highest class at which TOP SECRET running with the MVS system satisfies all the requirements of the Criteria is class C2. Therefore, the DoDCSC has assigned TOP SECRET/MVS a C2 rating. This rating, however, is contingent upon the system being configured as detailed in this report (e.g., the PASSWORD(NOPW) attribute, which allows users to submit batch jobs without a password on a job card, is not allowed, etc.).

A class C2 system enforces discretionary access control by making users individually accountable for their actions through login procedures, auditing of security-relevant events, and resource isolation.

A system that has been rated as being a C division system contains the features and assurances described in the Criteria. There is no assurance that a C division system is free of flaws that would allow the subversion or bypassing of the advertised security mechanisms through sophisticated penetration methods.

The integrity of the TOP SECRET package is dependent upon the integrity of the MVS system itself and the hardware upon which it is running.

SECTION 1

INTRODUCTION

1.1 BACKGROUND OF THE EVALUATION PROCESS

The Department of Defense (DoD) Computer Security Center was established in January of 1981 to encourage the widespread availability of trusted computer systems for use by facilities processing classified or other sensitive information. In order to assist in assessing the degree of trust one could place in a given computer system, the Department of Defense Trusted Computer System Evaluation Criteria were developed. The Criteria establish specific requirements that a computer system must meet in order to achieve a predefined level of trustworthiness. To determine at which level in the Criteria a system should be placed, the system must be evaluated against the Criteria by an evaluation team. The criteria are arranged heirarchically into four major divisions of protection, each with certain security relevant characteristics. These divisions are in turn subdivided into various classes.

The DoDCSC performs two types of commercial product evaluations: formal evaluations and developmental evaluations. A formal evaluation is assumed to be the evaluation of a system that is not to undergo any additional changes. The first step in a formal evaluation is the preliminary assessment. During this step the DoDCSC's evaluation team familiarizes themselves with the strengths, capabilities and weaknesses of the system and prepares a preliminary assessment report determining at what class the system should be considered to be a candidate for and emphasizing aspects of the system that need to be improved in order to achieve a higher rating. Because it is likely to reflect proprietary information, distribution of the preliminary assessment may be restricted to the vendor and the DoDCSC at the vendor's request. Also, a preliminary assessment does not require any "hands-on" exposure to the system.

The second step in a formal evaluation requires "hands-on" testing (e.g., functional and, if necessary, penetration testing). Once a vendor has agreed to submit a system to this step, the vendor may not withdraw the system from the evaluation. The formal evaluation report prepared at the end of this step represents the results of a formal evaluation. It defines, in detail, the scope of the evaluation and binds the rating to the product to which it applies. It completely identifies and describes the product that was evaluated and documents the

security mechanisms upon which the final rating is based. The report details how each of the security mechanisms rates against the requirements of the Criteria, the evaluation process employed, the evidence examined and the testing methodology used.

The second type of evaluation, the developmental evaluation, is based on a manufacturer's design for either security enhancements to an existing system or for a new trusted product. Included in a developmental evaluation is an in-depth examination of design plans. As with the preliminary assessment, no "hands-on" testing is required for a developmental evaluation and because the report produced during a developmental evaluation is likely to reflect proprietary information, the developmental report may be restricted to the vendor and the DoDCSC at the vendor's request.

1.2 OVERVIEW OF TOP SECRET

TOP SECRET has four modes of operation: DORMant, WARN, IMPLement, and FAIL. These modes allow for the gradual implementation of the security provided by TOP SECRET. In DORM mode, no security validation is performed except for the control of administrators. In WARN mode, users are warned of security violations, but no action is taken by the system on these violations. In IMPL mode, unauthorized access attempts involving users and objects defined to TOP SECRET are failed, but users and objects not defined to TOP SECRET continue to operate unaffected. In FAIL mode, unauthorized access attempts to all facilities and resources are failed. The requirements of the Criteria are not met when TOP SECRET operates in DORM or WARN mode. In IMPL mode, defined users and objects are protected. In FAIL mode, all users and objects must be defined. Therefore, the evaluation requires that TOP SECRET be tested in either IMPL or FAIL mode.

TOP SECRET recognizes three logical components: users, resources, and facilities. Users are identified to TOP SECRET by a unique ACcessor IDentifier (ACID), which is associated with a security record in the master security file. The master security file contains information used by TOP SECRET to determine what facilities and resources a particular user can access and the manner in which access will be granted. TOP SECRET recognizes seven types of ACIDs which fall naturally into four groups: administrator (control) ACIDs, DEPT and DIV ACIDs, PROFILE ACIDs, and USER ACIDs. The Central Security Administrator (SCA) has control over the entire system. A Divisional Security Administrator (VCA) has control over those ACIDs and resources that are owned by his division. A Departmental Security

Administrator (DCA) has control over only those ACIDs and resources that belong to his department. Although administrators control the environment, in terms of actual system access, they are treated as normal users.

Department (DEPT) and division (DIV) ACIDs provide a structure for dividing and delegating administrative control over users and objects. USER and PROFILE ACIDs must belong to departments. Departments may belong to divisions or may stand alone. Objects (resources) can be owned by any ACID (i.e., users, profiles, administrators, departments and divisions). However, resources may be accessed only by USER, CONTROL, and PROFILE ACID authorizations; department and division ACIDs cannot access objects.

A PROFILE ACID provides access to a set of objects for a group of users that need to access those objects in the same manner. PROFILEs eliminate the need to define access individually for every user. When a PROFILE ACID is added to a user's ACID, he inherits all of the access permissions granted to that PROFILE. Two types of PROFILE ACIDs can be defined and shared: department profiles, which can only be used to grant access between users and objects within the scope of a single department, and globally administrable profiles (GAPs), which can be used to grant access to users outside the scope of the administrator who owns the PROFILE. However, an unprivileged user cannot create his own profile or authorize access to a profile. This must be done by one of the security administrators (SCA, VCA, DCA) whose scope of authority encompasses the PROFILE.

Resources refer to named objects as defined in the Criteria. TOP SECRET provides protection for objects such as Direct Access Storage Device (DASD) data sets, DASD and tape volumes, programs, Time Sharing Option (TSO) commands, on-line terminals, remote terminals, Job Entry Subsystem (JES) readers, IMS applications, user resources, ROSCOE monitors, IMS and CICS transactions, CICS resources, database fields, the system facilities and individual CPUs in a multi-CPU environment.

Facilities are any MVS subsystem that processes work on behalf of users or jobs, (e.g., TSO, Batch, IMS, CICS, and ROSCOE). TOP SECRET automatically supports any vendor facility that recognizes and is supported by the Standard MVS Security Interface (SU-32, incorporated into the MVS Operating System at level 3.8) or the MVS Security Access Facility (SAF) supplied with MVS/SP 1.1 and MVS/XA 1.2 and above. TOP SECRET protects access to facilities by requiring users to identify themselves with a known ACID and valid password. Thus, for purposes of the evaluation, facilities can be treated as being protected by the Trusted Computing Base (TCB).

TOP SECRET allows four scopes of protection: global (all users), facility (all users within a facility), group (all users associated with a given profile) and user (one specific user). These scopes are hierarchical in precedence with access permissions granted to a specific USER overriding those granted to a PROFILE attached to that user, which overrides those granted to all users of a particular facility, which in turn overrides those granted to ALL users.

In order to provide DASD data set security, data sets must be "secured", (i.e. have a certain bit set in the Data Control Block (DCB), the RACF bit). This causes OS/MVS to automatically issue a system call (SU-32) through the MVS Security Interface to TOP SECRET whenever a data set is accessed in any way. All data sets created while TOP SECRET is in WARN, IMPL or FAIL mode are automatically "secured" upon creation. Datasets that are created before TOP SECRET is installed or when TOP SECRET is in DORM mode require that a utility program TSSPROT (supplied with TOP SECRET) be run to set the RACF bit. Alternatively, the MVS operating system can be instructed to always call the MVS Security Interface (MVS ALWAYS CALL option) regardless whether or not the RACF bit is set. As a minor note, because TOP SECRET utilizes the RACF bit, system messages may be generated that refer to RACF when, in fact, TOP SECRET is running.

1.3 TEST CONFIGURATION

The systems used for the functional testing during the TOP SECRET evaluation consisted of an IBM 3033 and an IBM 4381 running MVS Release 1.3 Level 8310 (and all its supporting subsystems and utilities) both with DASD and tape external storage.

User access was tested only via online terminals and user console. Access via card readers or remote job entry stations must be physically protected from unauthorized access. TOP SECRET should not be used to authenticate a batch user s identity via passwords when jobs are sumitted via card readers.

1.4 DOCUMENT ORGANIZATION

The balance of this paper consists of six sections. Section 2 presents the class C2 requirements from the Criteria and describes the security features of TOP SECRET that satisfy those requirements. Class C2 is the highest class at which TOP SECRET satisfies all the requirements for any class. Section 3 presents a brief summary of why TOP SECRET, as delivered by CGA, can not receive a rating higher than class C2. Section 4 describes how

the security mechanisms of TOP SECRET satisfy requirements above the class C2 level. Section 5 details security-relevant aspects of the TOP SECRET package that are not addressed by the Criteria and the evaluation team's inputs about those aspects. Section 6 presents a brief conclusion of the evaluation results. Appendix A contains a brief summary of the testing done for this evaluation.

SECTION 2

TOP SECRET vs. CLASS C2 REQUIREMENTS

THIS SECTION ADDRESSES THE REQUIREMENTS FOR CLASS C2, THE HIGHEST CLASS FOR WHICH TOP SECRET SATISFIES ALL REQUIREMENTS OF THE CRITERIA.

2.1 DISCRETIONARY ACCESS CONTROL

Requirement:

The Trusted Computing Base (TCB) shall define and control access between named users and named objects (e.g., files and programs) in the ADP system. The enforcement mechanism (e.g., self/group/public controls, access control lists) shall allow users to specify and control sharing of those objects by named individuals or defined groups of individuals or by both. The discretionary access control mechanism shall, either by explicit user action or by default, provide that objects are protected from unauthorized access. These access controls shall be capable of including or excluding access to the granularity of a single user. Access permission to an object by users not already possessing access permission shall only be assigned by authorized users.

Applicable Features:

In FAIL mode, facility access to TSO is limited to only named users, (i.e. users defined to TOP SECRET). Thus, only named users have access to the TCB. In IMPL mode, access to named objects by named users is controlled, but users not defined to TOP SECRET also have system access and may access all data sets that are not "secured" or to which access has been permitted for ALL (users).

Certain objects (data sets, volumes, applications, programs, and terminals) can be defined to TOP SECRET in two ways: by giving the explicit name of the object or by giving a generic prefix. Access to entire groups of objects can be controlled by using generic prefixes and data set masks.

Most objects must be "owned" before access to them can be authorized. This is done when the object is defined to TOP SECRET. In both IMPL and FAIL mode, all objects are protected by default and are therefore inaccessible to all users, except the owner, without specific authorization to the object.

By default, all online users "own" data sets that have the same prefix as their ACIDs and, therefore, have unlimited access to those data sets. On the other hand, ownership of an object by a department or division ACID does not imply automatic access of that resource by users in that department or division (the users are not the object owners). An explicit authorization must be performed to allow users to access objects owned by their department or division ACIDs.

TOP SECRET controls sharing of resources by individual users via their unique USER ACID or by groups of users through profiles.

Access to groups of individual users is granted by giving the desired access to a PROFILE ACID and then adding that PROFILE ACID to the individual USER ACIDs who are to compose the group. The different types of access permissions that can be granted are READ, WRITE, UPDATE, CONTROL, CREATE, SCRATCH, FETCH, ALL, and/or NONE.

2.2 OBJECT REUSE

Requirement:

When a storage object is initially assigned, allocated, or reallocated to a subject from the TCB's pool of unused storage objects, the TCB shall assure that the object contains no information for which the subject is not authorized.

Satisfied By:

When pages of main memory are allocated to a user, they are automatically cleared by the MVS system before being released to the requesting user.

TOP SECRET ensures that storage areas on secondary storage devices are erased automatically through the following methods:

- Virtual Storage Access Method (VSAM) data sets are erased by TOP SECRET forcing the ERASE option on during normal VSAM delete processing

- non-VSAM data sets are overwritten by TOP SECRET with binary zeros before TOP SECRET allows that data set to be deleted

These methods ensure that all storage, both primary and secondary, are cleared before they can be obtained by any user.

2.3 IDENTIFICATION AND AUTHENTICATION

Requirement:

The Trusted Computing Base (TCB) shall require users to identify themselves to it before beginning to perform any other actions that the TCB is expected to mediate. Furthermore, the TCB shall use a protected mechanism (e.g., passwords) to authenticate the user's identity. The TCB shall protect authentication data so that it cannot be accessed by any unauthorized user. The TCB shall be able to enforce individual accountability by providing the capability to uniquely identify each individual ADP system user. The TCB shall also provide the capability of associating this identity with all auditable actions taken by that individual.

Applicable Features:

With TOP SECRET, users are identified by their unique ACcessor IDentifier (ACID). In order to use a particular CPU in a multi-CPU system or access a system facility (such as TSO, BATCH, IMS, CICS, etc), the user or his job must supply a known ACID. In FAIL mode, all users of the system must be identified to TOP SECRET with a known ACID in order to access any facility. In IMPL mode, only defined users are required to be identified to TOP SECRET in order to access a facility; other users, that the TCB is not expected to control, are not required to be identified to TOP SECRET.

TOP SECRET provides for authentication of user ACIDs through the use of passwords. This authentication is performed by TOP SECRET at the time of logon/sign on/job initiation, (i.e., whenever a USER ACID requests access to a facility).

User and administrator ACIDs (as well as DEPT, DIV, and PROFILE ACIDs) are defined to TOP SECRET through the use of the TSS CREATE subcommand. User passwords are initially defined by an administrator but users can change their own passwords. The master security administrator may set certain control options that require passwords to comply with installation-defined syntax rules which define the alphanumeric structure with which all passwords must comply. Administrators may also set password expiration requirements on users under their control.

Passwords are first encrypted and then stored in the master security file. This file is stored in fetch-protected key 3 storage.

TOP SECRET also has the ability to limit user access to only

certain facilities on only certain days of the week and/or times of the day and/or to access online facilities only through certain terminals.

Batch jobs may be submitted through online methods or from physical readers such as local JES readers or remote job entry stations. All batch jobs must be identified with an ACID and password. Batch jobs that are submitted through online methods are fully secured, since the on-line user must have already supplied a correct password to gain access to the system. TOP SECRET derives the job ACID from either the jobname or userid parameters on the JOB card. The derived ACID is verified for authorization and inserted as USER=acid on each job card. TOP SECRET automatically inserts the ACID's password. This eliminates the potential exposure of having the password displayed on a terminal screen in a batch file.

NOTE: For online submission, a defined user is allowed, by default, to submit only those jobs which are identified by his ACID. However, TOP SECRET provides a mechanism that an administrator can explicitly authorize a user to submit jobs with other ACIDs (via the TSS PERMIT() ACIDS() function). It is also possible to allow production job scheduling systems to submit jobs under any ACID by bypassing online job submission validation (by adding the NOSUBCK attribute to the production job ACID), (i.e., the job will be submitted without checking that the production job ACID has been authorized to submit this job using this ACID).

Since both of these features allow a user to present himself to the TCB as another user, the requirements of the Criteria are not met when either of these features are used.

Jobs that are physically submitted from local card readers or remote job entry stations also require ACIDs and passwords. TOP SECRET provides a variety of ways (via the JOBACID control option) that the ACID can be automatically derived from various parameters on the JOB card or the ACID can be specified via the USER parameter of the JOB card. In either case, a password must be supplied via the PASSWORD keyword on the JOB card.

As hard coding of passwords on JOB cards is not recommended, other means could be used to secure jobs submitted from physical readers. For example, the PASSWORD(NOPW) attribute could be given to the ACID and instead the source of entry for the ACID can be limited to one or more specific JES readers (via the SOURCE attribute). Conversly, the reader can be protected so that only those jobs whose ACIDs are authorized to submit a job from the device will be eligible for execution. However, both of these methods depend upon physical procedures and do not meet the

requirement of the Criteria, which requires that the security mechanisms be under the control of the TCB. Also, both of these methods effectively allow the bypassing of the authentication mechanism and would invalidate the system's C2 rating if used. Therefore, it is recommended that batch jobs, other than those submitted via on-line users, not be allowed.

2.4 AUDIT

Requirement:

The TCB shall be able to create, maintain, and protect from modification or unauthorized access or destruction an audit trail of accesses to the objects it protects. The audit data shall be protected by the TCB so that read access to it is limited to those who are authorized for audit data. The TCB shall be able to record the following types of events: use of identifiaction and authentication mechanisms, introduction of objects into a user's address space (e.g., file open, program initiation), deletion of objects, and actions taken by computer operators and system administrators and/or system security officers. For each recorded event, the audit record shall identify: date and time of the event, user, type of event, and success or failure of the event. For identification/authentication events the origin of request (e.g., terminal ID) shall be included in the audit record. For events that introduce an object into a user's address space and for object deletion events the audit record shall include the name of the object. The ADP system administrator shall be able to selectively audit the actions of any one or more users based on individual identity.

Applicable Features:

By default, TOP SECRET records violations or unauthorized attempts to gain access to the system or to acess a resource. TOP SECRET writes these records to the System Management Facility (SMF) data sets and/or to an optional Audit/Tracking File. An installation can set a resource violation threshold at which various actions can automatically take place against users that accumulate too many violations per session.

In addition, selected resources and users can have their activities recorded. Such activities include: accesses, job initiations and terminations and invalid access attempts. Auditing can be performed and reports generated for departments, jobs, ACIDs, CPUs, facilities, files, volumes and many other selection criteria. Reports generated include date, time, CPU, ACID, jobname, facility, violation count, program, requested and granted access, return and error codes, security driver requesting security validation, resource, and terminal.

Administrators are allowed to audit only the events associated with users (ACIDs) within their scope (department or division). An auditor (administrator with audit authority) can request a report detailing all types of events and/or actions taken by all users.

2.5 SYSTEM ARCHITECTURE

Requirement:

The Trusted Computing Base (TCB) shall maintain a domain for its own execution that protects it from external interference or tampering (e.g., by modification of its code or data structures). Resources controlled by the TCB may be a defined subset of the subjects and objects in the ADP system. The TCB shall isolate the resources to be protected so that they are subject to the access control and auditing requirements.

Applicable Features:

TOP SECRET can and MUST be used to protect all of its own data sets, functions, routines, etc. Within the TOP SECRET/MVS environment there exists an identifiable Trusted Computing Base consisting of TOP SECRET, MVS, Job Entry Subsystem (JES2 or JES3), the system facilities (e.g., TSO, IMS, CICS, or BATCH) and the necessary system utilities and access methods.

The TOP SECRET package provides default, discretionary protection for all objects under its control. This protection is implemented through the use of access control lists. Access control lists are associated with every protected resource in the system. These access control lists are checked upon every attempted access by a user to a protected resource.

In addition to TOP SECRET, the following are MVS/SP protection mechanisms. MVS implements two techniques to preserve the integrity of each user's work. The first is a private address space for each user and the second is the use of multiple storage protect keys.

In MVS, a virtual storage address space consists of a system area, a common area, and a private area. MVS assigns a separate address space to each user to prevent users from accessing each others' address space. MVS uses multiple storage protect keys to protect the system and subsystems from unauthorized users. Before MVS performs services on the behalf of a user, it takes steps to prevent possible security violations (e.g., the use of invalid control blocks or the execution of unauthorized code) and to

avoid user-induced system failures due to improperly specified requests.

Under MVS, the information in real storage is protected from unauthorized use by means of multiple storage protect keys. A non-addressable protect key consists of a control field in storage and is associated with each 2K block of real storage (a 4K block is used in 308X processors). The key in storage contains the protect key of the owner and a fetch protect bit (as well as the reference and change bits maintained by the hardware and used by the software to make paging decisions).

The protect key protects the associated block of storage from unauthorized modification, while the fetch protect bit protects the block from an unauthorized attempt to read or fetch its contents. When a request is made to modify the contents of a real storage location, the key in storage is compared to the storage protection key associated with the request. If the keys match, the request is satisfied; if not, the system rejects the request and issues a program exception interrupt. When a request is made to access (read or fetch) the contents of a real storage location, the request is satisfied unless the block of storage is fetch protected. If the real storage location is fetch protected, the key in storage is compared to the key associated with the request and the resulting action is dependent upon whether or not the keys match.

Other security-relevant mechanisms included in MVS are:

1. Password protection of data sets. If a user desires an extra degree of protection, he can password protect his data. Different passwords can be used to allow different types of access (i.e., one password for read access, a separate password for write access, etc.).

2. The Authorized Program Facility (APF) provides the ability to limit the use of sensitive system services and resources to authorized users. The APF checks to see if the requesting process resides in an authorized library. If it does, the request is allowed, if not, the request is denied.

3. MVS provides for the erasure of main memory before it is released to any user or user process. This prevents the scavenging of residue from main storage.

4. The Job Entry Subsystem (JES2 or JES3) has, as one of its functions, the responsibility to recover from a

process error without lowering the integrity of the data that was in use at the time.

5. System Utilities provided by MVS are designed to assist in organizing and maintaining data within the system. There are three classes of utility programs. System utilities, data set utilities and independent utilities. System utilities are used for maintaining and manipulating system and user data sets. System utilities must reside in authorized libraries and are controlled by JCL and utility control statements. Also, they can only be executed by authorized programs.

Data set utilities are intended to be used for changing and/or comparing data at the data set or record level. They are controlled by JCL and utility control statements but can be called by any program.

Independent utilities are used to prepare devices for system use when the operating system is not available. They operate outside of the operating system, are controlled by utility control statements and can not be called by a program (they must be run independently).

2.6 SYSTEM INTEGRITY

Requirement:

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

Applicable Features:

The IBM supplied On-Line Test Executive Program (OLTEP) can be used to verify the correct operation of the system hardware.

In addition, MVS maintains the SYS1.LOGREC data set for the purpose of error recording. This data set is non-sharable and provides a record of all detected hardware failures and selected software errors and system conditions. Information about each incident is written into SYS1.LOGREC by the system recording routines and can be retrieved by using the environmental recording, editing and printing service aid (IFCEREP1). The IFCEREP1 output can be used for diagnostic and/or measurement purposes to maintain the devices and to support the system

control program.

The IFCDIP00 service aid initializes SYS1.LOGREC during system initialization. IFCDIP00 creates a header record and a time stamp record for the SYS1.LOGREC data set and allocates space for the data set which must reside on the system residence volume.

A record is made on SYS1.LOGREC for every detected hardware or software failure and system condition that has an associated recording request or recording routine. The records contain different types of data that document failures and system conditions. The records are stored in chronological order on SYS1.LOGREC. In general, each record contains:

- Relevant system information at the time of the failure.
- Device hardware status at the time of the failure.
- Results of any device/control unit recovery attempt.
- Results of any software system recovery attempt.
- Statistical data.

There are various types of records, containing device- or incident-dependent information that can be recorded on SYS1.LOGREC, which contain complete and specific information for the device, and type of failure or system condition that caused it to be written.

Recording Machine Check records are recorded on SYS1.LOGREC whenever the following detected machine failures occur:

- Central Processing Unit (CPU) processor
- Storage
- Storage Key
- Timer

When a machine failure occurs, the Machine Check Handler (MCH) receives control via a machine-check interrupt for a soft failure (one that was corrected by the hardware retry features) or for a hard failure (one that could not be corrected by the retry features).

If the machine check interrupt is for a soft failure, MCH

uses the environmental and model independent information describing the failure to build an MCH record. After formatting the information, MCH passes control to the Recovery Termination Manager (RTM). RTM then invokes the recording request routine which queues the MCH record on the asynchronous output queue and posts the asynchronous recording task. The recording task scans the output queue and issues an appropriate SVC to write any records on this queue to SYS1.LOGREC.

If the machine check interrupt is for a hard failure, MCH analyzes the information in the model independent logout area, isolates the error, and provides a record of the analysis to RTM. RTM then takes the same actions as it does for a soft failure.

With each Initial Program Load (IPL) the system begins a sequential count of errors. The sequence number is therefore unique for each detected software error or machine failure. The sequence number remains constant for subsequent software records associated with the same error (although the time stamp may change). Software records are recorded on SYS1.LOGREC for hardware detected hardware errors, hardware detected software errors, operator detected errors and software detected software errors. For error recording purposes, error data is collected in the System Diagnostic Work Area (SDWA) to assist in identifying the System Control Program (SCP) error and then invoke the RTM.

2.7 Security Testing

Requirement:

The security mechanisms of the ADP system shall be tested and found to work as claimed in the system documentation. Testing shall be done to assure that there are no obvious ways for an unauthorized user to bypass or otherwise defeat the security protection mechanisms of the Trusted Computing Base. Testing shall also include a search for obvious flaws that would allow violation of resource isolation, or that would permit unauthorized access to the audit or authentication data.

Applicable Features:

The evaluation team performed functional testing of the security features of the TOP SECRET/MVS system. The security features were found to work as claimed in the system documentation. No obvious ways to bypass the security features of the system were discovered and no obvious flaws were found during testing or documentation review.

2.8 DOCUMENTATION

2.8.1 Security Features User's Guide

Requirement:

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

Applicable Documents:

The User's Guide (US-03) and TSS Reference Manual (TS-03) supplied as part of the TOP SECRET documentation satisfy this requirement.

2.8.2 Trusted Facility Manual

Requirement:

A manual addressed to the ADP system administrator shall present cautions about functions and privileges that should be controlled when running a secure facility. The procedures for examining and maintaining the audit files as well as the detailed audit record structure for each type of audit event shall be given.

Applicable Documents:

The Security Administration (SA-03), Installation (IN-03) and Customization (CU-03) Guides provide the necessary information to satisfy this requirement.

2.8.3 Test Documentation

Requirement:

The system developer shall provide to the evaluators a document that describes the test plan and results of the security mechanisms' functional testing.

Applicable Documents:

Internal CGA documentation satisfies this requirement.

2.8.4 Design Documentation

Requirement:

Documentation shall be available that provides a description of the manufacturer's philosophy of protection and an explanation of how this philosophy is translated into the Trusted Computing Base. If the TCB is composed of distinct modules, the interfaces between these modules shall be described.

Applicable Documents:

The Implementation (IM-03) and Installation (IN-03) Guides, along with the Concepts and Facilities Manual (CF-03), provide the necessary information for this requirement.

SECTION 3

DEFICIENCIES AGAINST CLASS B1 REQUIREMENTS

THIS SECTION DESCRIBES WHY THE TOP SECRET PACKAGE DID NOT RECEIVE A HIGHER RATING BY DETAILING HOW SOME OF THE REQUIREMENT(S) OF CLASS B1 WERE NOT SATISFIED.

The major thrust of class B1 of the Criteria are the requirements that the TCB label all subjects and objects under its control with security levels consisting of hierarchical levels (e.g., SECRET, TOP SECRET, etc.) and non-hierarchical catagories (e.g., NATO, NUCLEAR, etc.). These labels are required to support a mandatory access control mechanism by which access of subjects to objects can be controlled based upon their assigned security levels.

Other mechanisms required by the Criteria at class B1 also depend upon these labels in order to provide the necessary functionality needed to satisfy those requirements. These include the identification and authentication and audit mechanisms.

TOP SECRET possesses no mechanism that supplies labels for resources. Therefore, TOP SECRET can not satisfy the labelling requirements introduced in Division B of the Criteria or any other requirements that depend upon labels. These requirements comprise the majority of the requirements at the B1 level.

SECTION 4

TOP SECRET VS. REQUIREMENTS ABOVE CLASS C2

THIS SECTION DESCRIBES HOW THE TOP SECRET/MVS SYSTEM SATISFIES SOME REQUIREMENTS ABOVE THE CLASS C2 LEVEL

4.1 DISCRETIONARY ACCESS CONTROL B3 (1)

Requirement: (Additional for class B3)

"... The enforcement mechanism (e.g., access control lists) shall allow users to specify and control sharing of those objects. ... These access controls shall be capable of specifying, for each named object, a list of named individuals and a list of groups of named individuals with their respective modes of access to that object. Furthermore, for each such named object, it shall be possible to specify a list of named individuals and a list of groups of named individuals for which no access to the object is to be given."

Applicable Features:

TOP SECRET uses access control lists for enforcing discretionary access control. These access control lists provide the capability of including and excluding access down to the granularity of a single user by allowing either the explicit granting of some type of access or by the granting of null access.

---

1. Although TOP SECRET satisfies this feature at the B3 level, TOP SECRET does not satisfy any of the assurance requirements above the class C2 level.

SECTION 5

EVALUATORS' COMMENTS

The TOP SECRET package possesses extensive audit capabilities and provides report utilities for the generation of audit reports. Reports can be obtained using various selection criteria, including: attempted unauthorized accesses, successful authorized accesses, job initiations and terminations, changes in the TOP SECRET security file, and many others. These audit features can be very useful to system administrators in determining how to delegate authority and privilege throughout the system.

Although the system documentation provided with TOP SECRET contains all the neccessary information to satisfy the Criteria requirements, the evaluation team feels that some the documentation is sometimes vague and thus misleading. The team recommends that system administrators review the documentation carefully. CGA, however, is currently in the process of re-writing the documentation for TOP SECRET.

For the maximum security possible, TOP SECRET should be run in FAIL mode. This will assure that all users of the system are defined to and controlled by TOP SECRET. Users should be given the minimal amount of authority that allows them to efficiently and effectively use the system. Administrative authorities (e.g., to list security-relevant data, perform auditing, permit access, etc.) granted by the SCA to lower level administrators should be the minimum necessary. All users should be especially careful when granting ALL access. TOP SECRET treats the ALL keyword in a special way that is not the same as listing all the options or user ACIDs for a given command. Regular password change should be enforced and the audit mechanisms provided should be used to their maximum reasonable extent. Finally, the report utilities should be run regularly to aid the system administrator in detecting abnormal system usage.

SECTION 6

CONCLUSIONS

The Department of Defense Computer Security Center's evaluation team has determined that the highest class at which Version 3.0 Level 163 of the TOP SECRET add-on security package running with the MVS operating system satisfies all of the requirements of the Criteria is class C2. However, the reader of this report should note that in order to meet all of the class C2 requirements some features of TOP SECRET can not be used and Feature Option #43, which provides the necessary functionality to satisfy the Object Reuse requirement, must be used. Therefore, TOP SECRET/MVS, configured only as detailed in this report, has been assigned a class C2 rating.

As delivered by CGA, TOP SECRET does not recognize security classification markings and can not be used to enforce mandatory access controls. Therefore, TOP SECRET can not satisfy the requirements of class B1.

TOP SECRET provides strong discretionary security controls and extensive auditing features and significantly improves the security of the MVS operating system.

GLOSSARY

ACID	- ACcessor IDentifier, 2
APF	- Authorized Program Facility, 12
CICS	- Customer Information Control System, 3
the Criteria	- Department of Defense Trusted Computer System Evaluation Criteria, iv
DASD	- Direct Access Storage Device, 3
DCA	- Departmental Security Administrator, 3
DCB	- Data Control Block, 4
DoD	- Department of Defense, iv
DoDCSC	- Department of Defense Computer Security Center, iv
GAP	- Globally Administrable Profile, 3
IMS	- Information Management System, 3
IPL	- Initial Program Load, 15
JES	- Job Entry Subsystem, 3
MCH	- Machine Check Handler, 14
MVS/SP (MVS)	- Multiple Virtual Storage/System Product, iv
OLTEP	- On-Line Test Executive Program, 13
RTM	- Recovery Termination Manager, 15
SCA	- Central Security Administartor, 2
SCP	- System Control Program, 15
SDWA	- System Diagnostic Work Area, 15
SMF	- System Management Facility, 10

TCB - Trusted Computing Base, 3

TSO - Time Sharing Option, 3

VCA - Divisional Security Administrator, 2

VSAM - Virtual Storage Access Method, 7

REFERENCES

1. Department of Defense Trusted Computer System Evaluation Criteria, Ft. Meade, MD: DoD Computer Security Center, 15 August 1983.

2. Gwatking, J.C., Automatic Erasure of Released Disk Space on an IBM 370 Computer Using the MVS Operating System, NTIS #AD-A091957, Department of Defence, Defence Research Centre, Salisbury, South Australia, June 1980.

3. Final Evaluation Report, Resource Access Control Facility (RACF) Version 1 Release 5, Ft. Meade, MD: DoD Computer Security Center, July 1984.

4. Final Evaluation Report, The Access Control Facility 2 (ACF2) Release 3.1.3, Ft. Meade, MD: DoD Computer Security Center, August, 1984.

TOP SECRET Publications:

5. Auditor's Guide, Document No. AG-03.

6. Concepts and Facilities Manual, Document No. CF-03.

7. Customization Guide, Document No. CU-03.

8. Implementation Guide, Document No. IM-03.

9. Installation Guide, Document No. IN-03.

10. Messages and Codes, Document No. MC-03.

11. Operator's Guide, Document No. OP-03.

12. Report and Tracking Guide, Document No. RT-03.

13. Security Administration Guide, Document No. SA-03.

14. TSS Reference Manual, Document No. TS-03.

15. User's Guide, Document No. US-03.

16. Utilities Guide, Document No. UT-03.

MVS Publications:

17. OS/VS2 JCL, GC28-0692.

18. OS/VS2 System Programming Library: Supervisor, GC28-0146-0.

19. OS/VS2 Supervisor Services and Macro Instructions, GC28-0683.

20. OS/VS2 System Programming Library: Job Management, GC28-0627.

21. OS/VS2 System Programming Library: System Management Facilities (SMF), GC28-1030.

22. OS/VS2 System Programming Library: Initialization and Tuning Guide, GC28-1029.

23. OS/VS2 System Programming Library: TSO, GC28-0629.

24. OS/VS2 TSO Command Language Reference, GC28-0646-4.

25. OS/VS2 TSO Terminal User's Guide, GC28-0645.

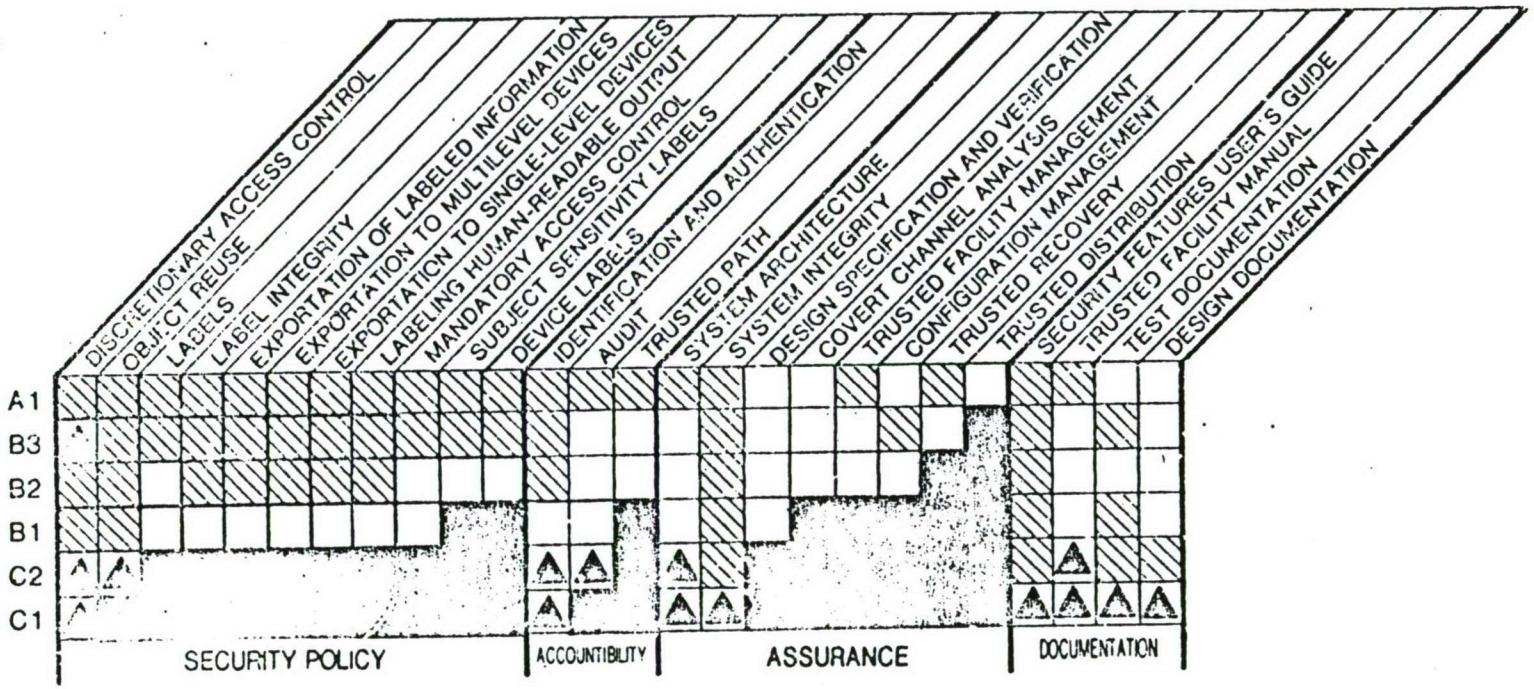
26. Operator's Library: OS/VS2 MVS System Commands, GC28-1031.

27. OS/VS2 System Programming Library: Data Management, GC28-3830.

28. OS/VS2 MVS Data Management Services Guide, GC26-3875.

29. OS/VS Virtual Storage Access Method (VSAM) Programming Guide, GC28-3838.

TRUSTED COMPUTER SYSTEM EVALUATION SUMMARY CHART



DOES NOT SATISFY THE REQUIREMENTS FOR THIS CLASS

NO REQUIREMENTS FOR THIS CLASS

NO ADDITIONAL REQUIREMENTS FOR THIS CLASS

MEETS OR EXCEEDS THE REQUIREMENTS FOR THIS CLASS

SYSTEM NAME	TOP SECRET Version 3.0
VENDOR	CGA Software Products Group, Inc.
EVALUATION DATE	2 April 1985

APPENDIX A

TEST SUMMARIES FOR CLASS C1 REQUIREMENTS

DISCRETIONARY ACCESS CONTROL TEST SUMMARY:

Create an access control matrix defining users and user groups (divisions, departments, profiles) vs. objects with different authorized access rights (i.e., READ, WRITE, UPDATE, etc.) to create the desired security profile.

Ensure that, in both FAIL and IMPL mode, access to "secured" named objects (i.e., data sets, programs, commands, DASD or tape volumes) can be limited to specific levels of access (i.e., NONE, READ, WRITE, UPDATE, CONTROL, CREATE, SCRATCH, FETCH, and ALL) by named individual users/administrators (i.e., users defined via ACIDs to TOP SECRET) or by groups of individuals users/administrators (via PROFILE ACIDs).

In particular, verify that individual users/administrators are able to access data sets with names beginning with their ACIDs (i.e., data sets that they own) and that users are not allowed access to any other objects without explicit authorization, including objects owned by divisions and departments to which those users belong. Verify that, in IMPL mode, users not defined to TOP SECRET are not allowed access to any object defined to TOP SECRET except those permitted to be accessed by ALL. Also verify that, in FAIL mode, users not defined to TOP SECRET are not permitted access to the system.

Ensure that TOP SECRET provides facilities to control which users are allowed to control the access and sharing of objects. Including that the authority of users (and administrators) to specify and control the sharing of resources that they own (or that their department/division owns) can be restricted to certain individuals.

Because PROFILES are added to USER ACIDs, there is no limit to the number of individual users that a PROFILE may be added to. Thus, there is no limit to the number of users allowed an access control list.

IDENTIFICATION AND AUTHENTICATION TEST SUMMARY:

Verify that all users are required to provide valid ACIDs and passwords in order to access the TCB defined by TSO in FAIL

mode. Ensure that, in IMPL mode, all users defined to TOP SECRET are required to supply valid ACIDs and passwords in order to gain access, but that undefined users were not denied access to the TCB.

Ensure that users are only able to submit online batch jobs under their own ACIDs and that valid ACIDs and passwords are required in order to submit batch jobs via physical local readers.

SYSTEM ARCHITECTURE TEST SUMMARY:

Examine the control points where TOP SECRET interfaces with MVS and determine if the system has an identifiable TCB. If so, determine whether the TCB provides protection for itself (i.e., protection from external interference or tampering).

Verify that the MVS service management requests (SRBs) and cross-memory services (new in MVS SP1.3), which require new instructions that are standard on the 308x series, do not allow unauthorized access to the TOP SECRET address space and the audit files.

SYSTEM INTEGRITY TEST SUMMARY:

Ensure that IBM supplied integrity features are sufficient to satisfy this requirement.

SECURITY TESTING TEST SUMMARY:

Using the system documentation, construct a set of functional tests for all aspects of TOP SECRET required to satisfy the requirements of the Criteria. Features of TOP SECRET that will not be tested include the extensive features for password structure and masking and the features for extracting information from batch job cards (both online submission and throught physical readers) to derive the job acid.

Verify that all features of TOP SECRET that pertain to meet the requirements of the Criteria work as claimed in the documentation.

Ground Rule: These attempts will not involve or assume the collusion of a system programming planting malicious code (e.g., Trojan Horse) or computer operator.

Attempts may be made to exploit either the existing code (as delivered by CGA) or code entered via a user/terminal interface.

DOCUMENTATION TEST SUMMARY:

Examine the system documentation to ensure that it contains the required information.

TEST SUMMARIES FOR ADDITIONAL REQUIREMENTS AT CLASS C2

OBJECT REUSE TEST SUMMARY:

Attempt to scavenge data from deleted data sets by utilizing system utilities and/or user written code. These attempts should be performed by a user who possesses no special attributed that would allow him to bypass the protection provided by TOP SECRET or MVS.

IDENTIFICATION AND AUTHENTICATION TEST SUMMARY:

Ensure that the TOP SECRET package provides unique identification of all users on the system. Use the audit utilities to determine whether TOP SECRET provides the capability of associating a users identity with all auditable actions taken by that individual.

AUDIT TEST SUMMARY:

Implement selective auditing of specified authorized accesses and unauthorized access attempts by specified users and for specified resources. Invoke the report utilities and generate the audit reports. Check these reports for correctness by comparing to the actions performed during the testing. Ensure that individual accountability is enforced.

Attempt to obtain unauthorized access to the audit files. Attempt to circumvent auditing for a specified access attempt by first attempting to overload the audit files by appending data to them and/or creating a series of unauthorized access attempts prior to the specified access.

Verify that access to the audit files is limited to those users who are authorized to access the audit information.

Ensure that audit records contain, for each entry; the userid, resource, type of access attempted or obtained, and the time of access.

DOCUMENTATION (Trusted Facility Manual) TEST SUMMARY:

Examine the documentation to determine if all the required information is present and in the appropriate manuals.

DISCRETIONARY ACCESS CONTROL TEST SUMMARY:

Ensure that newly created objects are protected to the specified default level. Attempt to bypass TOP SECRET protection by attempting unauthorized accesses to data sets created by the users in the access control matrix.

Attempt to gain unauthorized access to the TOP SECRET security profile to obtain, add, modify or delete any security related data. Attempt unauthorized accesses to batch facilities and to protected utility programs.